I J C T A, 9(25), 2016, pp. 1-11
© International Science Press

ISSN: 0974-5572

Security Enhancement in EQ-LEACH Routing Protocol

S. Deepa[1], Kamalraj Subramaniam[2], Sridhar K.P.[3] and C.N. Marimuthu[4]

ABSTRACT

The WSN is a collection of small energy constrained devices. In recent years WSN uses hierarchical routing protocol for routing the data packets and it has also been substantially focused by researches to improve performance of the network. There are n numbers of ways to improve the performance of the network, till 100% security and confidentiality plays a major challenge in wireless communication because of many attacks in the communication layers due to lack of memory, power and etc. EQ-LEACH protocol is one of the most widely used routing protocols for its minimum energy consumption in the network. In this paper we have proposed a signature based detection approach to detect variety of network layer attacks in EQ-LEACH.

Keywords: WSN security; EQ-LEACH; Network Layer attacks; Signature based approach.

1. INTRODUCTION

WSN has a vital role in many real time applications such as area monitoring in military, healthcare monitoring by collecting information about an individual's health, fitness, and energy expenditure, industrial monitoring for condition-based maintenance, environmental and earth sensing to detect air pollution, land slide and forest fire detection etc. Here the wireless sensor networks are divided in to different clusters by means of clustering property. And the sensor nodes in the cluster utilize multi hop data transformation without any proper infrastructure due its deployment nature. Here the region of deployment is not physically protected and any attackers can easily contact the region and capture few sensor nodes in the network. Now days due to extensive use of WSN it is necessary to improve its security. In order to protect these networks against various attacks we need to plan a strong security frame work. We know that the network routing protocols can be classified under any one of the following flat base routing protocol, hierarchical base routing protocol and location base routing protocol. [1]

[2][10]EQ-LEACH is the combination of location base routing protocol and Low Energy Adaptive Clustering Hierarchy. The life time of the sensor nodes in the cluster are mainly focused in the design of EQ-LEACH. In case any one of the adversary nodes becomes CH in the network then it can facilitate many routing attack. These routing attacks can be prevented easily by using many techniques such as cryptographic techniques, access control techniques, and authentication techniques etc. And here we propose a new scheme namely signature based approach and it is also called as specification based scheme. The main aim of this paper is to plan and apply the routing attack finding scheme for WSN. And this proposed system can be implemented with some precise rules. And these specific rules are designed based on nature of attacks in WSN [3].

[1] Research Scholar, Department of ECE, Faculty of Engineering, Karpagam University, Coimbatore, India, *Email: Deepaa.selva@gmail.com*

[2] Associate Professor, Department of ECE, Faculty of Engineering, Karpagam University, Coimbatore, India, *Email: kamalrajece@gmail.com*

[3] Assistant Professor, Department of ECE, Faculty of Engineering, Karpagam University, Coimbatore, India, *Email: capsridhar@gmail.com*

[4] Dean Research, Nandha Engineering College, Erode, India.

Here the proposed system has three modules such as

1) Information assembly – collects the data from the nearby nodes and filter out the required features or information.
2) Choice creation – applies the policies on filtered information and increases the breakdown count.
3) Attack discovery – the breakdown count values and threshold values are compared, if it ruptures, an assault was detected by using the extraordinary features.

2. SECURITY ATTACKS IN EQ-LEACH

The wireless sensor networks are susceptible to a variety of attacks. It happens not only from exterior but also from the interior network. These networks are largely subjected to two levels of attacks. Initial one is that the attack on the essential mechanisms of the wireless sensor network such as routing. And the next one is the attack that tries to spoil the safety mechanisms engaged in the network.

The classification of attacks in WSN.

2.1. Active attacks

[4] These attacks are extremely harsh attacks in the network and that will disturb the data packet flow between the two sensor nodes in the network. This active attack can be inside or outside network. The attacks that are approved by the outside source that does not fit inside the network are called external active attacks and internal attacks are due to the cruel nodes inside the network. The internal attack plays a very challenging and tough role inside the network than the external one. The attacks inside the network will create illegal permission to the network and that will helps the enemy node in the network to make alteration in the data packets, Denial of service and jamming etc. The attacks are generally due to the compromised nodes or cruel nodes in the network. The cruel or malicious node in the network will modifies the routing information by marketing itself as that it has a shortest path to the destination node.

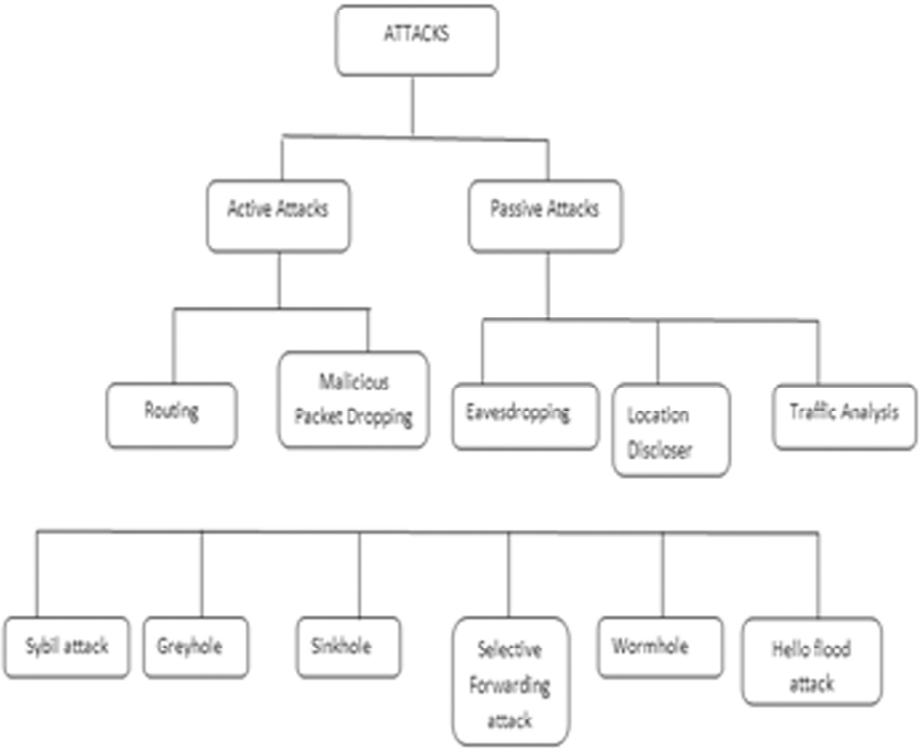


Figure 1: Types of Attacks

ATTACKS IN VARIOUS LAYERS [9]

Layers	*Types of Attacks*
Physical	Eavesdropping, jamming, active interference
Data link	Selfish misbehavior, malicious behavior, traffic analysis
Network	Black hole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource utilization Attack, Sybil attack, selective forwarding. Hello flood attack
Transport	Session hijacking attack, SYN Flooding attack
Session	Authorization issues, session Hijacking
Presentation	Personal Information Retrieval.
Application	Malicious code, Data corruption, viruses and worms

Till now there is no standard layered architecture for wireless communication, any layer can be hacked due to their dodge character. In this, the network layer attacks are most susceptible, because they commerce with the data reliability. The proposed work is to detect the routing attacks for securing the wireless sensor networks.

2.1.1. Black hole and Worm hole Attack

It is nothing but a packet drop attack i.e. the incoming and leaving traffic is dropped without any information the source node that is the data packets did not arrive at its planned receiver. Here the malicious node claim that is has a finest route to the destination node. In EQ-LEACH while broadcasting the data packets towards the destination some nodes may drop the packets intentionally. Once the node has been placed itself between any two communicating nodes, it can alter or discard the data packets passing between the nodes.

The fig indicates the Black hole attack and the node acts as malicious node. When the source node wants to send data packets to its destination node, it automatically sends the data by using restricted flooding. As shown in the fig 2 if any one of the node in the cluster drops the packets then data packets has to reach the destination using its other path in the cluster it may cause some delay in the transmission. In the fig 2 the dotted line indicates no transmission of data packets in that path. In some special case malicious node may be near the destination node itself and drop the packets as a outcome, all the data packets are disbursed or vanished at malicious node.

Wormhole attack is nothing but when more than one node in the network gets compromised within the same cluster, it is sensible to guess that these nodes work together in order to gain an extra benefit. Here the

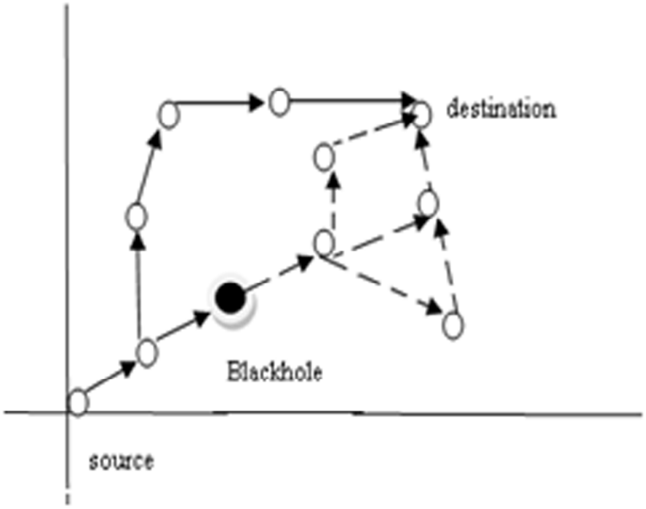


Figure 2: EQ-LEACH- Black hole Attack

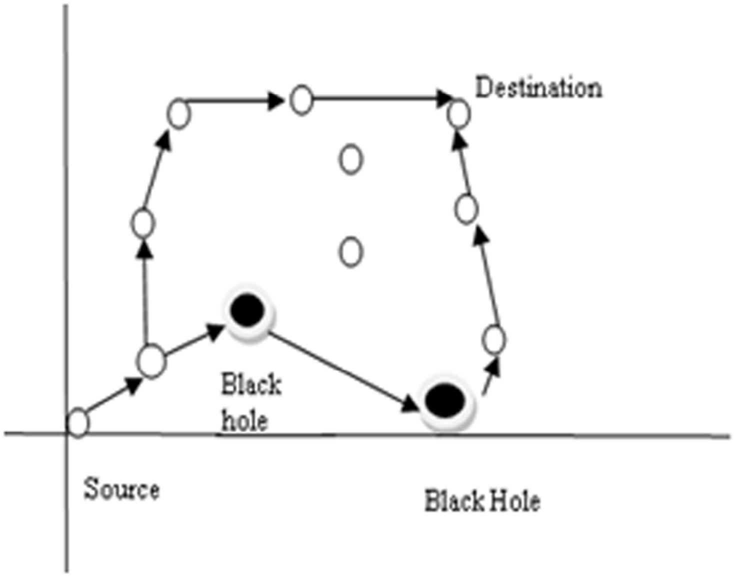


Figure 3: EQ-LEACH- Worm hole Attack

malicious node receives data packets from one point of the network and tunnel them to a new malicious node. The channel survives between two these two nodes is referred to as a wormhole attack. Due to this effect the path between the source and destination may get increased and in some case the malicious node may drop the packets and as a result data packets get lost.

2.1.2. Sybil attack

In this attack, one malicious node counterfeit and generates a large number of identities and mislead the legitimate nodes into believing that they have several neighbors. The supplementary identities that the node acquires are called Sybil nodes. [8] A Sybil attack posses a considerable threat to geographic routing protocols. In geographical routing protocol, each Sybil node requires to broadcast packet with its neighbors. Here the malicious node tries to magnetize the data packets from all its adjacent nodes. The sensor nodes in EQ-LEACH exchange their neighbors' location coordinates with their nearby nodes by sending beacons at regular intervals. Thus an adversary may claim to be present at more than one location to its neighbors' by sending multiple beacons, each time with different site information as in Fig. Here an adversary node sends

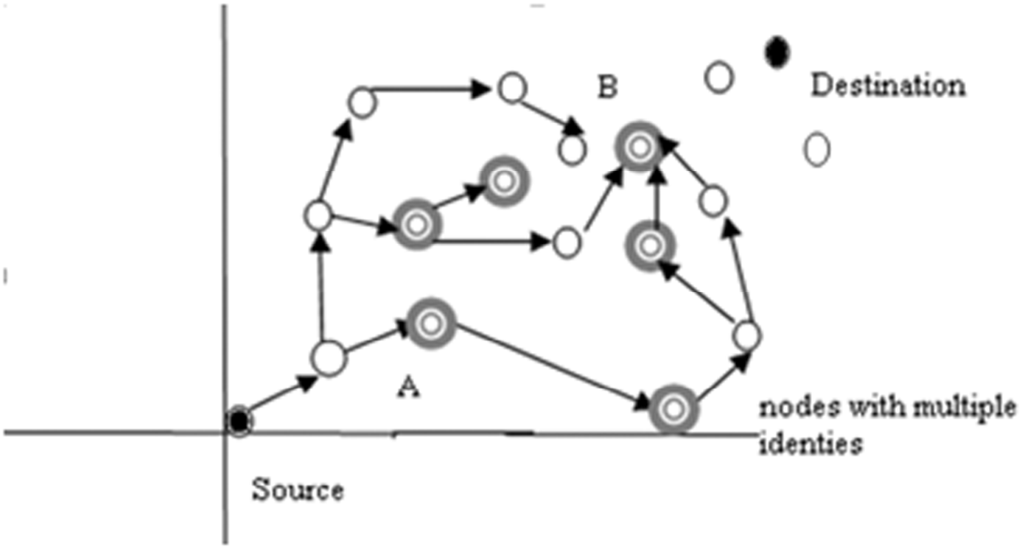


Figure 4: EQ-LEACH- Sybil Attack

different locations to neighborly nodes. Thus node A is forced to send packet to node B which is actually beyond the destination node to which it eventually wants to send the packet.

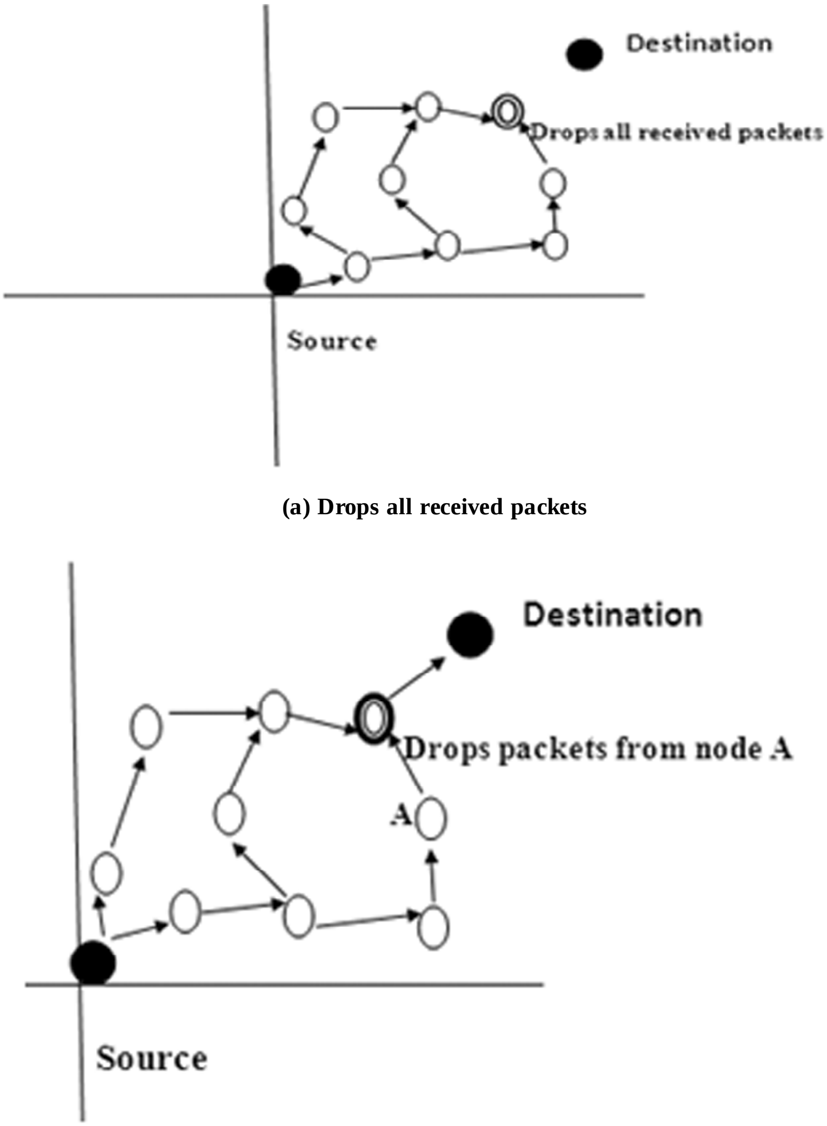
2.1.3. Greyhole attack

[5] Greyhole attack is an extraordinary distinction of black hole attack, in which malicious node will drop the data packets selectively and it is also called as selective forward attack. Here nodes change their state from black hole to sincere occasionally and vice versa. It is hard to notice Greyhole attack because nodes may crash some packets partially and behaves like an ordinary node in the network. [6] Two cases of attacks are possible in grey hole i.e. dropping all the packets while forwarding and in second case dropping 50% of packets or for shot time period it will drops the packets and switch to the normal mode as honest node.

Here the normal node and Greyhole node were same so it’s very difficult to find the attack

3. PROPOSED WORK- SIGNATURE BASED APPROACH

Here in the proposed work signature based detection system is described in the flowchart. this detection approach has three main phase as said before they are Information assembly, choice creation and attack discovery.



(a) Drops all received packets

(b) Drops packets from selective node

Figure 5: a & b EQ-LEACH- Grey hole Attack

3.1. Phase 1: Information Assembly

Whenever a node receives a message, here it will validate whether the data packet is from the valid neighbor node or not. If it is from the valid node, then the node will forward the data packets to the next node, Otherwise it will be discarded immediately. Here the Significant and necessary features will be filtered out and stored for next analysis.

3.2. Phase 2: Choice Creation

Here it finds the nodes that are being impaired by an enemy. Here the collected data is rated according to the order of particular rules. Those particular rules are applied to notice the network routing attacks. If the data fails in the particular rules, then a breakdown count will be increased and the message will be discarded and no need for further rules.

3.3. Phase 3: ATTACK DISCOVERY

Here threshold value was set by discovery the scheme. And the threshold values are set by analyzing the network in normal working mode and the way network behaves after some specific attacks are introduced in the network. The node behavior and its failure count in the network abuse this value during next time,

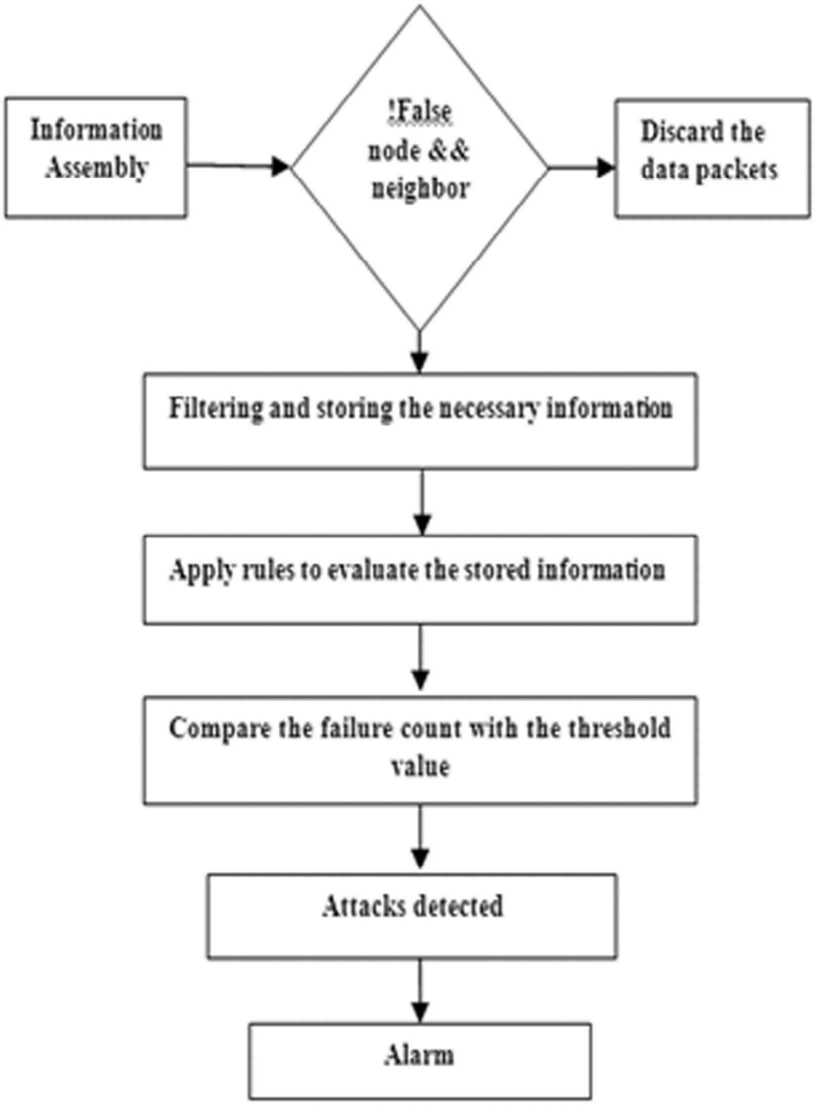

Information Assembly
!False node && neighbor
Discard the data packets
Filtering and storing the necessary information
Apply rules to evaluate the stored information
Compare the failure count with the threshold value
Attacks detected
Alarm

Figure 6: Routing attack detection system

and the attacks can be detected. In this system, the following routing attacks such Sybil attack, Wormhole attack and Black-hole attack as are measured.

4. RULES COUPLED WITH THE ATTACKS

Here the system feature was described by considering the different attacks and the rules associated with the attacks. The nodes will retransmit the data when the node gets is interloped, due to this two attacks are possible in the network namely selective forward attack and Black hole attack. Here retransmission rule is used. Here we can spot the intruder nodes that modify the original message by using the data integrity rule. So that nodes can receive message only from its neighbor nodes. To detect the wormhole and hello flood attack in the network and the radio range rule is used. When a node moves from one place to another fake physical identities can be created but its MAC identities cannot be changed. To detect Sybil attack this MAC identity rule cab be used.

5. IMPLEMENTATION DETAILS

In the planned work a network simulator was developed and implemented by using NS 2. By using a distinct event model, the states of the nodes were analyzed till any one transmission or reception takes place. Here the transmission or reception is generated by chance and the sensor nodes are not coordinated, this is just a trial to guess the simulator to the real time network. The nodes in the network collect the data and sends to the receiver node.

The node in the network is incharge to monitor its neighbors looking for false nodes. Because of this action, the nodes in the network keep its radio in a licentious mode, and store the information and process it in accordance to the framed rules. The nodes in the network is an ordinary nodes only were detection system is build in it and it performs the action of normal such as routing and etc. here the false node always changes its character from common action to the false action.

The different type of attack depends only on the action of the intruder nodes. Only attacks on the data messages were considered. The data message measured at this time has the subsequent fields such as next bound, data type, previous bound, source, final target, sequence number, and data. We have simulated this plan in a fixed network with a random node distribution.

6. RESULTS AND DISCUSSIONS

Here the performance is calculated by comparing the throughput and packet delivery ratio with and without various the attacks.

Simulation Parameters

Simulation Area	100m × 100 m
Number of Nodes	50
Packet size	512 bytes
Transmission protocol Type	User Datagram Protocol
Traffic type	Common Bit Rate
Simulation time	100 s
Queue type	Drop tail
Propagation model	Two ray ground
Antenna Type	Omni directional antenna
Routing protocol	Restricted flooding
Initial energy	100 J
Attack types	Sybil attack, worm hole attack and black hole attack

Network throughput is the amount of data delivered successfully and packet delivery ratio is the ratio of received packet over sent packet in the network. , and typically measured in bits per second (bps). The number of data packets transmitted and network throughput may vary due to the occurrence of false nodes. Here the false node illegitimately claims several identity or false IDs, and then there will be Sybil attack in the network.

The network throughput and Packet delivery ratio of the three attacks is shown in Figs. 7, 8, 9, 10, 11 & 12 respectively. The throughput of the WSN after the detection is comparatively higher than throughput of network with no attack detection. The packet delivery ratio is also greater after detecting the attacks in the network.

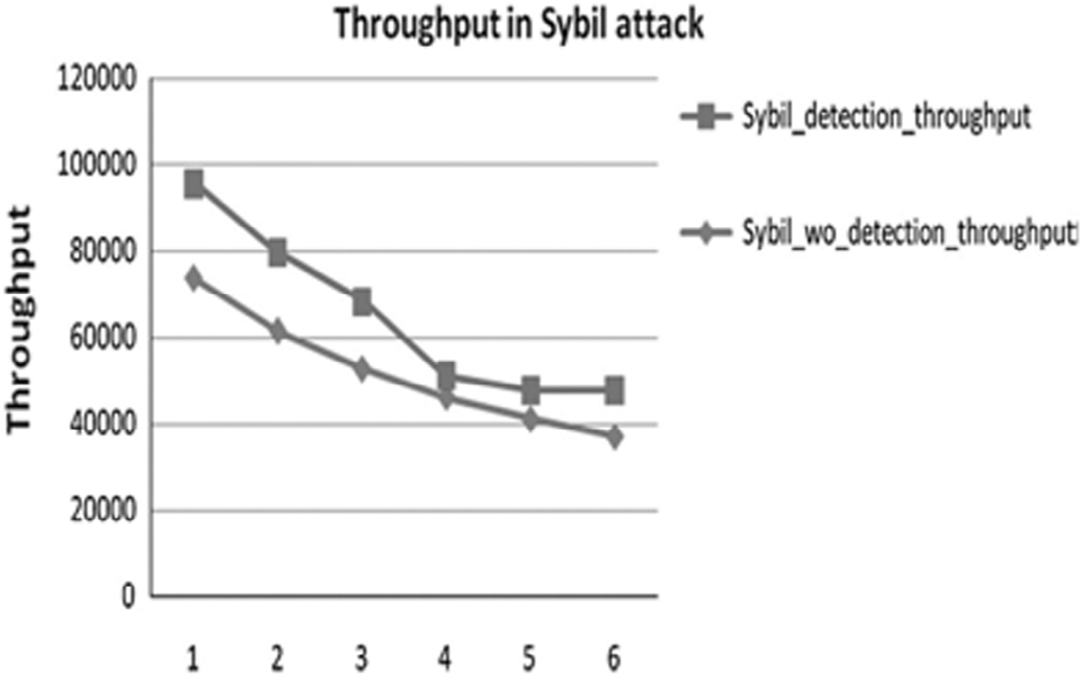


Figure 7: Sybil attack_Throughput

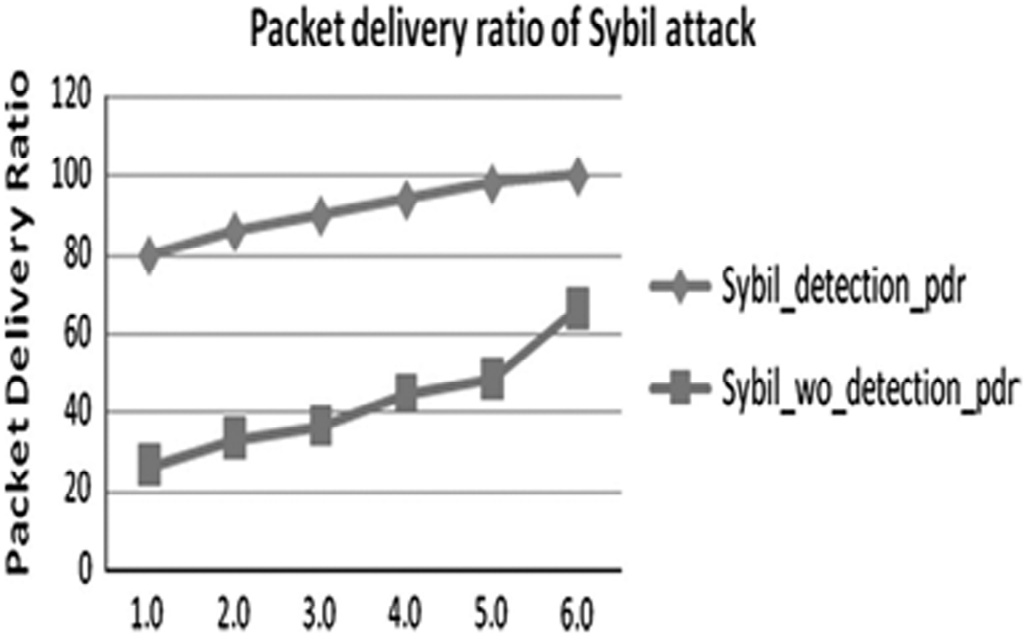


Figure 8: Sybil attack_pdr

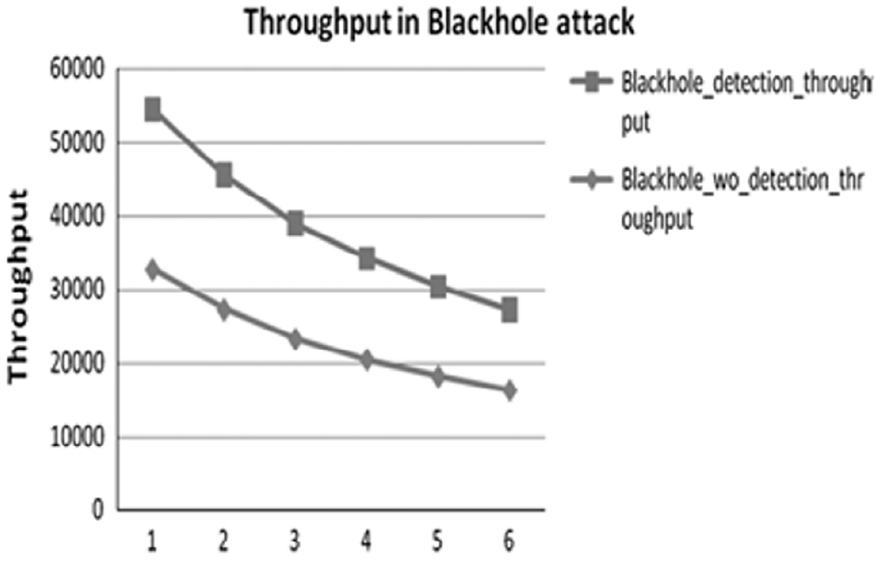


Figure 9: Black hole attack_Throughput

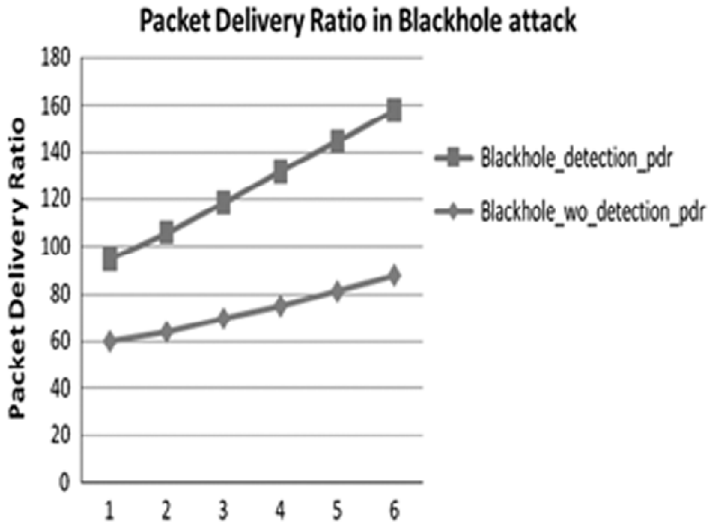


Figure 10: Black hole attack_pdr

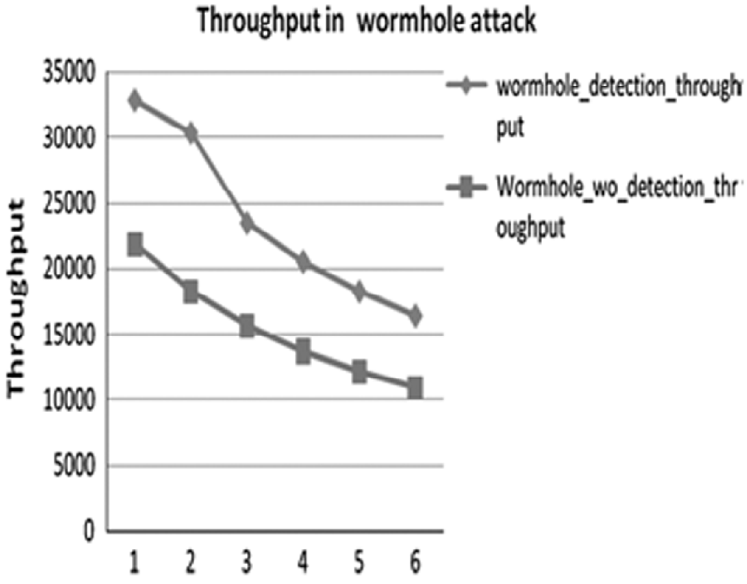


Figure 11: wormhole attack_Throughput

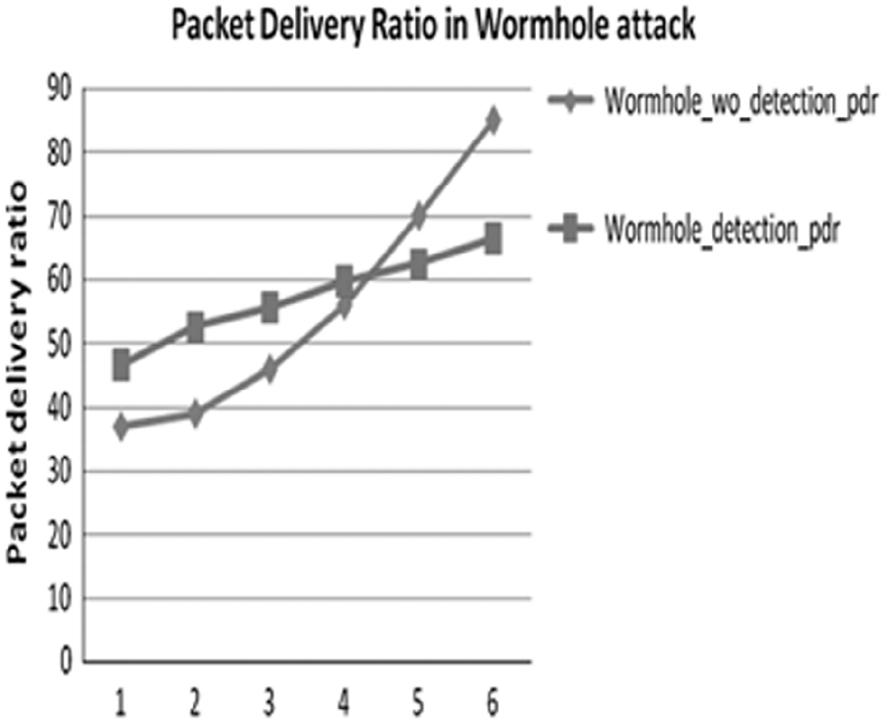


Figure 12: wormhole attack_pdr

7. CONCLUSION AND FUTURE WORK

Network security plays a very important role in wireless sensor networks but due to its lack of resource constraints and new forthcoming attacks. But these routing protocols were designed without seeing any safety measures to transmit the data. Hence, it is very essential thing to structure a safety measure that makes the network supple against network layer attacks. The attack detection approach is the main aim of this planned work. In that we had a brief in three main attacks namely black hole, wormhole and Sybil attack. And here we have proved the reliable data transformation from source to destination by detecting attacks in the network layer.

And here the parameters such as throughput and packet delivery ratio of the network have also got increased. As a future scope, we have planned detect even unknown attacks by using fuzzy logic scheme.

REFERENCES

[1] Gangandeep, Aashima, Pawan Kumar “Analysis of Different Security Attacks In MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2] Deepa S, C. N. Marimuthu, Dhanvanthri V “Enhanced Q-LEACH Routing Protocol for Wireless Sensor Networks”, ARPN Journal of Engineering and Applied Sciences. ISSN: 1819-6608, volume-10, Issuue-9, May 2015.

[3] N. M. Saravana Kumar, S. Deepa, C. N. Marimuthu, Eswari, S. Lavanya “Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission” published online: 11th October 2015.

[4] Alakesh Braman , Umapathi G. R. “A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks: A survey” , International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.

[5] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi “Various Attacks in Wireless Sensor Network: Survey”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[6] Leela Krishna Bysani, Ashok Kumar Turuk “A Survey On Selective Forwarding Attack in Wireless Sensor Networks”, international journal of scientific engineering and research(IJSER), ISSN(online): 2347-3878, Volume 2, ISSUE 6, June 2014.