International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Detection and Elimination of Black Hole Attack in WSN

S.Ilavarasan, P.Latha

ABSTRACT ***Wireless Sensor Network has become one of the most emerging areas of research in recent days. WSNs have been applied in a variety of application areas such as military, traffic surveillance, environment monitoring and so on. Since WSN is not a secure network and each sensor node can be compromised by the intruder. There are plenty of security threats in sensor networks like Black hole Attack, Wormhole attack, Sinkhole attack. Recently, there are so many algorithms are proposed to detect or to prevent attack by the researchers. Still, the research is continuing to evaluate sensor nodes' trust and reputation. At present to monitor nodes' behavior direct and indirect trust values are used and most of the detection method uses additional nodes to detect an attack. These method increases the cost and also overhead. This paper proposed a method which detects the Black hole attack without using any additional node to monitor the network. The proposed work uses Attacker Detection metric (AD metric) to detect malicious node based on the average sequence number, time delay and reliability. OLSR protocol is used for routing which improves the network lifetime by minimizing the packet flooding. Besides, to ensure reliable data transmission Elliptical Curve Digital Signature Algorithm is used. Simulation results are obtained and show malicious nodes are eliminated using AD metrics***

Keywords: AD metrics, OLSR, Black hole attack, ECDSA Algorithm

I. INTRODUCTION

In recent days, Wireless sensor networks (WSN) have gained worldwide attention for use in different applications to observe environmental conditions like temperature, vibration, sound, pollution etc. and aggregate the data and forward through the nodes to base location. The WSN has developed from military applications like surveillance in ware field. Recent days WSN has become more popular, industries are using this kind of network for monitoring and controlling machine, in Hospitals health monitoring, and so on. This kind of network has become popular because of its smaller in size and lesser cost, but the constraints on sensor nodes are limited memory, less computational speed, limited energy (battery power) and less bandwidth.

A WSN network consist of sensor nodes that are densely deployed in an location the need to be monitored called Sensor Field. Each Sensor nodes aggregate data and pass it to sink node or Base Station (BS). In general sensor networks communication pattern will be of multi-hop because the sensor nodes have limited processing capacity, communication range and limited energy.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Mr.S.Ilavarasan*, Assistant Professor(SG), Department of IT, Saveetha Engineering College, Chennai, India.
Dr.P.Latha, Professor, Department of IT, Saveetha Engineering College, Chennai, India.

While forwarding data packets to the sink node or base station, Data loss may occurs due to the vulnerability of malicious node.

There are several attacks on sensed information during transmission, out of all the most known attack is black hole attack also known as packet dropper attack. Here the intruder influences the sender that it has the best route to the destination. The packets that it receives from sender it drops or absorbs.

A black-hole attack [12], publicizing a paths as best path from the source node by a compromised node during the route establishment process in on demand routing or updating route information in table driven routing protocols. To resolve this attack, we proposed AD metric in which we need to calculate the value for Average Sequence Number, time delay and reliability.

II. LITERATURE SURVEY

To detect the malicious node the author proposed a method when a packet is broadcast by a source node, a virtual cylinder with radius w is created from the source node to sink node. All the nodes located in this virtual cylinder are allowed to forward the packet through the multipath, if any compromised node in virtual cylinder the packet may be forwarded to the sink through the other way of the virtual cylinder [1]. Multiple base station with an optimized position using a genetic algorithm has proposed for successful packet delivery in the presence of black hole attack [2]. "Improvised hierarchical vitality-efficient intrusion system" protects sensor fields from black hole attacks. It is based on forwarding control packets among the sensor node with base station.

To protect nodes from black hole attack, base station act as a monitor node to detect any malicious node. Sensor nodes can be pretend as black hole nodes with the cluster head and an efficient mechanism can be formulated. [3]. In this paper concentrated on Detection and Prevention of Black Hole Attack in cluster-based Wireless sensor networks. Clustering-based network with two cluster heads in each cluster that are being used for black hole detection and prevention. To detect malicious node, select two cluster heads in a cluster. Clustering increases the energy efficiency of the sensor network. It facilitates lower energy consumption. In the detection phase, the base station perceives the malicious nodes. In the removal phase, the compromised node is removed. [4]

The work impact of black hole attack against low energy adaptive LEACH protocol on the wireless sensor network is analyzed using identified metrics. They considered 50 nodes in the sensor field. For leach performance under Black hole attack, Ns2 is used.

Here based on the maximum node it should identify whether a network is under attack or not. If a node is not selected as CH>max, the network is under attack. This work can be extended by using different topology, different protocols, and different stimulation protocols. [5]

In this paper, a new clustering algorithm called "black hole entropic fuzzy clustering" has proposed. It calculates "black hole entropy-based information theory", Bayesian inference model, fuzzy and clustering. Partition accuracy is identified in form of the 1-m data set and also used Incremental version. Experimental result obtained on synthetic and real datasets and image of segmentation and shown that the results in improvement in clustering. Theoretical analysis & potential application of BHE – based fuzzy clustering with m being 1. This paper demonstrates how to develop a guideline about fuzifier setting of proposed algorithms, Imbalanced data sets and noisy data sets. [6]

The packet delivery performance purely based on the mobile nodes in wireless relay networks like delay-tolerant network and device to device communications. However, some nodes may avoid transmitting data from to others or sharing their data for several reasons such as limited resource or social predilections. It reduces the misbehaving node and also improves data transfer performance. [7]

III. PROPOSED METHODOLOGY

A Route Discovery

Discovery route in WSN achieved by Broadcasting (RREQ) Route Request Message. When a node need to forward data to a specific node it first refers its routing table to find the path. If path doesn't exist it will broadcast the RREQ message to all the neighbors'. The neighbor node updates its routing table and forward further till the RREQ reaches the destination.

If the node is the destination node it replies with RREP Message. The RREP carries the route information between sender and receiver. If intermediate node knows the destination and if it has bidirectional link it can send RREP with the entire path information between source & destination.

In the figure 1, S is the Source node wants to communicate with the destination node D and it forwards RREQ to its adjacent node J, L & M. Node J and M forward the RREQ packet towards the Destination node. Once the RREQ received by the destination node D, it replies with RREP.

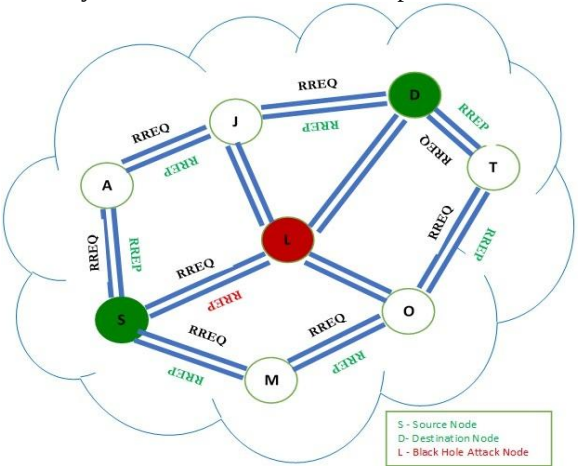

Figure 1 Route Discovery in WSN

B. Black hole attack

In Black hole attack [12], during route finding a Compromised node claim itself has a node with shortest path and does not propagate the packets to its neighbors' and drops it. The Node L is a malicious node which pretends as the destination node and forwards a RREP to the source nodes.

C. OLSR (Optimized Link state Routing Protocol)[8]:

OLSR is a link state protocol which categories under proactive routing that uses hello packet to ascertain and the broadcast link state information in the network. It is best routing protocol for wireless network which reduces packet flooding to Individual node through selecting a specific set of nodes as MPR node. Only selected MPR nodes will forward the hello packets in the networks.

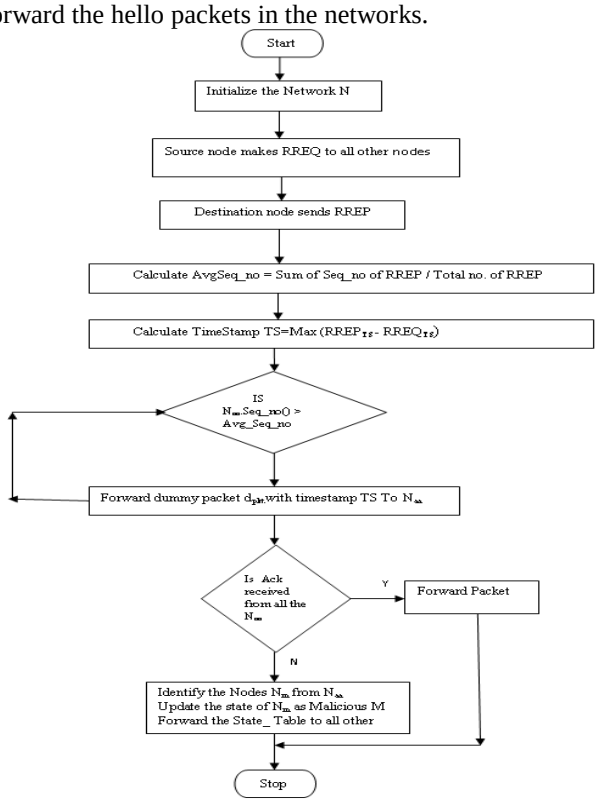

Figure 2 Flow Diagram of Proposed Work

D. PROPOSED ALGORITHM FOR BLACK HOLE ATTACK DETECTION & PREVENTION

1. Initialize the network N with n nodes

N = 1, 2… n

2. Source node N_s initialize Route Discovery to N_d by sending RREQ

$$N_s \xrightarrow{RREQ(N_d)} Adj(N_s) \xrightarrow{RREQ(N_d)}$$

3. $Adj(N_s) \longrightarrow$ Until it reaches N_d
4. N_s stores RREP of N node in State_Table [Seq_no., Node, State, Time]
5. Calculate Average Sequence value AvgSeq_no of n node using RREP message

AvgSeq_no = Sum of Seq_no of RREP / Total no. of RREP

6. Calculate TimeStamp $TS=Max(RREP_{TS} - RREQ_{TS})$
7. Select all nodes N_{aa} whose Sequence no is above avg. sequence

8. For all Node N_{aa}.Seq_no() > Avg_Seq_no
   Forward dummy packet dpkt with timestamp T
   To N_{aa} Wait until TS Expires
9. If Ack received from all the N_{aa} Then
Forward packet
Else
Identify the Nodes N_m from N_{aa}
Update the state of N_m as Malicious M
Forward the State_ Table to all other nodes
   End if

Once the RREP is received from various nodes the source node calculates the average sequence value. Average sequence number is the threshold value calculated by sum of sequence number divided by number of RREP. The source node also calculates Time stamp (TS) based on Maximum time difference between RREQ and RREPs. Source node identifies the nodes whose sequence value is greater than the average sequence value (Threshold) and forwards a dummy packet (dpkt) with time stamp (T) to them. Source node waits till time stamp Ts elapse and look for acknowledgement. If the source node receives the acknowledgement from any node it marks the status of the node as normal (NN). If any node fails to acknowledge then that node will be identify as a malicious node an update is done as Malicious (MN) on state table. Forward the information to rest of the nodes.

Table 1 State Table

Node	Seq_no	State	Time Stamp
A	1276	*NN*	2.32
L	1346	***MN***	TS expires
M	1302	*NN*	2.36
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.

E. Elliptical Curve Digital Signature Algorithm

In general, hard-to-solve problems are solved using public key cryptography algorithms. RSA is most popular algorithm for public-key cryptography, based on the prime factors. [13][14].

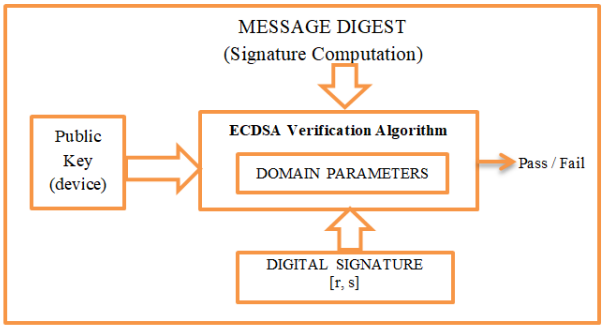

Figure 3 ECDSA Authentication System

The figure 3 shows the ECDSA authentication system, ECDSA uses Elliptical Curve Computation (ECC) which is constructed on the exertion of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curves associate with number theory and algebraic geometry. These curves can express in many arenas of numbers though It is usually seen them using over finite fields for applications in cryptography. The below diagram shows the process of ECDSA which comprises of Two phase. The first phase is signing phase where the message is converted in to hashed signature using public key. The sender calculated the hash value for the message and forwarded it along with message to the destination. In the second phase i.e. verification phase the received message is given as input to compute the hash value in destination and the computed hash value is compared with the hash value received from send. If both the hash value matches then the verification passed.

Signing	Verification
Given point, G, on Curve, E	
Message, m	
Select private key, d_A	
Compute public key $Q_A = d_A G$	
m, Q_A ---------->	e=HASH (m), z=leftmost bits of e
e=HASH (m),	
z = leftmost bits of e	
Select integer,	
Calculate (x1, y1) = k G	
r = x1 mod n	
$s = k^{-1} (z + r d_A) \bmod n$	
Signature (r, s) ---------->	$W = s^{-1} \bmod n$
	u1 = z W mod n
	u2 = r W mod n
	$(X1, y1) = u1\ G + u2\ Q_A$
	Signature valid if $r \equiv x1 \pmod n$

IV. SIMULATION RESULT & DISCUSSION

A. STARTING NETWORK SIMULATOR

Start Network Simulator using the commands

```
$ cd ns-allinone-2.28/ns-2.28/
$ startxwin.bat
```

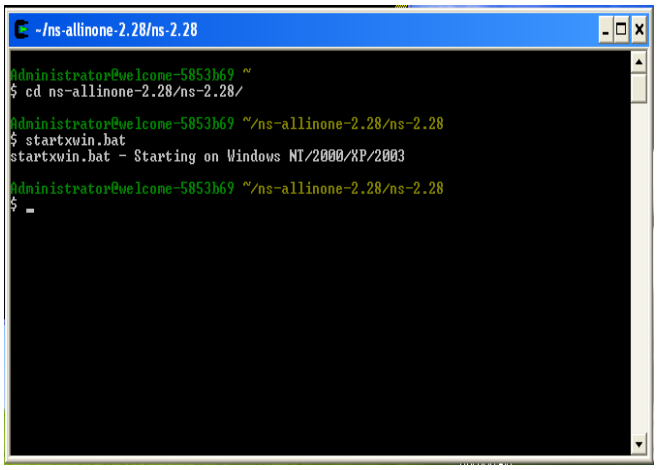

Figure 3 Starting Network Simulator

B. ASSIGNING SOURCE AND DESTINATION NODE

Source node and Destination node are assigned.

Figure 4 Assigning Source and Destination node

C DETECTING MALICIOUS NODE

Black hole attack (node which drops data packet) is detected in the path.

Figure 5 Detecting Malicious Node

D. DATA TRANSMISSION

Data is transmitted from source to destination in the safe path.

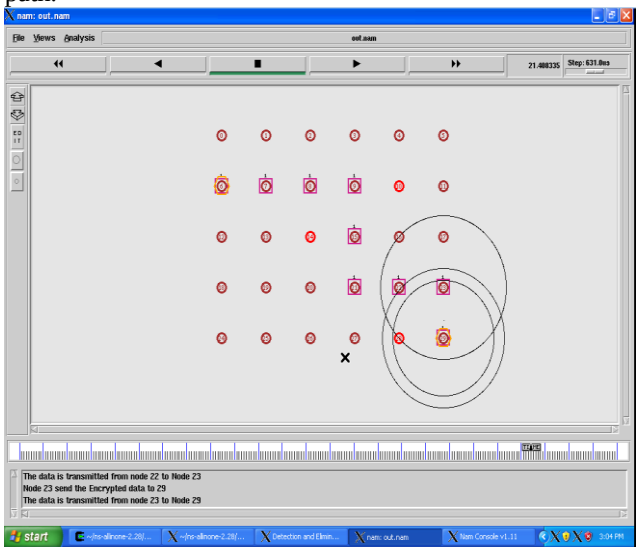

Figure 6 Data Transmission

E. SECURE TRANSMISSION

Data is received by the destination node in a safe manner.

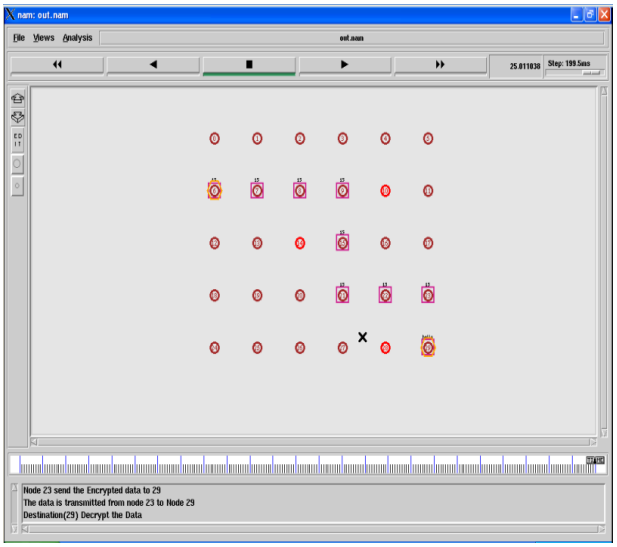

Figure 7 Secure Transmission Paths

V.PERFORMANCE ANALYSIS

A Simulation Parameter

PARAMETER	VALUE
Simulation area(m*m)	1500*300
Number of nodes	30
Simulation time(sec)	900
Mobility model	Random way point
Maximum speed(m/sec)	20
Pause time(sec)	0,30,60,120,300,600,900
Number of communicating nodes	10,20,30
Application layer	Constant Bit Rate(CBR)
Packet size	512 bytes
Packet rate	4 packets/second
Routing protocol	OLSR
Number of black-hole nodes	3

B Simulation Results

The performance analyses of the proposed algorithm are compared with three network environment namely normal network (without Black hole attack) network with black hole attack, proposed method. The following parameters are considered.

- End-to-End Delay
- Packet Delivery Ratio
- Throughput

C End-to-End Delay

Generally, Packets are delivered from source from to destination nodes with delay, which varies from packet to packet the random manners of end-to-end packet delay is the focus of this work.

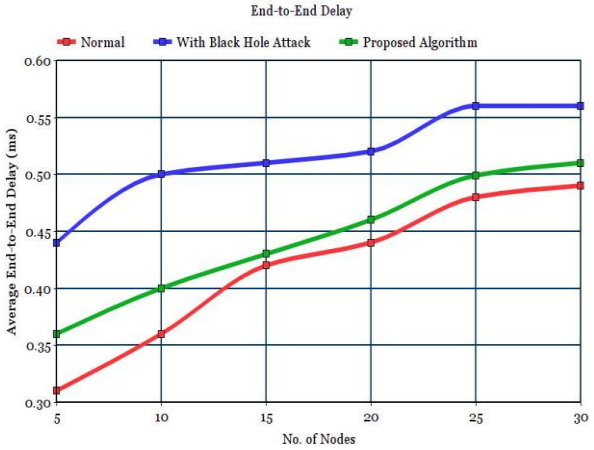

Figure 8 End-to-End Delay comparison

The above Figure 8, shows the comparison of average end-to-end delay between the network The simulation result has been obtained with different size of nodes over the period. In Normal network during 5 nodes, the average delay is 0.32 ms whereas when the network has a malicious node (black hole attack node) then the average delay has increased to 0.044ms, but In the proposed method the average end-to-end delay is 0.35 which is closer to the normal environment. When the number of node increases the in malicious node network the delay has drastically increased but in the proposed method the delay is 80% lesser which is closer to normal network. The simulation results show that the proposed method is efficient.

D Packet Delivery Ratio

To formulate the effectiveness of the proposed Blue algorithm, where the difference between the number of packets received and the actual packet transmitted in the particular period

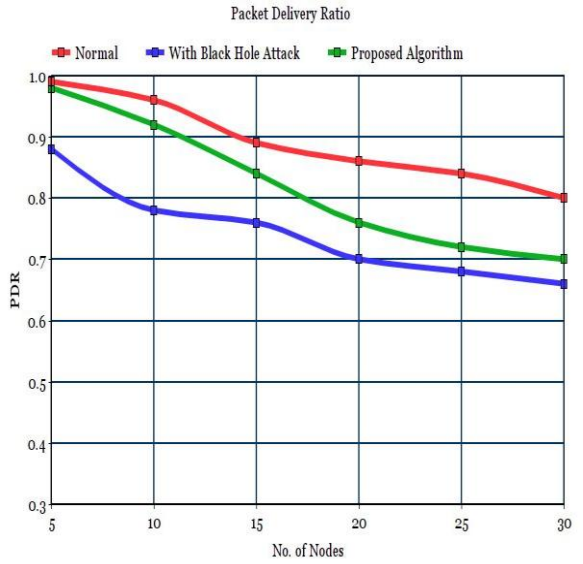

Figure 9 Packet Delivery Ratio

The above Figure 9, shows the comparison of average Packet delivery ratio between the network The simulation result has been obtained with number of packets received in different duration in different size of nodes. In Normal network during 5 node, the average packet delivered is 0.99 percent whereas when the network has a malicious node(black hole attack node) the average packet delivered is only 0.89, but In the proposed method the average packet delivery has increased because of the OLSR routing protocol which is 0.98 which is very closer to the normal environment. When the number of node increases the in malicious node network the packet delivery ratio has drastically decreased but in the proposed method the PDR is higher. The simulation results show that the proposed method has increased in packet delivery.

E Throughput

Data rate are measured with time interval by dividing the amount of successfully transmitted data by the interval duration. The amount of data or packets can be transferred from the source to destination(s) with a fixed time.

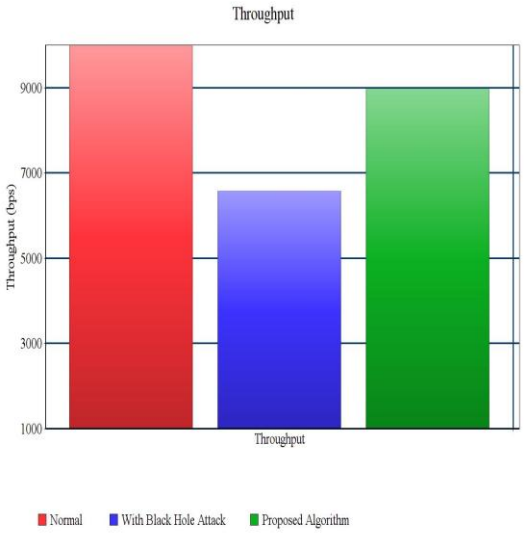

Figure 10 Throughput comparison

The above Figure 10, shows the comparison of Throughput achieved in various network. In Normal network throughput is 99 percent whereas when the network has a malicious node (black hole attack node) the average throughput is only 69, in the proposed method the average throughput has increased because of the OLSR routing protocol which is 89 percent. When the number of node increases the in malicious node network the throughput has drastically decreased but in the proposed method the throughput is stable. The simulation results show that the proposed method has increased in throughput.

VI. CONCLUSION

The proposed Attacker Detection metric (AD metric) is used to detect black hole attack in the WSN based on the parameters like bandwidth, time delay and reliability. OLSR routing protocol is used for effective packet forwarding which maximized the network lifetime. The proposed algorithm uses different metrics like average sequence number and maximum timestamp to identify the malicious node. Nodes with a higher sequence are identified as a potential malicious node and sent dummy packets to check its behavior. The malicious node will drop the packets so that it can be easily identified. The state of each node will be shared to the rest of the node. To enhances the security level in the network. Elliptical Curve Digital Signature Algorithm has been implemented for secured data transmission in the network.

Performance analysis has been done and proved that the proposed algorithm identifies the black-hole attack.

REFERENCES

1. Elham Bahmanih , Aso Mohammad Darwesh , Mojtaba Jamshidi , Somaieh Bali " Restricted Multipath Routing Algorithm in Wireless Sensor Networks Using a Virtual Cylinder: Bypassing Black hole and Selective Forwarding Attacks ",UHD Journal of Science & Technology 2019.
2. Gagan Singla, Sourav Garg, Jagbir Singh Gill et al. "Multi BaseStation optimized positioning for Black Hole Attacks in Wireless Sensor Networks," *Recent Trends in Sensor Research & Technology* 2018; :
3. An Improved Hierarchical Black hole Detection Algorithm in wireless sensor networks", A.Babu Karuppiah, J.Dalfiah, K.yuvashri,S.RajaRam (2015)
4. "Prachi Dewal,Gagandeep Singh Narula, Vishal jain", Detection and Prevention of Black Hole Attack in cluster based Wireless sensor networks, 3rd International Conference on computing for sustainable global development (2016).
5. "Visali bansal, Krishnan Kumar saluja ", Anomaly based detection of block hole attack on leach protocol in wireless sensor network March 2016, in IEEE conference.
6. Black hole Entropic fuzzy clustering, Jiefang Liu, FU-Lai chung, Shitong Wang 2017
7. A survey on Human centric communications in Non cooperative wireless relay Networks, feng xia, Zhalong Nisg, (2018)
8. Deng H, Li W, Agrawal DP: Routing Security in Wireless Ad-hoc Networks. *IEEE Communications Magazine* 2002,**40**(10):70–75.
9. Mustafa KocaKulak, Ismail Butun, "An Overview of wireless sensor Networks towards Internet of Things", IEEE-2017
10. Tapiwa M.Chiwewe, Colman F.Mbuya, Gerhard P.Hancke, "Using Cognitive Radio for Interference -Resistant Industrial Wireless Sensor Networks:An Overview", IEEE-2015
11. Minimization of Black Hole Attacks in Adhoc Networks using Aware response Mechanism",D.John Aravindhar, S.G. Gino Sophia, Padmaveni Krishnan, D.Praveen Kumar, IEEE-2019
12. Security Issues of Black hole attacks in MANET",Rakesh Ranjan, Nirnemesh Kumar Singh, Ajay singh, ", IEEE-2015
13. Pritam Gajkumar Shah, "An Empirical Study of Elliptic Curve Cryptography for the Resource Constrained Wireless Sensor Network", 'Australian Journal Of Wireless Technologies, Mobility and Security (2019)'.
14. Darshana Pritam Shah, Namita Pritam Shah,"Implementation of Digital Signature Algorithm by using Elliptical Curve p-192", Australian Journal of Wireless Technologies, Mobility and Security (2019).

AUTHORS PROFILE

Mr.S.Ilavarasan, who is currently working as Assistant Professor(SG) in the Department of IT, Saveetha Engineering College, Chennai and doing Part Time Research in Saveetha University. Having more than 12 Years of Teaching Experience and Published papers in 5 Internationals Journals, 4 International Conferences and 3 National Conferences. Attended more number of workshops, Faculty Development Program and organized 3 workshops in various topics. Currently pursuing his research in the area of WSN (Security issues particularly in Network Layers).

Dr.P.Latha, who is working as Professor in the Department of IT, Saveetha Engineering College, Chennai. Having more than 20 years of Experience in the field of teaching &Completed doctorate at Sathayabama University in 2011. Published papers in 10 International Journals, 6 International Conference and 3 National Conference. Having guide ship in Saveetha University and Doctorial Member of Various Universities .Received Rs 20,000 from TN state Council for organizing the science exhibition under the scheme of "Popularization of science activities" in June 2011. Active member of ACM, IACSIT, IAENG, and CSTA