# A lightweight Security Framework for Wireless Sensor Networks against the Blackhole Attack

Ganesh R. Pathak

*Dept. of Computer Science & Engineering
Sathyabama Inst. of Sci. & Tech. (Deemed to be University), Chennai, India
Sinhgad College of Engineering, Pune
parhak.gr@gmail.com*

M.S. Godwin Premi

*School of Electrical and Electronics Engineering Sathyabama Inst. of Sci. & Tech. (Deemed to be University), Chennai, India
msgodwinpremi@gmail.com*

Suhas H. Patil

*Dept. of Computer Science and Engineering
Bharati Vidyapeeth University College of Engineering, Pune, India
suhaspatil.bvucoe@gmail.com*

Shashank D. Joshi

*Dept. of Computer Science and Engineering
Bharati Vidyapeeth University College of Engineering, Pune, India
sdj@live.in*

## *Abstract:*

*In recent days the most emerging research field is the Wireless Sensor Networks. Wireless Sensor Networks have been used in numerous fields of application like traffic control, environmental monitoring, military etc. Since the attacker can compromise each sensor node, the WSN isn't a safe network. Security vulnerabilities such as Sinkhole Attack, Black Hole Attack, Wormhole Attack are numerous in sensor networks. In recent times too many algorithms are being suggested to identify or prevent the researchers from attacking. Still, the work continues to assess the trust and credibility of the sensor nodes. Currently, indirect and direct trust values are used to track the behavior of nodes and a majority of the monitoring system detects an attack using additional nodes. This approach raises costs and overheads as well. This paper proposes an EDPMBA i.e. Enhanced Detection and Prevention Mechanism for Black Hole Attack Method of Trust which detects the Black Hole attack in the network. Attacker Detection metric is used in the proposed work to identify malicious nodes based on time delay and reliability.*

***Keywords:*** *Protocol, Black hole attack, EDPMBA Algorithm.*

## I. Introduction:

Recently, WSN i.e. Wireless Sensor Networks have been gaining popularity worldwide for its usage in various application to detect conditions environmentally such as vibration, temperature, noise, sound, etc. and to collect and forward data to the base position through the nodes. The origination of WSN was from military applications including monitoring of war fields. Recently, wireless sensor network has become more common; businesses use this kind of network to track and manage equipment, hospital monitoring of health, and so on. Thanks to its smaller size and lower cost this kind of network has become popular, but limited memory, limited battery power, lower processing speed and lower bandwidth are the limitations on sensor nodes. A highly dispersed sensor nodes are consisted in a WSN network, which must be tracked at a location called the Sensor Field. Sensor node aggregates data and moves it to either the Base Station (BS) or the sink node. Communication patterns in the regular sensor networks must be multi-hop, since there are limited resources, processing capacity and communication range in the sensor nodes. loss of data can occur due to the vulnerability of malicious nodes as data packets are forwarded to the base station or sink node.

During transmission, the sensed information is attacked many times; packet dropper attack is the same as black hole attack, amongst the most common attacks. Here the fastest path leading to the destination is got and told by the intruder to the sender. The packets received from the sender is removed or eaten. A black-hole attack [12], advertising a way through a compromised node in route information updating or on-demand routing in table-powered protocols of routing during route setup process from the source node as the best path.

## II. Literature survey:

During past research work, multiple approaches to defend WSN from black hole attacks are introduced. Karakehayov [18] came across a one of a kind approaches to develop a REWARD (Receive Watch Redirect) routing algorithm for WSN to experience a single or a black hole attack team. REWARD provides a centralized database for the storage of malicious nodes and their positions respectively immediately as the wrongdoing nodes are detected. Tiwari et al.[7] made the paradigm local information-based known through which a local information-based attack can still be detected while sensor nodes are not wary of the global view. To do this, an algorithm was proposed that followed a specification-based principle that takes into account the actions of the nodes and is calculated on the basis of that action. The sensor network uses a tree topology, where the network entirely is separated in clusters and every cluster perceived to be a tree leaf and the cluster head is referred to as the cluster’s parent. The detection of malicious node function in the WSN is assessed [9, 11, 15, 17], depending on the trust of the individual nodes.

The author suggested a method on detection of malicious node when the transmission of a packet from a source node, the radius created between the source and the sink nodes of virtual cylinder is termed as w. Both the cylinders virtual nodes are permitted to transmit packets over the multipath, in case of a corrupted node within a virtual cylinder it is transmitted to the sink via a virtual cylinder [1]. In case of black hole attacks [2], some base stations using a genetic algorithm with optimized position have proposed efficient packet distribution. "Improvised hierarchical intrusion-efficient vitality system" defends the sensor fields against attacks by black hole. It focuses on the forwarding of control packets between the sensor node in the base station. Easy station serves as a control node for detecting any malicious node protecting nodes from black hole attack. Sensor nodes with the cluster head may be imagined as black hole nodes, and an effective method may be formulated [3]. The emphasis in this transcript has been on Black Hole Attack for detecting and preventing in cluster-based WSNs. With two cluster heads Clustering based network is used to identify black hole in each cluster and prevent it. "Improvised hierarchical intrusion-efficient vitality system" defends the sensor fields against black hole attacks [11]. Forwarding of control packets between the sensor node in the base station is focused on. Simple station serves as a control node for detecting any malicious node that defends nodes against black hole attack. You can picture sensor nodes with the cluster head as black hole nodes, and an effective approach can be devised [3]. The emphasis in this research has been on detecting and preventing Black Hole Attack in cluster-based WSNs. With two cluster heads the clustering-based network used in every cluster to identify and avoid black hole. The network would then be under attack in case the node selection is not as per CH > max. Various topologies, various protocols, and similar stimulation protocols can be used to expand this work [5].

## III. Proposed Work:

We will discuss the suggested approach and how it operates in the following session,

### *A.* Node discovery and Trust Initialization

In the Lifetime system the node discovery process is performed by sending hello packets after a short interim period. A sensor node talks about Hello packets for finding neighbours. Neighboring hubs will pick a node 's reliability from which they will accept packets of hello when collecting packets of hello. Suppose the node is sent by bundles of hi I consider its neighbors. A j node supports node I reliability when it comes to receiving hello packets [12]. For I, a neighboring node is enforced by a proportion ascertaining the amount of j that is the hello packets node received from I node against the sent hello parcel numbers. In the case following, investigate with the help of node j, The location of node I in the up and up list, the off chance that node I will be on the up and up list, The trust at this stage will be undermined by an opportunity indicated by any steady factor as "down" and the down estimate will be set to "0.3." If that node I'm absent from the insider savvy list, encouraging some steady item to say "up" would increase their faith. Bring the neighbor into the neighboring rundown and thus upgrade an opportunity node I to the comparable trust and store it in a trust table.

On the off chance that a hub is available on the up and up list, at that point
new trust = down * trust ;/down = const esteem else
new trust = up * trust ;/up =const worth Update trust an incentive for neighboring hubs.

### B. Nodes selection and Revocation

At this point, the troublesome node is boycotted and a trustworthy communication node is chosen. While j i.e. the neighboring node accepts packets from I node state, it will evaluate its reliability. In order to measure this, a ratio called the conveyance ratio is determined immediately for a neighboring node off the bat as the ratio of information packet numbers received from node I to the sum of information packets sent. At the same time, I get an old node-trust component. In the event that the node I delivery ratio is found not exactly old node I trust calculation at this point declines the confidence a node I incentive by any stable indicated factor as "down," and this estimate is "0.3" and does not accept the demand of the course from node I, expect to say, expel a node from a round [11]. At the off chance that confidence value is discovered more prevalent than its conveyance ratio, at this stage its confidence is strengthened by an opportunity to say "up" by some steady factor and its value is set to "0.5." Finally update an opportunity for node I to the relevant trust.

i. A node that gets course demands neighboring node packets, gets the delivery ratio (DR I) and I trust neighboring nodes. If that (DR I trust I) is the case then
new trust = down * trust I + DR I; else
new trust = up * trust I + DR I;

Often, get the appreciation of vitality for a neighbor node and check how much vitality it has spent before further procedures. Confirmation should be done for all esteems of vitality and trust.

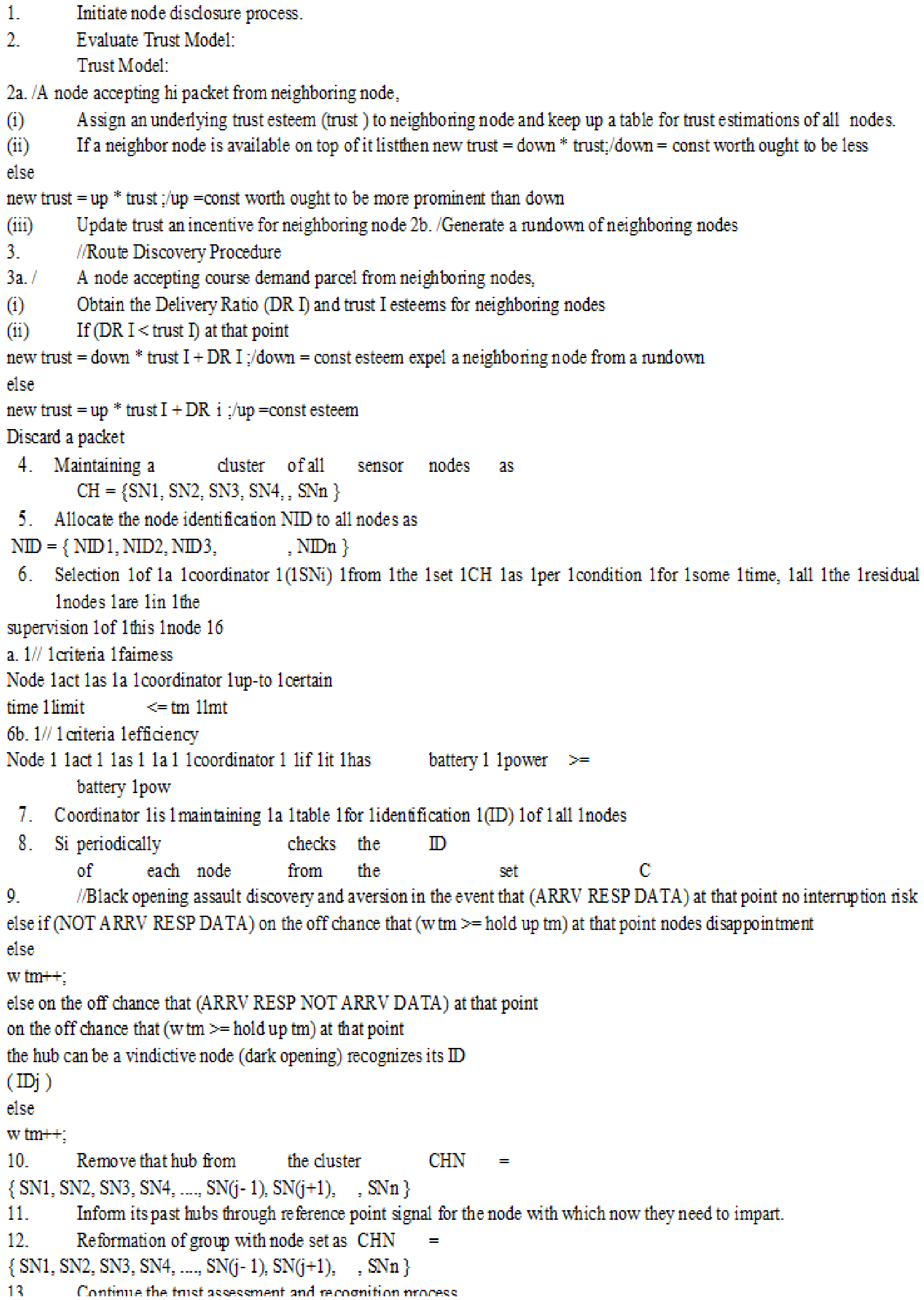
ii. In case of vitality and trust esteems exceeding past preordained limits of confidence and edge of vitality, a packet will be available at that level.

## Routing Procedure

EDPMBA runs periodic patterned system. The process length defines how much data is being shared and modified in time direction. Node discovery process begins after an appropriate interval that produces the list of nodes that are neighboring. Cluster is established amongst the neighboring collections. CH and CO are chosen to play a crucial role in the packet transfer process and overall communication [12]. A path to the destination node must be identified, to which a data packet must be communicated or sent before the start of a node with the forwarding phase of the actual data packet. Therefore, a route discovery process is initiated by sending packets for path requests. A major role is played by the trust metric in setting up a safe path.

## Algorithm 1: Algorithm for Enhanced Detection and Prevention Mechanism for Black hole Attack (EDPMBA) Trust Model

ISSN: 2233-7857 IJFGCN



```
1.        Initiate node disclosure process.
2.        Evaluate Trust Model:
          Trust Model:
2a. /A node accepting hi packet from neighboring node,
(i)       Assign an underlying trust esteem (trust ) to neighboring node and keep up a table for trust estimations of all  nodes.
(ii)      If a neighbor node is available on top of it listthen new trust = down * trust;/down = const worth ought to be less
else
new trust = up * trust ;/up =const worth ought to be more prominent than down
(iii)     Update trust an incentive for neighboring node 2b. /Generate a rundown of neighboring nodes
3.        //Route Discovery Procedure
3a. /     A node accepting course demand parcel from neighboring nodes,
(i)       Obtain the Delivery Ratio (DR I) and trust I esteems for neighboring nodes
(ii)      If (DR I < trust I) at that point
new trust = down * trust I + DR I ;/down = const esteem expel a neighboring node from a rundown
else
new trust = up * trust I + DR i ;/up =const esteem
Discard a packet
  4.  Maintaining a          cluster    of all     sensor    nodes     as
          CH = {SN1, SN2, SN3, SN4, , SNn }
  5.  Allocate the node identification NID to all nodes as
 NID = { NID1, NID2, NID3,              , NIDn }
  6.  Selection 1of 1a 1coordinator 1(1SNi) 1from 1the 1set 1CH 1as 1per 1condition 1for 1some 1time, 1all 1the 1residual
      1nodes 1are 1in 1the
supervision 1of 1this 1node 16
a. 1// 1criteria 1fairness
Node 1act 1as 1a 1coordinator 1up-to 1certain
time 1limit          <= tm 1lmt
6b. 1// 1criteria 1efficiency
Node 1 1act 1 1as 1 1a 1 1coordinator 1 1if 1it 1has          battery 1 1power    >=
          battery 1pow
  7.  Coordinator 1is 1maintaining 1a 1table 1for 1identification 1(ID) 1of 1all 1nodes
  8.  Si periodically                  checks    the       ID
          of        each   node        from      the                set                  C
9.        //Black opening assault discovery and aversion in the event that (ARRV RESP DATA) at that point no interruption risk
else if (NOT ARRV RESP DATA) on the off chance that (w tm >= hold up tm) at that point nodes disappointment
else
w tm++;
else on the off chance that (ARRV RESP NOT ARRV DATA) at that point
on the off chance that (w tm >= hold up tm) at that point
the hub can be a vindictive node (dark opening) recognizes its ID
( IDj )
else
w tm++;
10.       Remove that hub from        the cluster          CHN      =
{ SN1, SN2, SN3, SN4, ...., SN(j- 1), SN(j+1),    , SNn }
11.       Inform its past hubs through reference point signal for the node with which now they need to impart.
12.       Reformation of group with node set as  CHN      =
{ SN1, SN2, SN3, SN4, ...., SN(j- 1), SN(j+1),    , SNn }
13        Continue the trust assessment and recognition process
```

## IV. Performance Evaluation

The success of the suggested protocol is calculated with parameters such as 'Average Energy' 'End-to-End Delay', 'Jitter', 'Packet Delivery Ratio,' 'Throughput' vs 'Interval' in both environments as with and without an attack. The simulation results in the presence of attacks shown in Figure 1 to 5 mean that, with the increasing interval, PDR continues to increase, while the throughput decreases by a small amount, the average energy consumed by nodes decreases at interval 0.07 and then increases marginally and remains nearly constant until interval 0.1. Delay and Jitter increase or decrease by a small factor that does not show a significant difference and can be assumed because their findings remain consistent. Protocol performs much better, without the involvement of attacks. The protocol achieves better PDR as it decreases the probability of packet collision and flooding the network so that maximum packets are reaching to the destination with the that interval[11].

The plots represent the performance with the number of nodes at a fixed interval, and it is observed that there is no significant difference between performance parameters with the number of nodes increasing and decreasing. Therefore, it can be argued that the current protocol fits best with network scalability.

In Figures, a comparison of the current protocol (DPMBA) and proposed protocol (EDPMBA) is presented. The proposed protocol provides better PDR, throughput, and end-to - end delay performance. Since the current system uses waiting time mechanisms that can cause further delay and latency in packet transmission, while the confidence model in the proposed system eliminates this delay by separating earlier misbehaving nodes. The proposed protocol needs a little more energy than the current protocol as it overcomes some of the current system's limitations as node mobility, detects single and cooperative attacks and it maintains neighborhood trustworthiness, and therefore is considered to be acceptable[12].

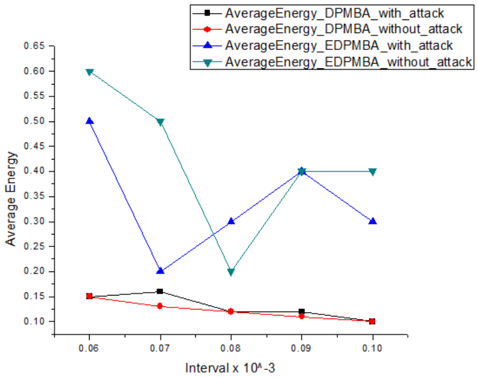


**Fig. 1:** Intervals Vs Average Energy with and without attack DPMBA and EDPMBA

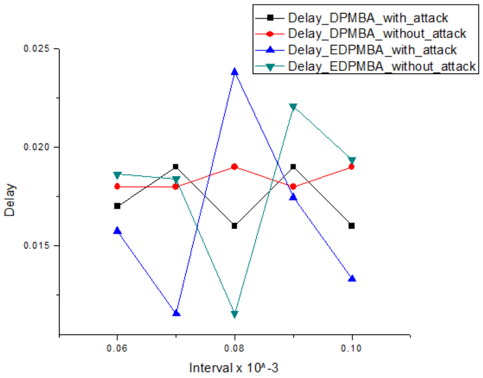


**Fig. 2:** Intervals Vs Delay with and without attack DPMBA and EDPMBA

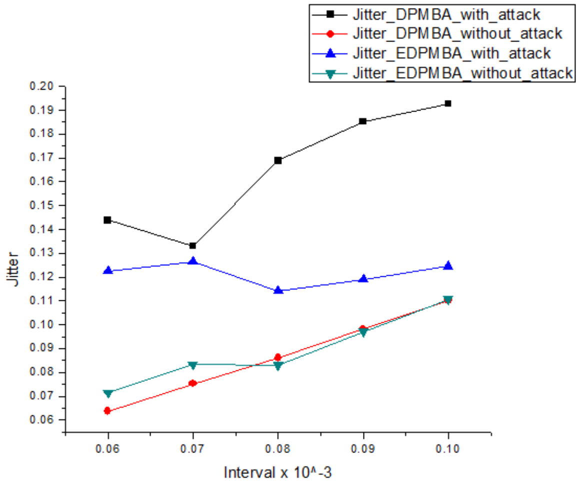


**Fig. 3:** Intervals Vs Jitter with and without attack DPMBA and EDPMBA

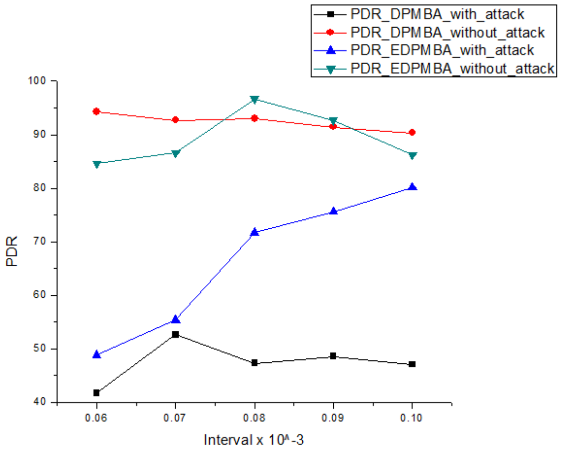


**Fig. 4:** Intervals Vs PDR with and without attack DPMBA and EDPMBA

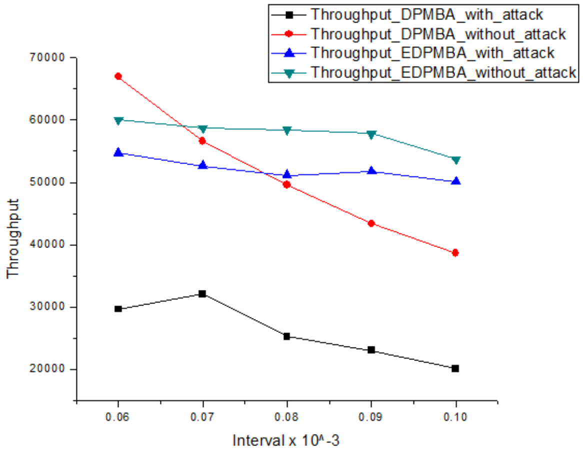


**Fig. 5:** Intervals Vs Throughput with and without Attack DPMBA and EDPMBA

## V. Conclusion:

The proposed algorithm detects black hole attacks in the wireless sensor network, based on the parameters such as time delay, reliability and bandwidth. The DSR protocol of routing is used for forwarding efficiently the packets, that has increased network life to the maximum. The algorithm proposed differently uses metrics to identify malicious aim node. Misbehaving nodes also called the potential malicious node are checked for their behavior by sending dummy packets. Packets must be dropped by the malicious node, so they can be identified easily. Each Node 's state is shared with the rest of the node. Improves the standard of network security. The proposed trust model documented an efficient and safe method for detecting black hole attacks and provided a routing route protected from the sensor node to the base station. Tests analysis was carried out and the proposed algorithm recognizes the black-hole attack and provides protection for the network was proven.

## 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. Atul B Kathole, Dr.Dinesh N.Chaudhari, “Pros & Cons of Machine learning and Security Methods ”, 2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588 ,Volume 21 Issue 4
12. Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, “ Machine Learning & its Classification Techniques ”,International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.
13. 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
14. Security Issues of Black hole attacks in MANET”,Rakesh Ranjan, Nirnemesh Kumar Singh, Ajay singh, “, IEEE-2015
15. 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)'.
16. 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).