Asian Journal of Information Technology 15 (3): 393-405, 2016
ISSN: 1682-3915

Light Weight Prediction Algorithm Based IDS for Wireless Sensor Networks

[1]S.M. Udhayasankar, [2]V. Vijaya Chamundeeswari and [2]N. Dharini
[1]Department of CSE,
[2]Velammal Engineering College, Chennai, India

Abstract: Wireless sensor networks when deployed in an unmanned environment to monitor the surroundings are prone to various security threats. Threats go severe in case of hierarchical WSN where the powerful cluster heads gets attacked thereby affecting the entire cluster. These hierarchical WSN are prone to various denial of service attacks such as black hole, gray hole, sybil, wormhole, flooding, etc. DoS attacks occur in the network layer during routing process; hence, they are also called as routing layer attacks. These Denial of Service (DoS) 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 anyone 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. To serve this purpose, a learning based prediction algorithm is proposed. Thus, a prediction based Intrusion Detection Scheme (IDS) to detect the malicious nodes is proposed and simulations were carried out using NS2 Mannasim framework. Simulation results prove the performance of the proposed work by achieving good detection ratio and less false positive.

Key words: Denial of service attacks, hierarchical routing, cluster head, cluster member, IDS

INTRODUCTION

Wireless Sensor Network (WSN) is the collection of sensor nodes deployed in a large area to monitor the environment. Wireless sensor networks are often organized in the form of clusters leading to the new framework of WSN called cluster or hierarchical WSN where cluster head sensor nodes act as an intermediate between the source and the sink nodes to relay the sensed data thereby achieving energy efficiency. Each cluster head is responsible for its own cluster and its members. These networks find application in various fields such as environmental monitoring, defense and military applications. 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 (Abduvaliyev *et al*., 2013). Particularly, denial of service attacks happening in the routing/network layer 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 behaviors of sensor nodes consumes energy resources, thus, they are not suitable for resource-constrained WSNs (Khalil *et al*., 2010; Son *et al*., 2010). Furthermore, the packet forwarding in WSNs is unstable and packet loss is likely to occur during transmission process. Therefore, IDSs based on monitoring the behaviors of sensor nodes cannot detect routing layer attacks efficiently.

Attacks 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) (Wood and Stankovic, 2002) 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.

Corresponding Author: S.M. Udhayasankar, Department of CSE, Velammal Engineering College, Chennai, India

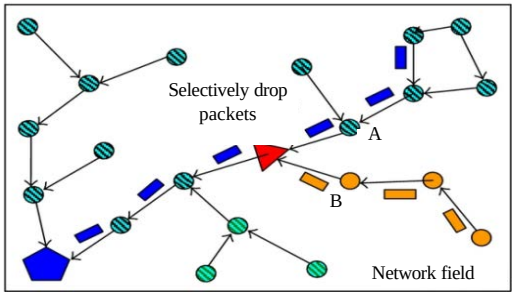

Fig. 1: Gray hole attack

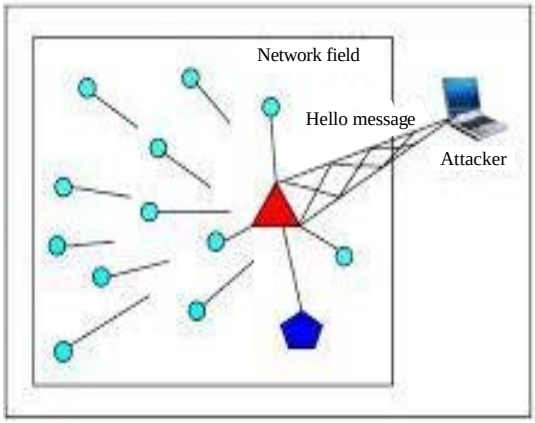

Fig. 2: Flooding attack

Denial of service attacks: In gray hole attack 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.

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. In a sinkhole or black hole 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.

Literature review: IDS mechanisms and techniques make 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

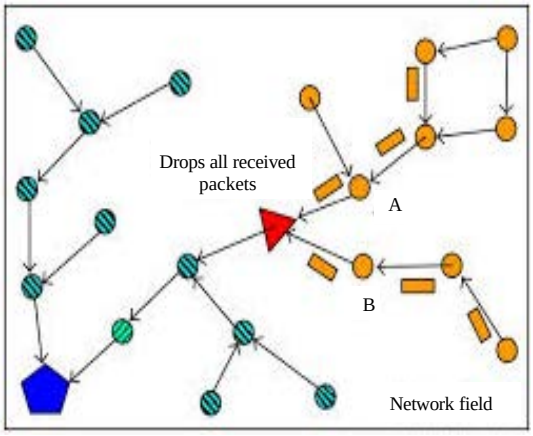

Fig. 3: Blackhole attack

technique used for studying the audit data. Therefore, we can classify IDSs into three groups: misuse, anomaly and 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 study (Roman *et al*., 2006) 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.

The main idea of IDSEP (Han *et al*., 2013) 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 Shen *et al*. (2008). In this study, the packet forwarding nodes are selected based on its residual energy prediction. This research does not consider the security aspect of the network.

Cluster-based mechanism for multiple spoofing attackers in WSN (Tiwari *et al*., 2009) 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 need correlation among the neighbors, thus, consuming more energy.

In research (Meena *et al*., 2014) black hole and selective forward attacks are detected by means of local information obtained from neighbors. Neighborhood nodes do not have a global view of the network which is vital for intrusion detection design.

Isolation table (Chen *et al*., 2009) based approach to detect intrusions in hierarchical WSNs in an energy efficient way was proposed. The proposal required two levels of clustering. According to their experiment, their- isolation table intrusion detection method could detect attacks effectively. In the case that the higher level node is the intruder, it will not allow the BS to be aware of its misbehavior by simply blocking the alert messages it receives from the lower level nodes.

An IDS based on clustering approach (Strikos, 2007) was proposed. Their proposal also ensured the security of the CHs. In their approach, members of a cluster monitor their CH in a time scheduled manner. In this way, energy for all cluster members is saved. On the contrary, cluster members are monitored by the CH not by the contribution of cluster members. This also saves the energies of the cluster members. Through simulations, the researchers showed that their proposed algorithm is much more efficient compared to other algorithms in the literature. The problem with this approach is its key management mechanism. It is a part of the IDS and helps IDS to establish pairwise keys among the nodes. The IDS uses these keys through the authentication of the messages. The key management assumes that the nodes are stationary (non-mobile) and the new nodes cannot be added after the pair wise keys are established. This constitutes a handicap for the model considering the fact that WSN may periodically require deployment of new nodes.

The research in Su *et al*. (2005) incorporated a hierarchical IDS model in which the network is divided into clusters and for each cluster, a CH is elected. They issued centralized routing meaning that every packet of transmitted data will be forwarded to the CH and then to the base station. Their proposal included a method to place intrusion detectors in the CHs so that the entire network is covered with a minimum number of detectors. The researchers did not provide any simulation results or any real experimental data. So, it is not clear whether the system would perform as promised.

Energy consumption is very high in state of art IDS. Thus, it is critical to develop effective IDS to defend routing layer 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 routing layer attacks efficiently.

In this study, an intrusion detection mechanism based on light weight learning based energy prediction algorithm is proposed. The objective of this study is as follows:

- Comparative performance analysis of various types of routing layer attacks
- An IDS approach is implemented where sink nodes monitor the cluster heads and cluster heads monitor the cluster members for their malicious activity
- Light weight 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
- Detected malicious nodes are removed from the network

Network model: Hierarchical WSN is formed with various clusters. The entire network of nodes is organized into various clusters. Each cluster will have one Cluster Head (CH) and depending upon the radio range of CH, cluster member joins the cluster. Operation of such a network starts with setup phase where nodes with highest energy are elected as CH nodes. In the steady state, phase cluster members communicate the sensed data to their CH. Sensed data is collected and aggregated by each CH and transmits them to the sink node.

Cluster members are programmed to sense the data at particular time interval called sensing interval. Sensed data is disseminated to the CH at particular time interval called dissemination interval. Sensor nodes are programmed similar to mica2 motes characteristics.

Assumptions:

- Static 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
- Sensor nodes cannot lie about their energy consumption

Energy model: Sensor nodes have five operation states. Sleeping state: sensor nodes in sleeping state do not interact with other nodes. Therefore, there is no need to evaluate their energy consumption. Sensing state: in this state, sensor nodes are responsible for sensing physical parameters, such as temperature, atmospheric pressure, etc. Calculate: sensor nodes process the sensed data. Receiving state: sensor nodes monitor and receive data packets. Transmitting state: sensor nodes transmit data packets to the sink node. It is believed that energy is mainly consumed in the last two states. We adopt the energy model in (Heinzelman *et al*., 2000) to obtain energy consumption of normal nodes. When sending a message with k bits, the energy consumption is given in Eq. 1:

$$E_{Tx} = E_{elec} \times k + \varepsilon_{amp} \times k \times d^2 \quad (1)$$

Where:

E_{tx} = The transmitting energy

E_{elec} = The transmitter and receiver electronics, i.e., energy consumption for sending and receiving each bit, d is the distance between the sender and receiver

ε_{amp} = The energy consumption exponent

To receive this message, energy consumption of each sensor node is given in Eq. 2:

$$E_{Rx} = E_{elec} \times k \quad (2)$$

where, E_{Rx} is the receiving energy:

$$E_{c(k)} = (n_{s(k)} \times E_{Tx}) + (n_{r(k)} \times E_{Rx}) + E_{sensing} + E_{idle} + E_{calculate} \quad (3)$$

Where:

$E_{c(k)}$ = The total energy consumption of sensor node at time k

$n_{s(k)}$ = The number of bits transmitted at time k

$n_{r(k)}$ = is the number of bits received at time k

$E_{sensing}$ = Energy consumption during sensing

E_{idle} = Energy consumption in idle mode

$E_{calculate}$ = Energy consumption during processing of information

MATERIALS AND METHODS

Proposed system

Modelling of denial of service attacks: In order to analyze the severity of attacks, gray hole, black hole and flooding attacks are implemented using the steps given below. 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 (N_i) works according to the AODV routing protocol. In AODV routing protocol, the source node requests the neighboring nodes for the route to reach the destination by sending the RREQ (Route Request) packets. The neighbors having the route replies the source node with RREP (Route Reply) packets. The freshness of the route is maintained by the sequence numbers. 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).

The nodes (GN) launching flooding attack unwantedly flood the network with large number of Route Request (RREQ) packets. The nodes (GN) launching blackhole attack works as follows:

- Send fake Route Reply (RREP) packets with large sequence numbers
- Disable the Route Error (RERR) 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 (GN) launching gray hole 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. So, the above steps are repeated for a certain amount of time interval

Flooding attacker node exhausts the network resources in terms of bandwidth and energy. Gray hole attacker node intentionally drops packets thereby leading to misinterpretation of sensing data. The energy consumption of attack varies based on the nature of attack, thus among the three, flooding and gray hole 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

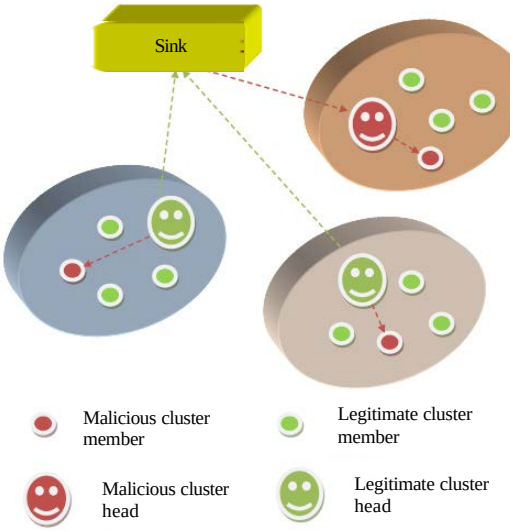

Fig. 4: Proposed IDS architecture

nature of working of routing layer attacks we Implemented two level Distributed IDS Scheme.

IDS architecture: Existing IDS either depends 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, only if cluster heads act as intrusion detection agent, there are possibilities that cluster heads may be compromised. So, the malicious behavior of both cluster member and cluster head 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 intrusion detection architecture is shown in Fig. 4.

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. Identified malicious nodes are deleted from the routing table.

Light weight learning based energy prediction algorithm: All nodes are programmed to send their residual energy after a particular interval of time (say 50 sec) to their cluster heads. Upon receiving the residual energy, the actual energy consumed is calculated as follows in Eq. 4:

$$\text{Actual energy } (E_1(v)) = \text{Initial energy-Residual energy} \quad (4)$$

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

$$E_0(v) = 0 \quad (5)$$

where, $E_0(v)$ in Eq. 5 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:

$$E_K(v) = e_k \quad (6)$$

where, e_k is the energy realistically consumed by the node v during $T_{k-1, k}$ as shown in Eq. 6 e_k is the energy, the cluster heads obtain from all nodes at the end of kth interval (say 100 sec). Upon having E_0 and E_k where k = 1, 2, 3.. the predicted energy consumption is calculated as follows in Eq. 7:

$$\text{Predicted Energy}(E_{k+1}(v)) = e_k + Ø(E_k(v) - E_{k-1}(v) \quad (7)$$

The 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 A below.

Algorithm A:

```
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 Ek(i) be the energy consumed at time instant 'k' by node I;
Let E0(i) = 0;
Ek(i) = ek(i) ;
Predicted Energy(Epk +1(i)) = Ek(i)+Ø(Ek (I)–Ek-1(i));
}
```

Usually, learning based prediction is accompanied by prediction error. Weight factors need to be adjusted accordingly to reduce the error between desired and predicted output. Initially by default 0.5 is set as weight factor Ø and prediction is carried out. Prediction error is calculated using the formula Eq. 8 given below:

$$\text{Error}_{k(i)} = |\text{Actual Energy Consumed}_{k(i)} - \text{Predicted Energy}_{k(i)}| \quad (8)$$

In order to bring the prediction error minimal, the weight factor is calculated using the formula given below, thus from Eq. 7:

$$Ø = (\text{Actual Energy}_{k+1(i)} - E_{k(i)})/(E_{k(i)} - E_{k-1(i)}) \quad (9)$$

Where:

Ø = The weight factor

$E_{k(i)}$ = The energy consumed at time instant 'k' by node i

$E_{k-1(i)}$ = The energy consumed at time instant 'k-1' by node i

From the above Eq. 9 weight factor is tuned according the actual energy consumption. Thus, the weight factor calculation is carried out for all the sensor nodes. Simulations are carried out to adjust the weight factor under various scenarios and tabulated in simulated results study.

The algorithm is light weight in nature because it requires only the past 2 inputs to predict the future output at various time instants. Prediction error can also be maintained within an optimum range by suitably adjusting the weight factor. Prediction accuracy also depends upon the time interval chosen. Our simulations were carried at an interval of 20 sec. Thus, for every 20 sec prediction of nodes' energy consumption takes place.

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, (0-50 sec) sensor nodes will send a packet indicating their residual energy E_{r1}, upon which the actual energy consumption is calculated as follows:

$$E_{c1} = E_{i1} - E_{r1}. \quad (10)$$

Based on the proposed energy prediction algorithm, the cluster head node can predict sensor nodes' energy consumption for the second interval (50-100 sec) 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:

$$E_{c(i)} = E_{r(i)} - E'_{r(i)} \quad (11)$$

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.

The difference between actual and predicted energy consumptions (Prediction Error) of every node is calculated using Eq. 12-15 given below:

$$E_i = \text{Actual Energy Consumed}_i - \text{Predicted Energy}_i \quad (12)$$

$$T1 = \min(\text{Error}_{k(i)}) \quad (13)$$

$$T2 = \text{average}(\text{Error}_{k(i)}) \quad (14)$$

$$T3 = \max(\text{Error}_{k(i)})) \quad (15)$$

In Eq. 13-15 and $\text{Error}_{k(i)}$ refers to Eq. 8. error values of all the nodes are aggregated and minimum, maximum and average of all the nodes' error are formulated and set as thresholds T1-T3.

Attackers are classified by comparing every node's error value with the minimum, maximum and average error values as follows.

If $T1 < E_i = T2$, then the sensor node i is the legal one. Prediction error is greater than the minimum and maintained within the average value.

If $0 < E_i = T1$, then sensor node i is regarded as a malicious one launching a gray hole attack. In gray hole

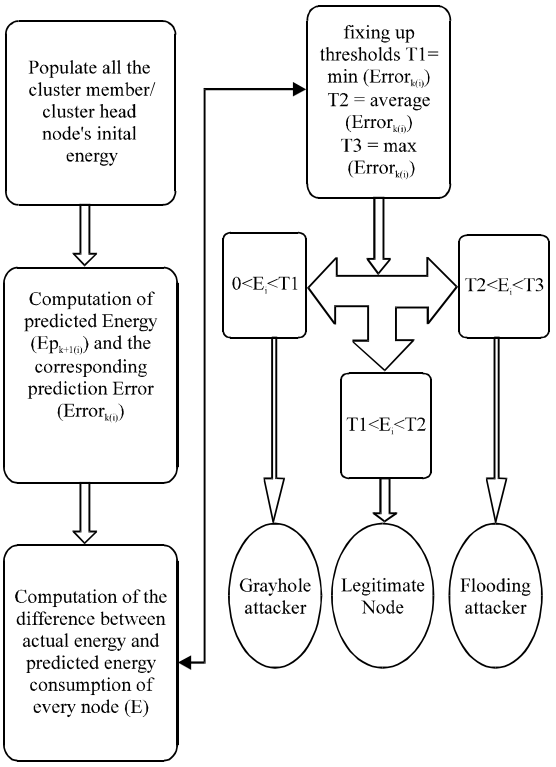

Fig. 5: Intrusion detection process

attack, the attacker node selectively drops certain number of packets, so its transmission becomes less. Prediction error is very less than the expected minimum value hence it is a gray hole node which consumes energy less than the legal one.

If $T2<E_i = T3$, then sensor node i is regarded as a malicious one launching a flooding attack. Prediction error is greater than the average value and more or less equal to maximum error value thus, contributing high energy consumption in the network. In a flood attack, node sends as many packets as possible with abnormally high transmission energy to all the nodes. Thus, flooding node consumes higher energy than the legitimate node.

Thus, the nodes detected as malicious are added in the blacklist of the routing table by the cluster heads and sink and thereby they are removed from the network. No routing process takes place via malicious nodes. The fore mentioned process is depicted in Fig. 5.

Energy analysis of sensor nodes: According to mica2 motes characteristics in NS2 MANNASIM simulator the transmission power for sensor node is set to 0.036W.

$$\text{Energy} = \text{Power} \times \text{time} \quad (16)$$

Upon analyzing the additional energy consumption of nodes to send packets indicating their residual energy through simulation, each node approximately consumes 0.03 J sec every time more than the normal scenario.

Advantages:

- More number of malicious nodes can be detected simultaneously-detection ratio is high
- Faster intrusion detection because of distributed detection architecture
- Computation complexity is less due to the learning based energy prediction algorithm
- Proposed IDS consumes fewer amounts of network resources

RESULTS AND DISCUSSION

Network Simulator-2 with MANNASIM framework is used to evaluate the performance of the proposed work. 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 characteristics can be simulated. The simulation parameters are given below in Table 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 learning based energy prediction algorithm is implemented in NS-2. Ø (Weight factor) is tuned for various scenarios using Eq. 9. 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.

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.

Table 1: Simulation parameters

Parameters	Values	Parameters	Values
No. of nodes	10, 20	Initial energy (sink)	100 J
No. of sink	1	Initial energy (access point)	100 J
No. of cluster heads	2	Initial energy (nodes)	10 J
No. of attackers	9 (each 3)	Initial energy(CH)	50 J
Routing protocol	AODV	Sensing interval	5 sec
MAC	MAC/802.11	Disseminating interval	20 sec
Physical layer	Phy/wirelessphy-mica2	Simulation time	150 sec

Table 2: The Ø (weight factor) determination

No. of nodes	Ideal scenario	Black hole	Gray hole	Flooding
10	0.70	0.60	0.68	0.90
20	0.50	0.50	0.50	0.99
30	0.50	0.80	0.80	0.98
40	0.80	0.80	0.80	0.95
50	0.80	0.90	0.80	0.98
AVG	0.66	0.72	0.73	0.96

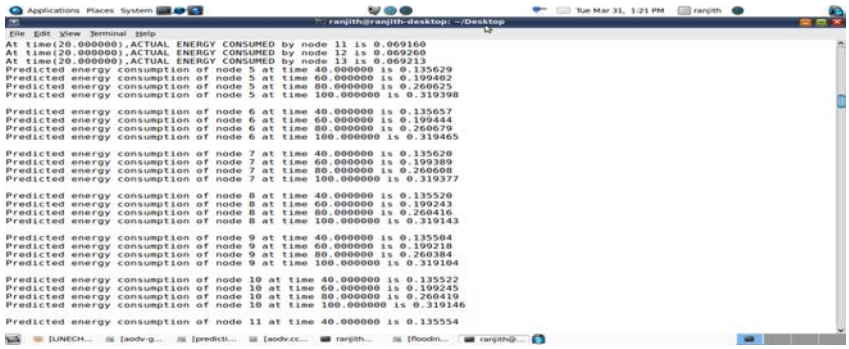

Fig. 6: Predicted energy values of cluster members at various time instants

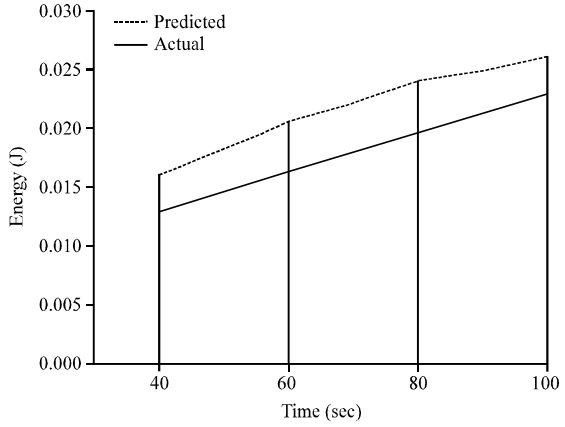

Fig. 7: Comparison between actual and predicted energy consumption under Ideal hierarchical WSN scenario

The terminal output of the network with nodes' predicted energy at various time instants is shown below in Fig. 6.

The comparison between predicted energy calculated with the above weight factor values and the

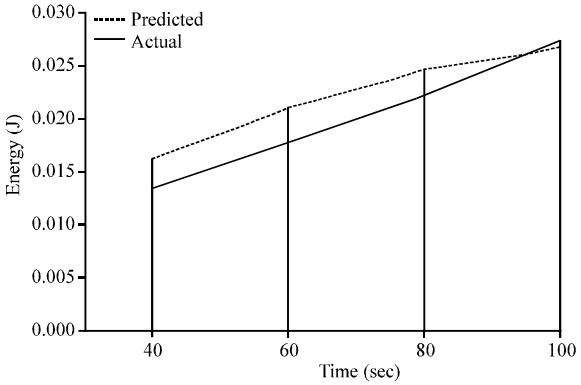

Fig. 8: Comparison between actual and predicted energy consumption under Blackhole attack scenario

a comparison between predicted and actual output under flooding, gray hole, blackhole and ideal scenario are shown below in Fig. 7-10. 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.

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 12. Nodes marked with red circles are malicious nodes. Corresponding terminal outputs are shown in Fig. 13 and 14.

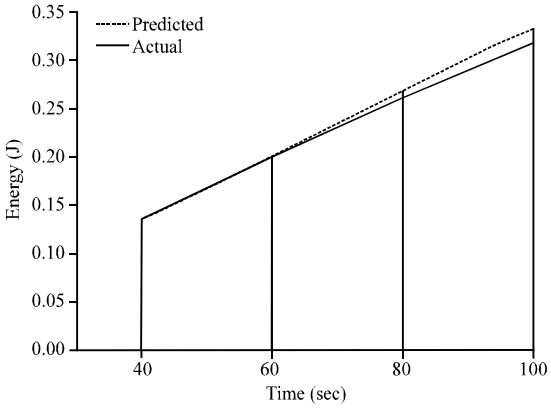

Fig. 9: Comparison between actual and predicted energy consumption under flooding attack scenario

Performance analysis of hierarchical WSN with flooding, blackhole, gray hole, proposed IDS and without attack: Each of the 3 attack is initiated by 3 malicious nodes in the network. The following network

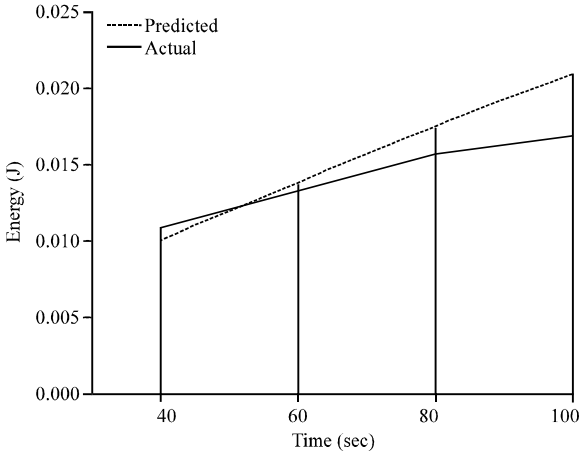

Fig. 10: Comparison of actual and predicted energy under gray hole attack scenario

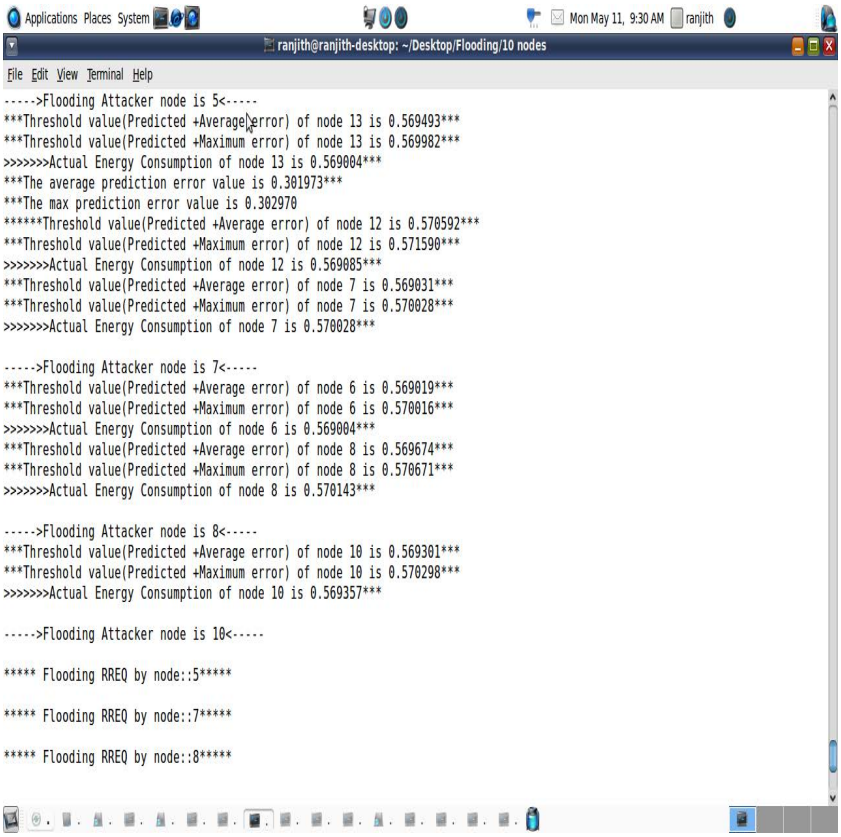

Fig. 11: Detection of flooder node in terminal

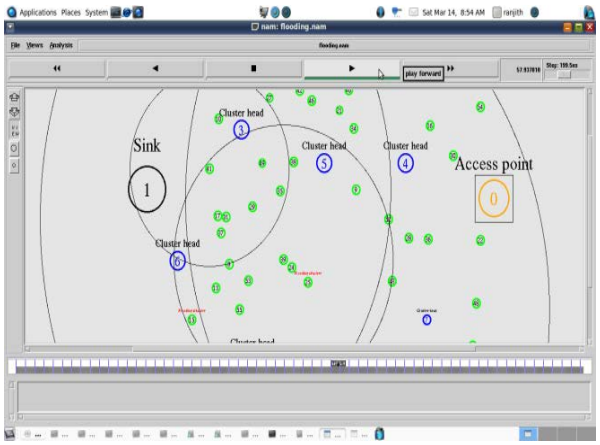

Fig. 12: Detection of flooding attacker node in nam window

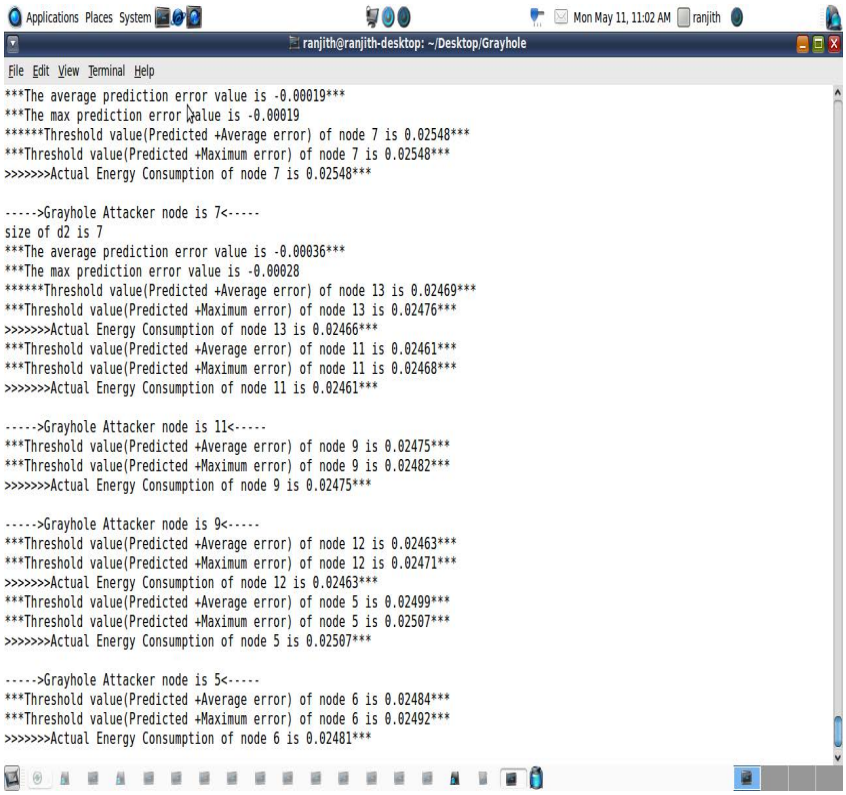

Fig. 13: Detection of gray hole attacker in terminal

parameters are analyzed using the trace file generated under different attacks generated. Trace files are evaluated using AWK scripts and the corresponding values are plotted.

Effective throughput: Effective throughputs of WSN with and without attacks are shown in the following Fig. 15. Effective throughput refers to the rate of successful legitimate message delivery over a communication channel. It is measured in bits/sec. Packets are delivered successfully under flooding and selective forward attacks because the former only floods unwanted packets thus, the meaningful packets were 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.

Packet Delivery Ratio (PDR): It is defined as the ratio between number of packets received to the number of

Fig. 14: Detection of gray hole attacker in Nam window

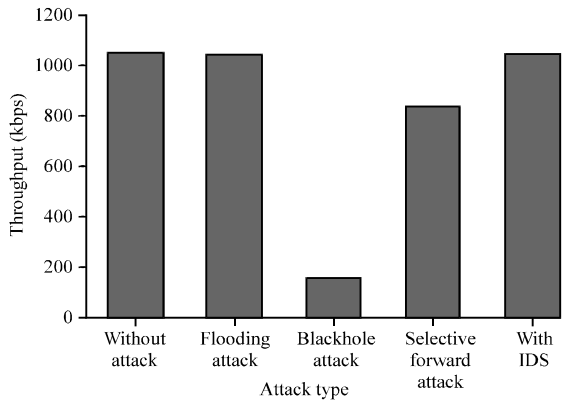

Fig. 15: Comparison of throughput

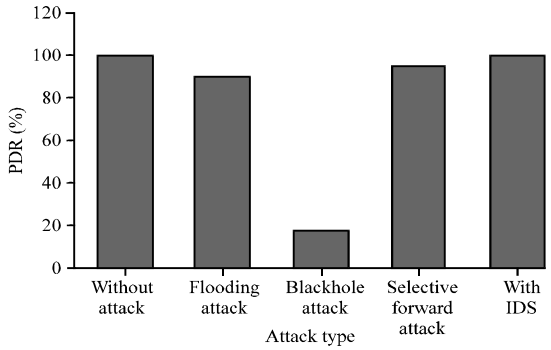

Fig. 16: Comparison of PDR

packets sent ideally PDR should be 100%. PDR of various attacks are shown in Fig. 16 of which black hole attack's PDR is very less due to large number of intentional packet drop.

Average end-to-end delay: The time taken by the data and control packets to reach the destination is called average end to end delay. This delay also includes transmitting, forwarding, queuing delays. Ideally in a network, delay must be minimum. From Fig. 17, among others flooding attack suffers higher delay. Due to

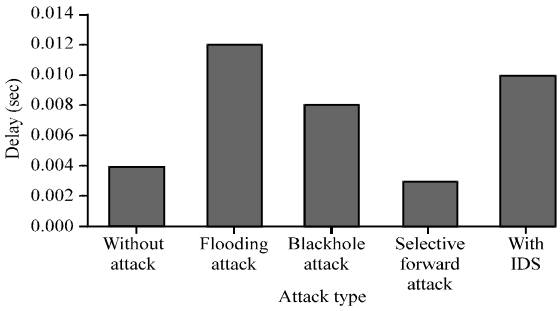

Fig. 17: Comparison of delay

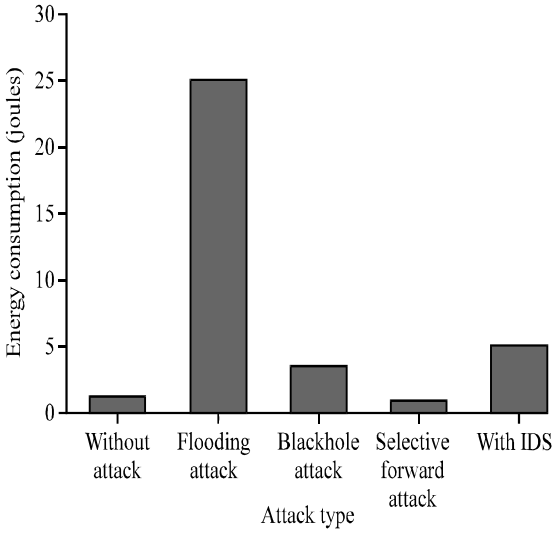

Fig. 18: Comparison of energy

dissemination of unwanted data or control packets, the network traffic increases steadily thereby the delay is very high in case of flooding attack.

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. 18.

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.

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. 19-22 under flooding and gray hole attack detection scenarios.

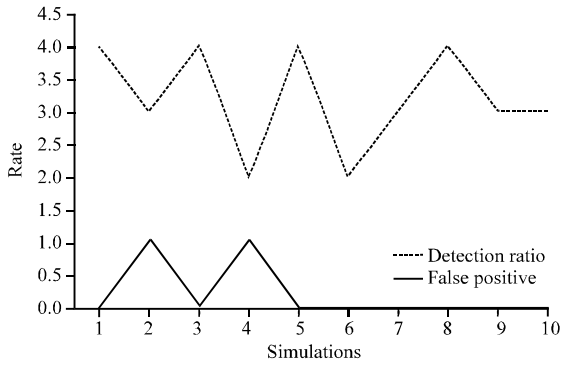

Fig. 19: Detection ratio and false positive under flooding attack detection (with 5 malicious nodes)

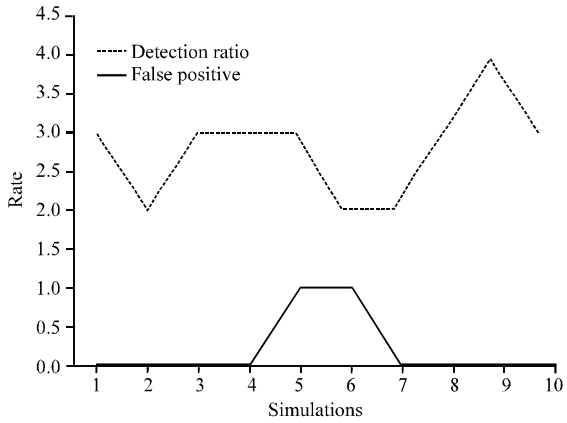

Fig. 20: Detection ratio and false positive under gray hole attack detection (with 5 malicious nodes)

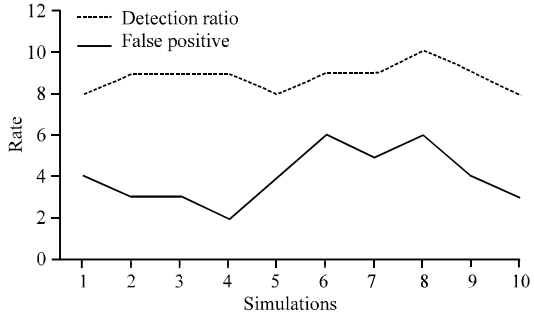

Fig. 21: Detection ratio and false positive under flooding attack detection (with 10 malicious nodes)

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 0.1.

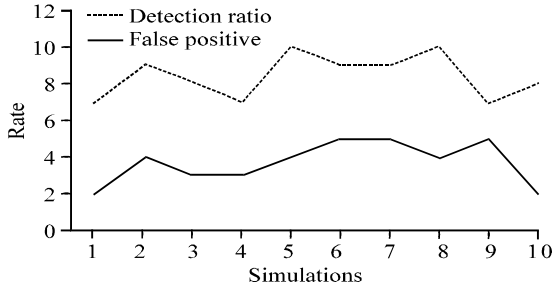

Fig. 22: Detection ratio and false positive under gray hole attack detection (with 10 malicious nodes)

CONCLUSION

The need for effective intrusion detection scheme in wireless sensor networks is analyzed and a light weight prediction based IDS for 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. 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 based on different network parameters is carried out. Light weight learning based energy prediction is implemented 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

Abduvaliyev, A., A.S.K. Pathan, J. Zhou, R. Roman and W.C. Wong, 2013. On the vital areas of intrusion detection systems in wireless sensor networks. Commun. Surv. Tutorials IEEE., 15: 1223-1237.

Chen, R.C., C.F. Hsieh and Y.F. Huang, 2009. A new method for intrusion detection on hierarchical wireless sensor networks. Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, January 15-16, 2009, ACM, New York, USA., ISBN: 978-1-60558-405-8, pp: 238-245.

Han, G., J. Jiang, W. Shen, L. Shu and J. Rodrigues, 2013. IDSEP: A novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. Inf. Secur. IET., 7: 97-105.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless micro sensor networks. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, January 4-7, 2000, Maui, HI., USA., pp: 3005-3014.

Khalil, I., S. Bagchi, C.N. Rotaru and N.B. Shroff, 2010. UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. Ad Hoc Networks, 8: 148-164.

Meena, T., M. Nishanthy and E. Kamalanaban, 2014. Cluster-based mechanism for multiple spoofing attackers in WSN. Proceedings of the 2014 International Conference on Information Communication and Embedded Systems (ICICES), February 27-28, 2014, IEEE, Chennai, India, ISBN: 978-1-4799-3835-3, pp: 1-5.

Roman, R., J. Zhou and J. Lopez, 2006. Applying intrusion detection systems to wireless sensor networks. Consum. Commun. Networking Conf., 1: 640-644.

Shen, Z.W., Y .H. Zhu, X .Z. Tian and Y.P. Tang, 2008. An ant colony system based energy prediction routing algorithms for wireless sensor networks. Proceddings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, October 12-14, 2008, IEEE, Dalian, China, pp: 1-4.

Son, J.H., H. Luo and S.W. Seo, 2010. Denial of service attack-resistant flooding authentication in wireless sensor networks. Comput. Commun., 33: 1531-1542.

Strikos, A.A., 2007. A full approach for intrusion detection in wireless sensor networks. School of Information and Communication Technology, Stockholm, Sweden, https://people.kth.se/~maguire/courses/IK2555 /ExamplePapers/Andreas_Strikos-paper-20070301.pdf.

Su, C.C., K.M. Chang, Y.H. Kuo and M.F. Horng, 2005. The new intrusion prevention and detection approaches for clustering-based sensor networks (wireless sensor networks). Proceedings of the 2005 IEEE Conference on Wireless Communications and Networking, March 13-17, 2005, IEEE, USA., ISBN: 0-7803-8966-2, pp: 1927-1932.

Tiwari, M., K.V. Arya, R. Choudhari and K.S. Choudhary, 2009. Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. Proceedings of the Fourth International Conference on Computer Sciences and Convergence Information Technology, ICCIT'09, November 24-26, 2009, IEEE, Seoul, South Korea, ISBN: 978-1-4244-5244-6, pp: 824-828.

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.