A Two level Detection of Routing layer attacks in Hierarchical Wireless Sensor Networks using learning based energy prediction

Jeevaa Katiravan[1], Duraipandian N [2] and Dharini N[3]
[1]Associate Professor,Department of Information Technology,Velammal Engineering College
Chennai, India
[2]Professor, Department of Computer Science,Velammal Engineering College
Chennai, India
[3]PG Scholar,Velammal Engineering College
Chennai, India
[e-mail:dharini1990@gmail.com]
*Corresponding author: Dharini N

Received June 25, 2015; revised August 29, 2015; accepted September 20, 2015; published November 30, 2015

Abstract

Wireless sensor networks are often organized in the form of clusters leading to the new framework of WSN called cluster or hierarchical WSN where each cluster head is responsible for its own cluster and its members. These hierarchical WSN are prone to various routing layer attacks such as Black hole, Gray hole, Sybil, Wormhole, Flooding etc. These routing layer attacks try to spoof, falsify or drop the packets during the packet routing process. They may even flood the network with unwanted data packets. If one cluster head is captured and made malicious, the entire cluster member nodes beneath the cluster get affected. On the other hand if the cluster member nodes are malicious, due to the broadcast wireless communication between all the source nodes it can disrupt the entire cluster functions. Thereby a scheme which can detect both the malicious cluster member and cluster head is the current need. Abnormal energy consumption of nodes is used to identify the malicious activity. To serve this purpose a learning based energy prediction algorithm is proposed. Thus a two level energy prediction based intrusion detection scheme to detect the malicious cluster head and cluster member is proposed and simulations were carried out using NS2-Mannasim framework. Simulation results achieved good detection ratio and less false positive.

Keywords: Routing layer attacks, Hierarchical routing, Cluster head, Cluster member, IDS

1. Introduction

Wireless Sensor Network(WSN) is the collection of sensor nodes deployed in a large to monitor the environment. These networks find application in various fields such as environmental monitoring, defence and military applications. WSN. Thus they are deployed in mission critical and application specific areas where security of the data is vital. But due to broadcast wireless communication nature of the sensor nodes they are prone to various attacks.

In fact, security in WSN features a large range of challenges which will not be seen in different kinds of wireless networks [1]. For example several kinds of wireless networks are attacked severely by Denial of Service (DoS) attack which disables the legitimate nodes to access the network resources. One such kind of network called Cognitive radio is an opportunistic communication technology designed to help unlicensed users utilize the maximum available licensed bandwidth in which a selfish cognitive radio node can occupy all or part of the resources of multiple channels, prohibiting other cognitive radio nodes from accessing these resources. An easy and efficient selfish cognitive radio attack detection technique, called COOPON, with multichannel resources by cooperative neighboring cognitive radio nodes was proposed in [2]. In contrast to various works like [2] energy constraint issues need to met in the proposed future works.

1.1 Hierarchical WSN

A hierarchical approach of WSN breaks the network into clustered layers. Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads.

1.2 Motivation

These hierarchical routing protocols were very simple and designed to attain energy efficiency thus not developed with security in mind, so the adversary can launch various attacks in the network.Cluster heads, which are elected to manage local clusters, are adversaries' ideal targets. If one cluster head is captured or compromised by adversaries, an entire local cluster will be affected by routing layer attacks. This highlights the fact that cluster-based or heirarchical WSNs require an efficient Intrusion Detection Scheme (IDS) to detect these routing layer attacks. There is no IDS which can detect Multiple attacks with same metric in the state of art, but the proposed system fulfills the same proving its novelty.

Among the various DoS attacks, routing layer attacks are hard to defend as they come along easily during the traversing of the packet between the source and destination. Strong encryption authentication and cryptographic techniques are to be place to prevent these attacks. But there are many cases in which nodes may be compromised by the adversaries. In such situations a second line of defense called Intrusion Detection Schemes (IDS) are needed to locate these malicious nodes. Monitoring behaviours of sensor nodes consumes energy resources, thus they are not suitable for resource-constrained WSNs [3, 4]. Furthermore, the packet forwarding in WSNs is unstable and packet loss is likely to occur during transmission

process. Therefore IDSs based on monitoring the behaviours of sensor nodes cannot detect routing layer attacks efficiently.

2. Security attacks and threats in WSN

Security attacks against WSNs are classified into two: Active and Passive. In passive attacks, assailants are normally disguised (covered up) and either tap the correspondence connection to gather information; or devastate the working components of the system. Active attacks can be grouped into Denial-of-Service (DoS) [5] is any event that diminishes or eliminates a network's capacity to perform its expected function, jamming, hole attacks (blackhole, wormhole, sinkhole, etc.), flooding and Sybil types. The above mentioned DoS attacks affects the routing of packets thus they are named also as routing layer attacks.

2.1. Routing layer attacks

- In Gray hole attack or Selective Forward as shown in **Fig. 1**, malicious node refuses to forward sensitive messages or just drops the messages making certain that they're not propagated any more. The malicious node drops all the packets which it received from sensor node B in the below figure thus leading to selective forward or grayhole attack.

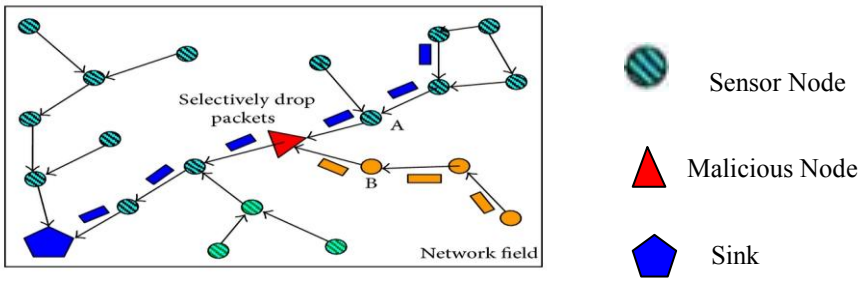

Fig. 1. Grayhole attack

- In a flood attack as shown in **Fig. 2**, malicious node broadcasts large quantities of useless packets to neighbor nodes in its communication range. The common characteristic of flood attack is to exhaust the available network communication bandwidth. The flooding attacker node present externally ruins the sensor node within network by large number of hello messages in figure shown below.

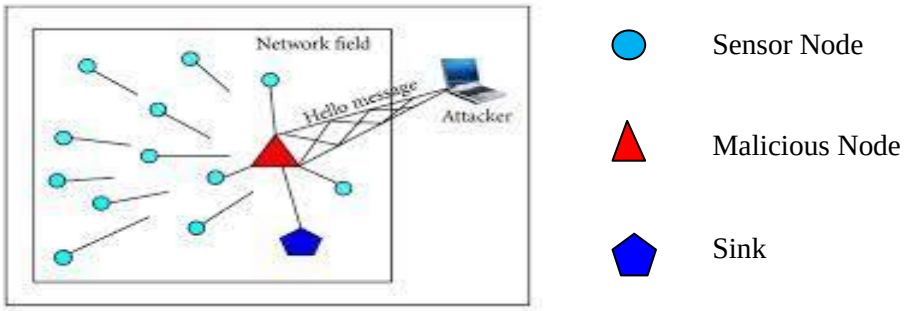

Fig. 2. Flooding attack

- In a sinkhole or blackhole attack as shown in **Fig. 3**, malicious node typically works by misleading itself look especially attractive to surrounding nodes. For example, malicious nodes pretend to have the shortest paths to the base station. Therefore they can trick other nodes into forwarding messages to them. By tricking the neighbor nodes with route information the malicious blackhole attacker ▲ in figure shown below drops the packets which it receives from sensor node A and B

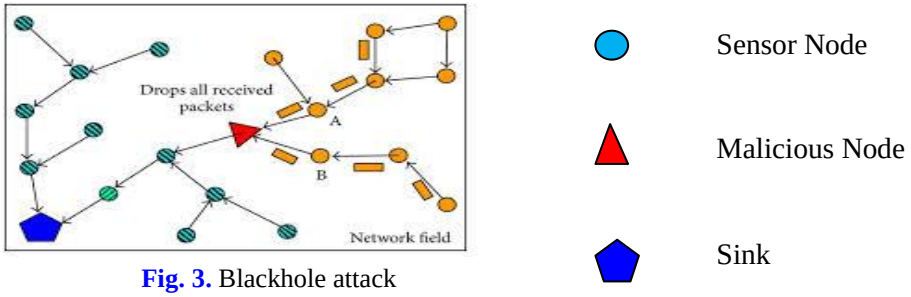

Fig. 3. Blackhole attack

3. Contributions

- Comparative performance analysis of various types of routing layer attacks.
- A two level IDS approach is implemented where sink nodes monitor the cluster heads and cluster heads monitor the cluster members for their malicious activity.
- Learning based energy prediction algorithm is proposed, which is used to identify the abnormality in the energy consumption of attacker nodes.
- Malicious nodes are detected in the network.

4. Related Works

IDS mechanisms and techniques makes use of different underlying principles. Most of those principles are based on the assumption that there exists a noticeable difference between the behavior of an attacker and the behavior of a legitimate node, such that the IDS can match those preprogrammed or learned rules. Following this assumption, it is clear that IDSs can be classified according to the specific detection technique used for studying the audit data. Therefore, we can classify IDSs into three groups: (a) misuse, (b) anomaly, and (c) specification based. The misuse detection systems are used to detect known patterns of intrusions while anomaly detection techniques are used to detect new or unknown intrusions. Specification-based detection is based on some deviations from normal behaviors.

Many schemes have been proposed to defend malicious attacks, for example, trust management and encryption key schemes. A technique known as spontaneous watchdogs in the paper [6] adopts both local and global agents to watch over communications. Global agents are activated in every cluster. Global agents with spontaneous watchdogs can receive both normal and relayed packets. If malicious nodes alter or selectively forward packets, the global agents can easily detect those using spontaneous watchdogs. The problem with this approach is that not all packets can be overheard by a global agent, due to the randomness of the selection process. Another drawback of the work is that it does not deal with the collision of packets, which is high likely due to the high density of nodes in various wireless sensor

networks applications.

The work [7], analyzed the performance of LEACH with Gray hole attack. LEACH [12] is hierarchical routing protocol with dynamic cluster head selection. This work analyzed the performance of LEACH under Gray hole attack based on throughput, delay and packet delivery ratio. This work does not address about the energy consumption of the network under attacks.

The main idea of IDSEP [8] is to detect malicious nodes based on energy consumption of sensor nodes. Based on abnormal energy consumption malicious cluster heads are detected with Markov chain based prediction algorithm. Drawback of this approach is that it can only detect malicious cluster heads and sink is overloaded and a highly computationally complex algorithm is used.

An ant colony based routing decision is obtained based on the energy prediction algorithm in [9]. In this paper the packet forwarding nodes are selected based on its residual energy prediction. This work does not consider the security aspect of the network.

Cluster-based mechanism for multiple spoofing attackers in WSN [10] used spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as same node identity; and localizing multiple adversaries. Support vector machines were used to further improve the accuracy of determining the number of attackers. Metrics such as special information need to be obtained from the neighbors which in turn needs correlation among the neighbours, thus consuming more energy.

In work [11] black hole and selective forward attacks are detected by means of local information obtained from neighbors. Neighborhood nodes does not have a global view of the network, which is vital for intrusion detection design

Energy consumption is very high in state of art IDS. Thus, it is critical to develop effective IDS to defend DoS attacks. All these IDSs are carried out by observing or monitoring sensor nodes. Observing the network characteristics and node's behavior consume lot of energy thus they are not suitable for resource-constrained WSNs. Furthermore, the packet forwarding in WSNs is unstable and packet loss is likely to occur during transmission process. Therefore intrusion detection based on monitoring the behaviors of sensor nodes cannot detect DoS attacks efficiently

5. Proposed System

5.1 Implementation of Routing layer attacks

In order to analyze the severity of attacks, Gray hole, Black hole and Flooding attacks are implemented using the algorithms given below. Three types of attack were implemented in the AODV routing protocol. So in order to model these attacks as a preliminary study let us see the short description of the working principle of AODV routing protocol.

5.1.1 AODV Routing Protocol

The Ad hoc On Demand Distance Vector (AODV) [16] routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the

source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery

5.1.2 Modeling of Attacks

Let GN be the malicious node, $N_i \ldots N_n$ be the number of source nodes, N_{ie} be the residual energy of source nodes and CH be the cluster head. Usually the nodes having maximum residual energy are chosen as cluster head. A Simple sensor node works according to the AODV routing protocol.
The nodes launching Flooding attack unwantedly flood the network with large number of route request (RREQ)packets.
The nodes launching Blackhole attack works as follows

- Send fake route reply packets with large sequence numbers
- Disable the route error messages regarding the fake packets to the neighbor nodes
- Neighbor nodes gets falsified route information and thus they forward their packets
- Malicious nodes receives the packets and drops the packets

The nodes launching Grayhole or Selective Forward attack is a kind of Black hole except that the malicious nodes drops the packets either only for a particular interval of time or from a particular source node.

Algorithm

Implementation of Attacks

Let GN be the malicious node
Let $N_i, \ldots N_n$ be the number of source nodes Let
N_{ie} be the residual energy of source nodes Let

```
CH be the cluster head
CH()
{
If(N_ie is the highest among all other N_i-1)
Elect N_i as CH();
Else
N_i is simpleSensorNode();
}
N_i()
{
sendRouteRequest();
recv RouteReply();
forwardPacketToNeighbor();
}
GN()
{
switch(Case)
 Case 1: Flooding
{
sendLargeNumberOfFakeRouteRequest();}
 Case 2: Blackhole
{
sendfakeRouteReply ();
disableRouteError();
recvPackets();
dropPackets();
}
Case 3: Grayhole
{
sendfakeRouteReply ();
disableRouteError();
recvPackets();
dropPackets for an interval T_b ();
}
}
```

Flooding attacker node exhausts the network resources in terms of bandwidth and energy. Grayhole attacker node intentionally drops packets thereby leading to misinterpretation sensing data. The energy consumption of attack varies based on the nature of attack, thus among the three, flooding and grayhole attack consumes the maximum and minimum energy of the sensing element. Gray hole attack may even go unnoticed since it consumes less energy than the legitimate nodes. Thus the attacker can be distinguished in terms of energy. Upon studying the nature of working of routing layer attacks we implemented distributed IDS scheme.

Existing IDS either depend sink nodes or cluster heads to perform the intrusion detection process. If sink node alone act as intrusion detection agent it can only detect the malicious cluster heads, where in the sink node may be compromised and may even fail. More over malicious nodes are detected only after gaining the responsibility of the cluster head which

becomes the scenario worse. On the other hand if cluster heads alone act as intrusion detection agent, what if the cluster head becomes malicious. So both cluster member and cluster head malicious behavior need to be monitored simultaneously. Thus a two level detection is necessary in case of hierarchical wireless sensor network to provide enhanced form of security, in a way even if anyone level fails(cluster head or sink) another takes over role of intrusion detection agent. The two level intrusion detection architecture is shown below in **Fig. 4**.

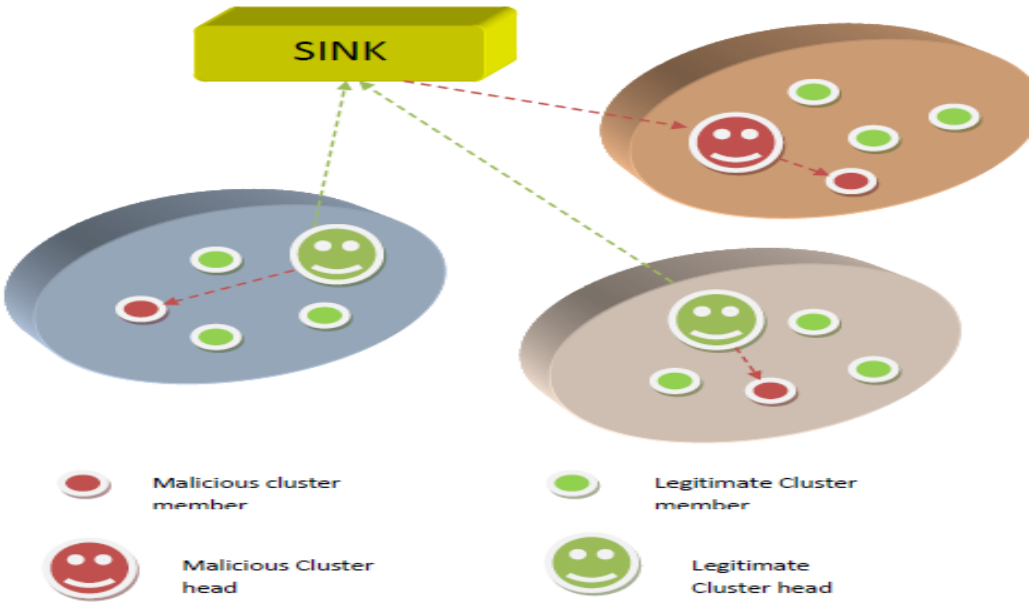

Fig. 4. Proposed IDS architecture

Malicious nodes are detected in a distributed fashion by the cluster head thus distributing the computational complexity of detection among various cluster heads. Simultaneously sink node will also look for the malicious activity of cluster heads, whenever a new cluster head gets selected. Energy prediction for all the nodes is done by the respective cluster head and sink nodes and the actual energy consumption is obtained from all the nodes. Thus a comparison is made between the two. Abnormality between the predicted and actual energy results in an attack.

5.2 Assumptions

- Homogeneous wireless sensor network is established, so all the nodes will have the same transmit receive and idle power.
- Sensor nodes are compromised externally from the network. So initially all the nodes are legitimate.

5.3 Learning based energy prediction algorithm

All nodes are programmed to send their residual energy after a particular interval of time (say 50s) to their cluster heads. Upon receiving the residual energy the actual energy consumed is calculated as follows in (1).

$$Actual\ energy\ (E_1(v)) = Initial\ energy - Residual\ energy \quad (1)$$

where $E_1(v)$ is the energy consumed by the node in the first interval

$$E_0(v) = 0 \quad (2)$$

where $E_0(v)$ in eqn (2) is the energy consumed by the node during the initial formation of the network. By the time the network gets formed all the nodes are idle and they will not consume any energy. So the energy consumed here is assumed to be zero.

$$E_K(v) = e_k \quad (3)$$

where e_k is the energy realistically consumed by the node *v during* $T_{k-1,k}$ as shown in (3) . e_k is the energy, the cluster heads obtain from all nodes at the end of kth interval(say 100s). Upon having E_0 and E_k, where k=1, 2, 3..; the predicted energy consumption is calculated as follows in (4)

$$Predicted\ Energy\ (E_{k+1}(v)) = e_k + \emptyset\ (E_k(v) - E_{k-1}(v) \quad (4)$$

Ø is a parameter used to balance "past" and "current" energy consumption included in the prediction energy consumption. In other words, if we emphasize "past", i.e., we need E_k (*v*) to reflect more past energy consumption than current energy consumption at node *v*, we should choose a small value of Ø. Conversely, if we place emphasis on"current", i.e., need *E* (*v*) *k* to reflect more current energy consumption than past energy consumption, we should choose a large value of Ø . Specifically, if we take Ø =1, no past energy consumption contributes to *E*(*v*) *k*. The above process is briefly explained in the form of algorithm below

Learning based energy prediction algorithm

*for(i=1;i<N;i++) /*N=Total number of sensor nodes within the cluster*/*

{

Let k=0, 1, 2, 3... be the time instants;

Let $E_{k(i)}$ *be the energy consumed at time instant 'k' by node i;*

Let $E_{0(i)} = 0$*;*

$E_{k(i)} = e_{k(i)}$ *;*

Predicted Energy($Ep_{k+1(i)}$*)=*$E_{k(i)} + \emptyset\ (E_{k(i)} - E_{k-1(i)})$*;*

}

Usually learning based prediction is accompanied by prediction error. Weight factors are to be adjusted accordingly to reduce the error between desired and predicted output. Simulations are carried out to adjust the weight factor under various scenarios and tabulated in simulated results section.

5.4 Detection of malicious nodes

Every time a new cluster head gets selected the old cluster head will share its routing table to the newly elected cluster head. Initial energy E_{i1} of the cluster members are known to the corresponding cluster heads. At the end of first interval(0-50s) sensor nodes will send a packet

indicating their residual energy E_{r1}, upon which the actual energy consumption is calculated $E_{c1} = E_{i1} - E_{r1.}$ Based on the proposed energy prediction algorithm, the cluster head node can predict sensor nodes' energy consumption for the second interval(50-100s), denoted as E_{p1}. The cluster head node uses the residual energy $E_{r(i)}$ to predict energy consumption for the further intervals denoted as $E_{p(i)}$. After receiving the residual energy $E'_{r(i)}$ from all sensor nodes for the consecutive intervals, the actual energy consumption is $E_{c(i)} = E_{r(i)} - E'_{r(i)}$.If there is a mismatch between $E_{p(i)}$ and $E_{c(i)}$ then the node is regarded as a malicious node and the type of malicious activity is differentiated as follows.

When this scheme detects abnormal energy consumption of a sensor node, the cluster head node identifies the node id launching the attack and isolates it from the network.

The same process is carried out by sink node to identify the malicious cluster heads. The above energy comparison is made among the cluster head. If any cluster head is found with abnormal energy consumption it is marked as an attacker node and isolated from the network.

The flooding attacker node maximizes its broadcast range. Therefore energy consumption is significantly high. Thus the nodes consuming the highest energy are detected as malicious nodes launching a flood attack and the nodes consuming the lowest energy are detected as malicious nodes launching gray hole attack.

If $E_{c(i)} > E_{p(i)}$+average(prediction error), then sensor node i is regarded as a malicious one launching a flooding attack. In a flood attack, node sends as many packets as possible with abnormally high transmission energy to all the nodes.

If $E_{c(i)}<E_{p(i)}$+average(prediction error),then sensor node i is regarded as a malicious one launching a gray hole attack. In gray hole attack, the attacker node selectively drops certain number of packets, so its transmission becomes less. Hence it will consume less energy than the normal node.

The fore mentioned process is depicted in **Fig. 5**. The energy comparison between the predicted and the actual energy consumption is the key to detect malicious nodes.

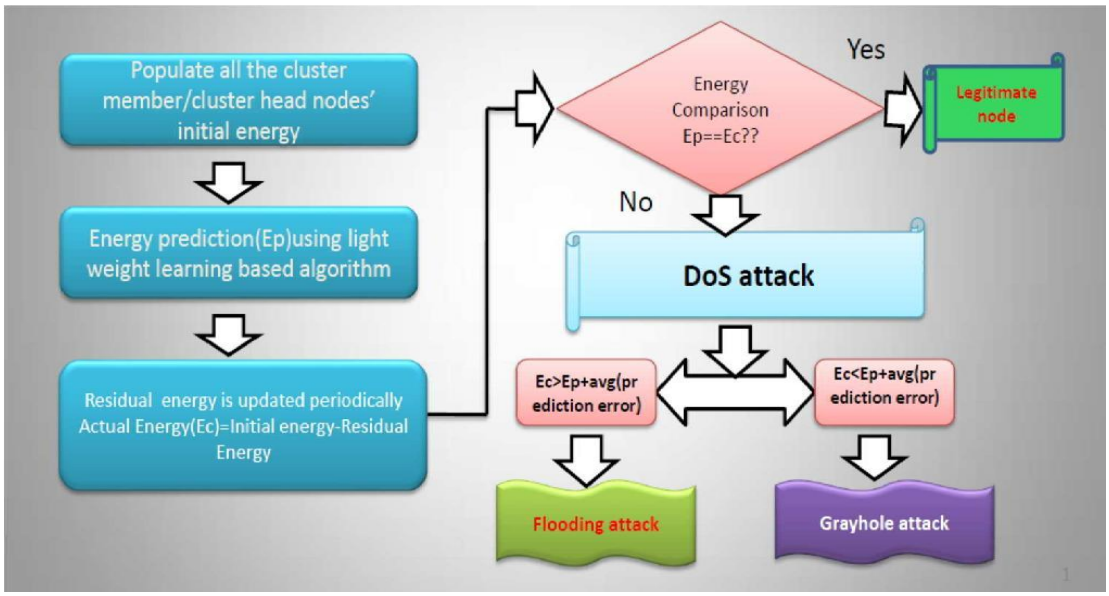

Fig. 5. Intrusion detection process

5.5 Advantages

- More number of malicious nodes can be detected simultaneously-Detection ratio is high.
- Network's lifetime is increased.
- Faster intrusion detection because of distributed detection architecture.
- Computation complexity is less due to the learning based energy prediction algorithm. Early detection of attacker nodes.

6. Simulation Results

Network Simulator-2 [13] with MANNASIM framework [14] is used to evaluate the performance of the 3 types of denial of service attacks. MANNASIM is a framework with script generator tool having the front GUI to configure the wireless sensor network characteristics. Using MANNASIM, the real sensor mica2 motes[15] characteristics can be simulated. The simulation parameters are given in **Table 1**.

Table 1. Simulation Parameters

Parameters	*Values*
No.of nodes	*50*
No.of sink	*1*
No.of cluster heads	*5*
No of attackers	*9(Each 3)*
Routing protocol	*AODV*
MAC	*MAC/802.11*
Physical layer	*Phy/wirelessphy-mica2*
InitialEnergy(Access point&Sink)	*100J*
Initial Energy(Nodes)	*10J*
Initial Energy(CH)	*50J*
Sensing interval	*5seconds*
Dessiminating interval	*20seconds*
Simulation time	*100 seconds*

6.1. Energy Prediction Results

The accuracy of the detection algorithm lies in the accuracy of the energy prediction. Accurate energy prediction can be achieved by means of finding the exact weight factor. The proposed light weight energy prediction algorithm is implemented in NS-2. Ø (Weight factor) is tuned for various scenarios. Simulations are carried out under different number of nodes with different types of attacks and the average value of the weight factor is found out and shown in **Table 2**.

Table 2. Ø (Weight factor) determination

No. of Nodes	*Ideal scenario*	*Blackhole*	*Grayhole*	*Flooding*
10	*0.7*	*0.6*	*0.68*	*0.9*
20	*0.5*	*0.5*	*0.5*	*0.99*
30	*0.5*	*0.8*	*0.8*	*0.98*
40	*0.8*	*0.8*	*0.8*	*0.95*
50	*0.8*	*0.9*	*0.8*	*0.98*
AVG	*0.66*	*0.72*	*0.73*	*0.96*

Based on the above results the weight factors for various attacks are tabulated and among which flooding attack has the maximum value of 0.96.

Weight factor determines the accuracy of the prediction. By fixing the above values as weight factor for the proposed energy prediction algorithm the prediction accuracy is very high with a minimal error.

The comparison between predicted energy calculated with the above weight factor values and the actual output under flooding, grayhole, black and ideal scenario are shown below in **Fig. 6, 7, 8** and **9**. It is noted that the predicted energy is almost similar to the actual energy consumption of nodes at various time instants thus proving its accuracy.

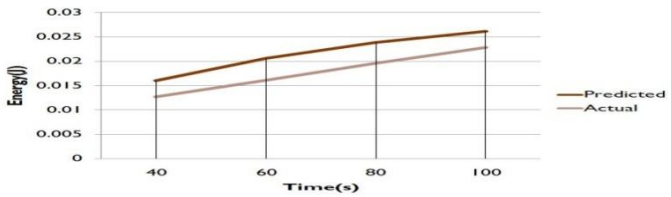

Fig. 6. Comparison between actual and predicted energy consumption under Ideal hierarchical WSN

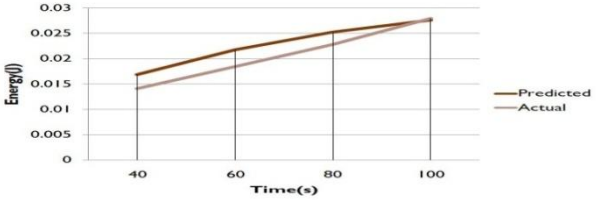

Fig. 7. Comparison between actual and predicted energy consumption under Blackhole attack

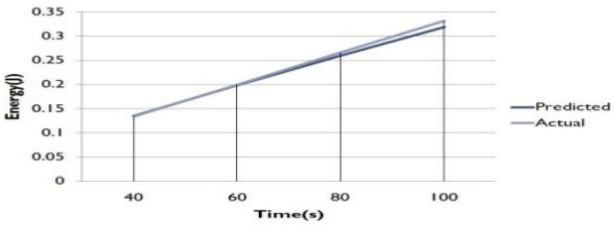

Fig. 8. Comparison between actual and predicted energy consumption under Flooding attack

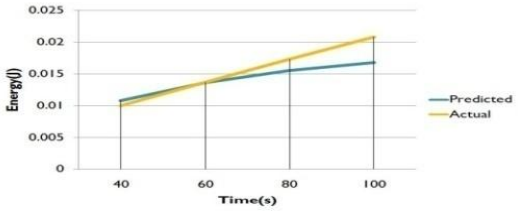

Fig. 9. Comparison of actual and predicted energy under Grayhole attack

6.2 Detection of attacks

Thus by using the proposed system, the flooding attacker nodes and gray hole attacker nodes are detected and is shown in **Fig. 11** and **Fig. 13**. Nodes marked with red circles are malicious nodes. Corresponding terminal outputs are shown in **Fig. 10** and **Fig. 12**.

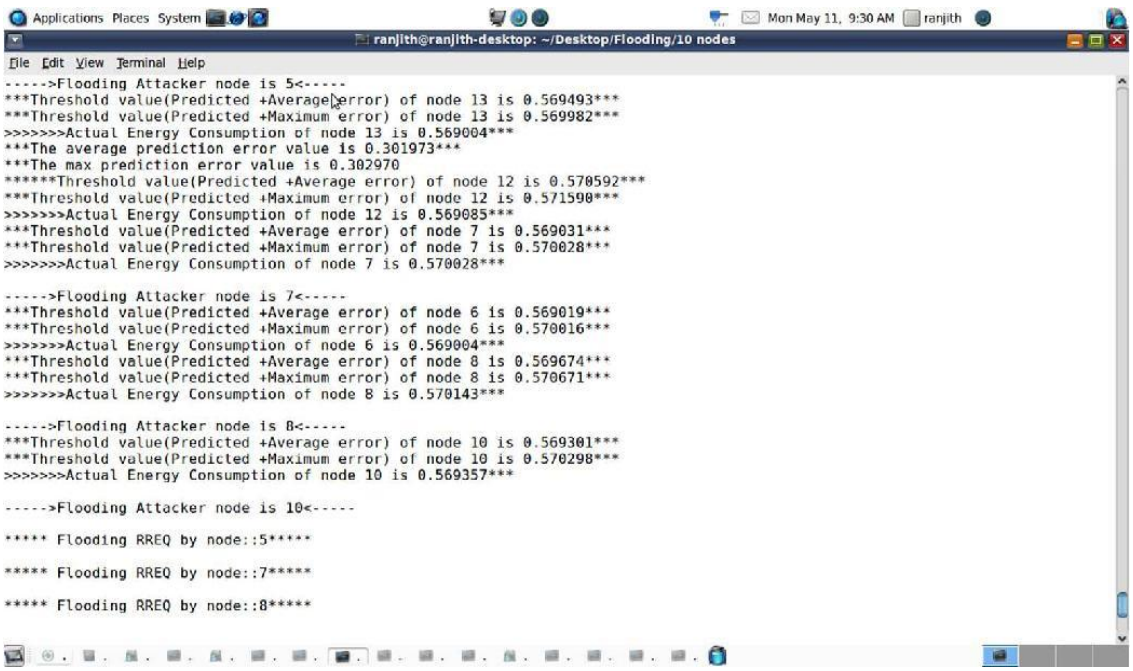

Fig. 10. Detection of flooder node in terminal.

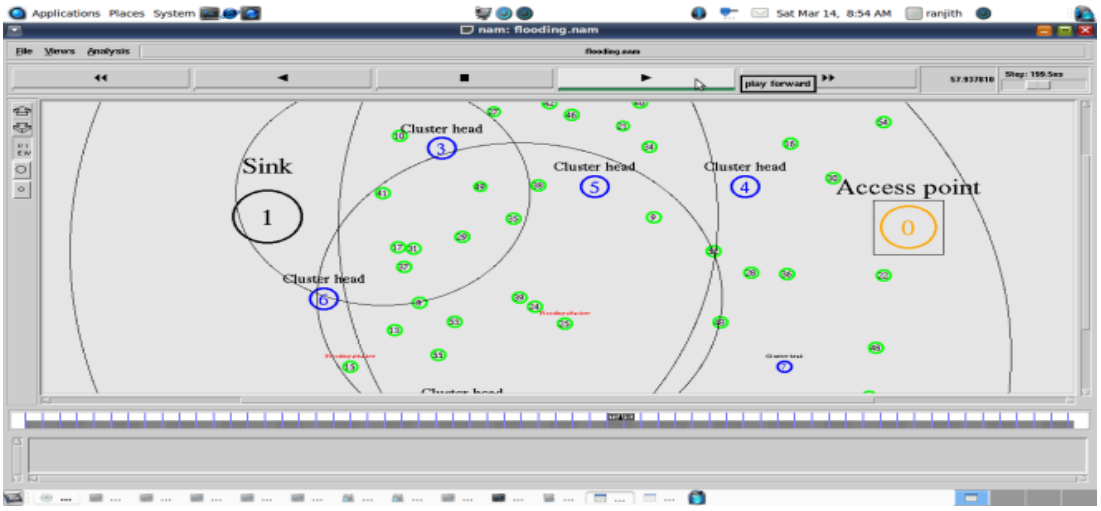

Fig. 11. Detection of Flooding attacker node in Nam window

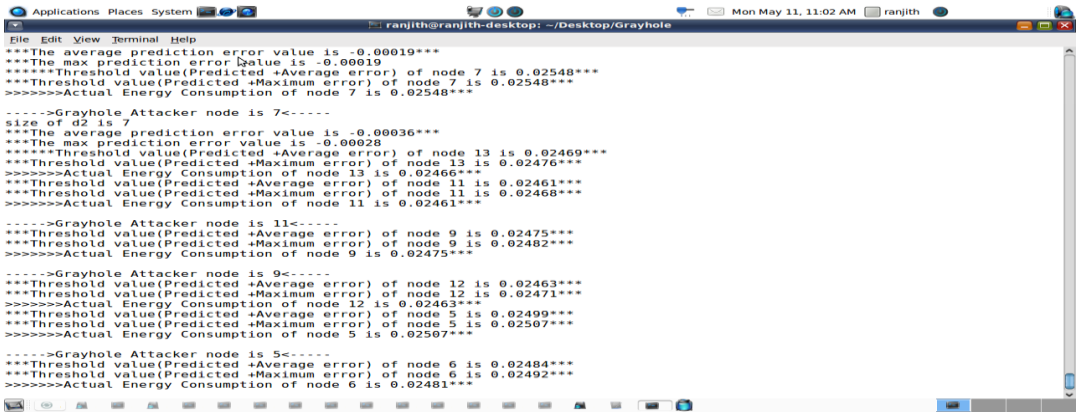

Fig. 12. Detection of Grayhole attacker in terminal

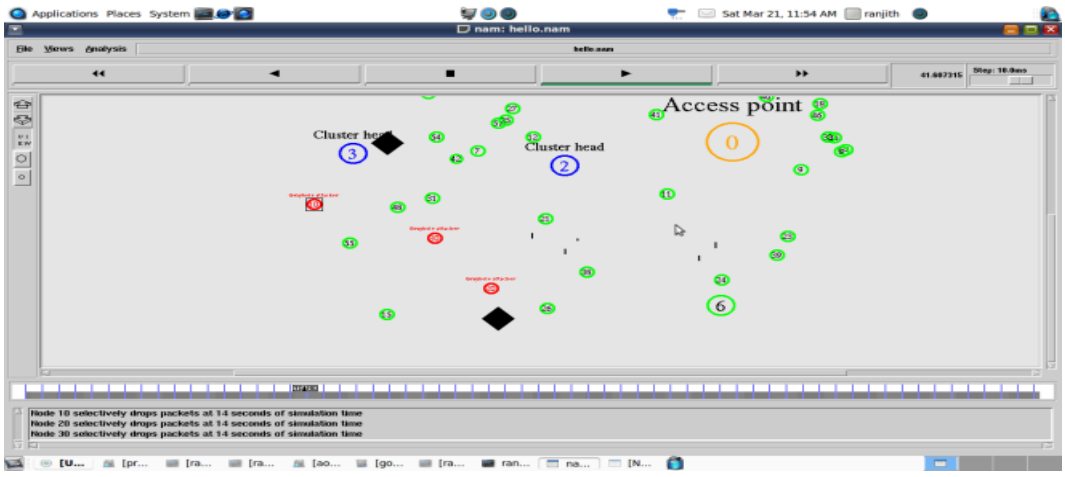

Fig. 13. Detection of Gray hole attacker in Nam window

6.3 Performance analysis of Hierarchical WSN with Flooding, Blackhole, Grayhole, Proposed IDS and without attack

Each of the 3 attack is initiated by 3 malicious nodes in the network. The following network parameters are analyzed using the trace file generated under different attacks generated. Trace file is evaluated using AWK scripts and the corresponding values are plotted.

6.3.1 Throughput: Network throughputs of WSN with and without attacks are shown in the following **Fig. 14**. Network throughput refers to the rate of successful message delivery over a communication channel. It is measured in bits/second. Packets are delivered successfully under Flooding and selective forward attacks because the former only floods unwanted packets thus the meaningful packets are delivered successfully. In the later case only few packets are dropped so throughput is not affected as much as black hole where all the packets were dropped.

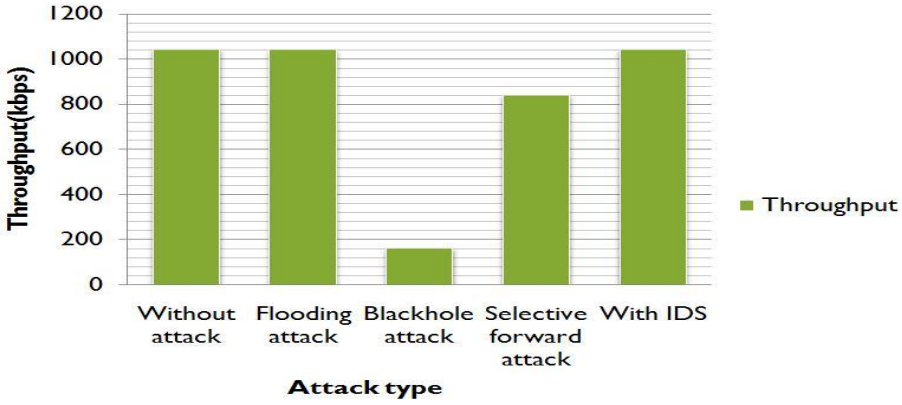

Fig. 14. Comparison of Throughput

6.3.2 Packet delivery ratio (PDR)*:* It is defined as the ratio between number of packets received to the number of packets sent Ideally PDR should be 100%. PDR of various attacks are shown in **Fig. 15**, of which black hole attack's PDR is very less due to large number of intentional packet drop.

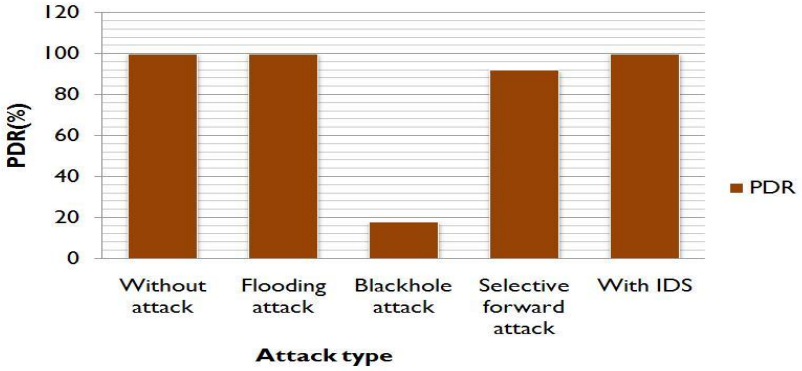

Fig. 15. Comparison of PDR

6.3.3 Energy Consumption: Since the entire sensor nodes are battery operated, they drain off their energy very soon. Thus the energy consumption of nodes due to computation and consumption are to be monitored periodically. The energy consumption of the network under different attacks is given below in **Fig. 16**.

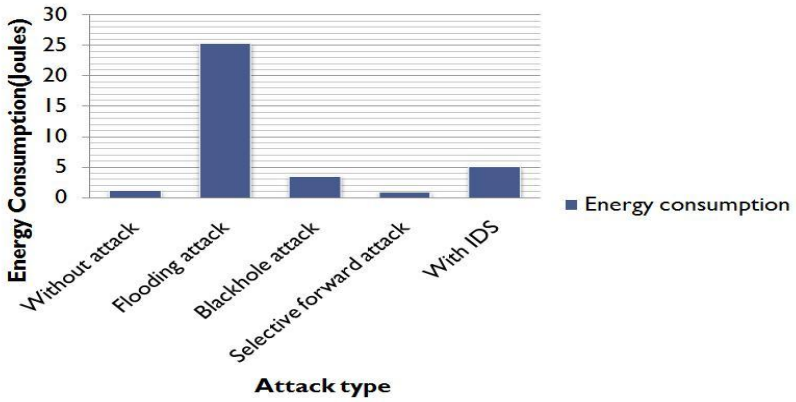

Fig. 16. Comparison of Energy

Thus among the other routing layer attacks, Flooding attack affects the network's lifetime severely. Gray hole attack consumes the minimal amount of energy. The proposed detection mechanism consumes less energy and also there is not much change in the throughput, packet delivery ratio and delay when compared to ideal hierarchical wireless sensor network scenario. Thus the proposed detection mechanism is light weight in nature, hence proving its efficiency.

6.3.4 Detection Ratio and False Positive: Detection ratio is the ratio of number of detected malicious nodes to the total number of malicious nodes in the network. False Positive is used to describe the number of innocent sensor nodes incorrectly identified as malicious nodes. These two parameters are analyzed and shown in **Fig. 17** and **Fig. 18** under flooding and grayhole attack detection scenarios.

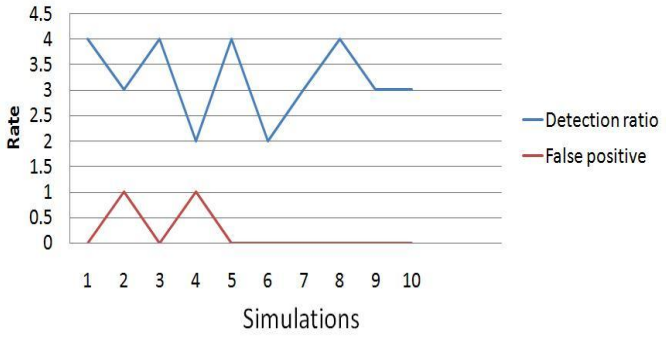

Fig. 17. Detection ratio and false positive under flooding attack detection (with 5 malicious nodes)

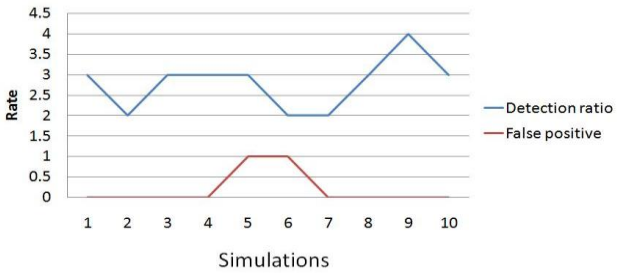

Fig. 18. Detection ratio and false positive under flooding attack detection (with 5 malicious nodes)

Upon using the energy prediction algorithm malicious nodes are identified successfully in the network with a maximum detection ratio of 4:5 and false positive in the range of 0.2.

7. Conclusion

The need for effective intrusion detection scheme in wireless sensor networks is analyzed and energy based detection of Flooding and Gray hole attack is proposed for the same. A learning based energy prediction algorithm is implemented to observe the abnormality of the nodes' behavior. Prediction accuracy obtained is quite high thereby the detection accuracy is also achieved. The proposed detection scheme will increase the detection ratio. By effectively detecting and isolating the intruders from the network, the network's lifetime is also enhanced. Working towards the proposed system Sinkhole, Gray hole, Flooding attacks are launched in the network and their outputs are also recorded. Performance analysis of different types of attacks and the proposed IDS based on different network parameters is carried out. Learning based energy prediction is carried and comparison between the predicted and actual energy is carried out. Flooding attack and Gray hole attacks are detected using the proposed mechanism successfully.

References

[1] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman and Wai-Choong Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," *Communications Surveys & Tutorials, IEEE*, vol 15, pp.1223-1237, July, 2013. Article (CrossRef Link)

[2] Minho Jo ,Longzhe Han and Dohoon Kim, "Selfish attacks and Detection in Cognitive radio adhoc networks,"*Networks, IEEE*, vol 27, Issue 3, pp 46-50, June,2013.

[3] I. Khalil, S.Bagchi,C.N. Rotaru, "UnMask: utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," *Ad Hoc Netw.*,vol 8, pp. 148–164, June,2010 Article (CrossRef Link)

[4] J.H. Son,H. Luo, S.W Seo, "Denial of service attack-resistant flooding authentication in wireless sensor networks," *Comput.Commun.*, vol 33, pp. 1531–1542, 2010. Article (CrossRef Link)

[5] A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, pp 54-62, October 2002. Article (CrossRef Link)

[6] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proc. of IEEE Consumer Communications and Networking Conference*, vol. 1, pp 640-644, January 2006. Article (CrossRef Link)

[7] A.PravinRenold, R.Poongodhai, R.Parthasarathy, "Performance analysis of Leach with gray hole attack in Wireless sensor networks," in *Proc. of International conference on Computer, Communication and Informatics*, pp 1-4, January, 2012.
[8] Guangjie Han. Jinfang Jiang. Wen Shen. Lei Shu. And Joel Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Information Security journal*, vol. 7, Iss. 2, pp. 97–105, June, 2013.
[9] Zhen-wei Shen; Yi-hua Zhu, "An Ant Colony System Based Energy Prediction Routing Algorithms for Wireless Sensor Networks," in *Proc. of 4th International Conference on Wireless Communications, Networking and Mobile Computing,WiCOM '08* .pp 1-4,October, 2008. Article (CrossRef Link)
[10] M.Tiwari,K.V.Arya,R.Choudari,R.Choudari, "Designing Intrusion Detection to Detect Black Hole and Selective Forwarding Attack in WSN Based on Local Information," in *Proc. of Fourth International conference on Computer Sciences and Convergence Information Technology*, pp 824-828, November, 2009
[11] T.Meena,M.Nishanti,E.Kamalabalan,"Cluster-based mechanism for multiple spoofing attackers in WSN," in *Proc. of International Conference on Information Communication and Embedded Systems (ICICES)*, pp.1-5, February, 2014. Article (CrossRef Link)
[12] W.R. Heinzelman,A. Chandrakasan,H. Balakrishman, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. of Hawaii International Conference of System Sciences*, pp. 3005–3014, January, 2000. Article (CrossRef Link)
[13] http://www.nsnam.com
[14] http://www.mannasim.dcc.ufmg.br/msg.html
[15] http://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf
[16] http://moment.cs.ucsb.edu/AODV/

Jeevaa Katiravan received the Bachelor degree in Information Technology from Madras University, India in 2003 and Post Graduate Degree from Sathyabama University, India in 2005.He completed his Doctorate in Information Security from Anna University,Chennai in 2013. Currently, he is an Associate Professor at Velammal Engineering College and has 11 years of teaching experience. His research interests include Network Security and Mobile Security.

Duraipandian.N Completed his Bachelor and Master Degree from REC Trichy. He completed his doctorate in the year 2009 from Anna University. He has nearly 25 years of teaching experience. His Research interest include Context Aware Computing and Sensor Networks.

Dharini Natarajan completed her B.E degree in Electronics and Communication Engineering from Anna University, India in 2012 and M.E degree in Mobile and Pervasive Computing, Anna University, India in 2015.Her research interests are Energy Optimization in Wireless Sensor Networks.