Journal of Computer Science 9 (9): 1106-1116, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1106.1116 Published Online 9 (9) 2013 (http://www.thescipub.com/jcs.toc)

A LEADER BASED MONITORING APPROACH FOR SINKHOLE ATTACK IN WIRELESS SENSOR NETWORK

[1]Udaya Suriya Rajkumar, D. and [2]Rajamani Vayanaperumal

[1]Department of Computer Science and Engineering, Sathyabama University, Chennai, India
[2]Department of Electronic and Communication Engineering, Indra Ganesan College of Engineering, Trichy, India

Received 2013-01-31, Revised 2013-06-14; Accepted 2013-07-10

ABSTRACT

Security is one of an important factor to be considered seriously in wireless sensor networks. In WSN, in many ways intrusion may occur, in the past decades there is no perfect IDS, without any wasting of resources like time, energy, cost and number of physical items. The main objective is to ensure the security and improve the quality of network by applying a Leader based intrusion detection system in the Wireless Sensor Network (WSN). Here, we are focusing on the attack known as sinkhole attack which is considered as the biggest threat in wireless sensor network which spoils the complete communication and a data loss between a pair of nodes as source node and a destination node. In order to provide a complete solution to detect and avoid sinkhole attack a Leader Based Intrusion Detection System (LBIDS) is proposed. In this approach a leader is elected for each group nodes within the network, region wise and it do compares and calculates the behavior of every node, logically executes our detection module and monitors each node behaviour within the cluster for any sinkhole attack to occur. When a node gets detected as a compromised node, it informs that nodes status to the other leader within the WSN, so all the leaders in the network knows about the sink hole node information and the leaders stop communication with sinkhole Node.

Keywords: Energy Efficiency, IDS, Illegal Node, LBIDS, Node Status, Transmission Range, WSN

1. INTRODUCTION

Network consists of sensor nodes deployed over a geographical area for a wireless Sensor monitoring physical phenomenon like temperature, humidity, vibrations, seismic events and so on. The basic components for data transmission using wireless communication are tiny devices. The development of wireless sensor network was originally motivated by military applications like battlefield surveillance, medical care and forest monitoring (Werner-Allen *et al*., 2006; Zhao and Guibas, 2004). However, WSNs are now used in many civilian application areas including the environment and habitat monitoring. Sensor networks are used for many applications where security is crucial. It is essential to ensure secure communication among the nodes because of the importance of the sensed data. There are various types of attacks on sensor networks, while some of the attacks are common in different types of networks. But we are focusing on the sinkhole attack, a serious threat which prevents the base station from obtaining complete and correct sensing data in this study of (Edith *et al*., 2007; Kalita and Kar, 2009; Perrig *et al*., 2004). A novel algorithm for detecting the intruder in a sinkhole attack is proposed where the algorithm first finds a list of suspected nodes through checking data consistency and then effectively identifies the intruder in the list through analyzing the network flow information. It is not possible to use a general intrusion detection technique for WSNs because of resource-constraint and communication overheads involved (Anjum and Mouchtaris, 2007; Akyildiz *et al*., 2011; Rezaei and Mobininejad, 2012). The main resource constraint is that a power source supplies the energy needed by the device to perform the programmed tasks. This power source often consists of a battery with a limited energy budget. The major difference between the wireless sensor network and the traditional wireless network sensors are

Corresponding Author: Udaya Suriya Rajkumar, D., Department of Computer Science and Engineering, Sathyabama University, Chennai, India

very sensitive to energy consumption. Moreover, the performance of the sensor network applications highly depends on the lifetime of the network (Rezaei and Mobininejad, 2012; Chang and Sheu, 2009). Here, a light weight intrusion detection system is designed to detect the sinkhole attack within the sensor network which uses the leader election based approach for executing instruction detection system in WSN (Mohammed *et al*., 2011) helps to overcome limited energy problem, by dividing the MANET into a set of one hop clusters where each node belongs to at least one cluster. The nodes in each cluster elect a leader node (cluster head) to serve as the IDS for the entire cluster. This approach aims to reduce the overall resource consumption of IDSs in the network (Li *et al*., 2008). The rest of this study is organized as follows: Section 2 presents the detailed leader based intrusion detection mechanism, sinkhole attack and its remedies, its routing algorithm. Section 3 provides results and discussion of the proposed algorithm. Conclusions and further works are presented in section 4.

2. MATERIALS AND METHODS

In this section we have made an attempt to analyze and avoid intrusion in the route (EI-Khatib, 2010) in which the source transfers the data to the destination. There are two chances of intrusion which can happen in the route. One is inside the network region and the other is outside the network region. Inside the network region and in the route may be the sinkhole attack, where an intermediate node can act as sink and it never transfers the data to the next node shown in the following **Fig. 1**.

The effect of a sinkhole in a WSN is shown in **Fig. 1**; imagine that a sinkhole node is M. When node S broadcasts a RREQ packet, all the nodes and M also receive it. Node M, being a sinkhole node, does not check up with its routing table for the requested route to node D. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node S receives the RREP from M ahead of the RREP from node B and node E. Node S assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node S sends data to M, M absorbs all the data and there is no acknowledgement from the other nodes especially from node D. So the attacks can be achieved. A sinkhole attack in wireless sensor networks can cause serious problem in the operations and services of the networks. It may lead to the problem of system failure in terms of network availability (Sharma and Ghose, 2010). It makes the sensor node unable to transmit and receive information. It is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and without forwarding them to the destination. To get as much influence on routes as possible, a sinkhole will have to take action every time a route is being created. When a sinkhole route reply message indicating that it has been found the destination with the lowest possible hop count. All nodes along the route back to the source of the route request will store the route towards the sinkhole in the routing table (Fessant *et al*., 2011). If the real destination is a larger number of hops away from the source than the sinkhole, the route to the sinkhole will be chosen. When the real destination is closer, the route to the sinkhole will be ignored. The next one is finding intrusion in outside region. Over all nodes in the network are assumed as beacon nodes and those nodes always knows about their locations and send to other nodes. Also we are giving an id for each node in the network. So in a second, the same route, the nodes location and ID are checked. One of the main issues in the wireless sensor network is an intrusion.

2.1. A Leader Based Intrusion Detection System

There are many intrusion detection system developed for WSN (Anastasi *et al*., 2009; Mohammed *et al*., 2011). In this study we used Leader Election Mechanism for LBIDS approach. In this mechanism a leader is elected for solving the IDS in the WSN, which is a cost effective and resource effective approach. In this technique the WSN area is split into regions. Each region is considered as a sub-network. All the M number of regions might have N number of nodes and each node is assigned with initial energy value 100. There is a base station BS, which should be in centre of the network and it has the highest energy value than all the nodes.

In the initial stage, there is a random node is considered as a leader node and the other nodes are regular nodes. Also, while constructing the nodes, it has to register its information to the cluster head. At the time of data transaction the leader will be elected dynamically due to the energy level, having the highest energy (Rong *et al*., 2011) in the network region. It is clear that the regions and the common cluster, region wise cluster and the table which stores the ID and location of the nodes are shown in **Fig. 2**. Whenever a node starts communication in the network, the clusters can verify the table and permit various phases of leader based algorithm. They are explained below. In this proposed approach, the complete functionality is defined by three algorithms as Leader

Election Algorithm, Algorithm for Avoid Malicious, CheckIDS Algorithm.

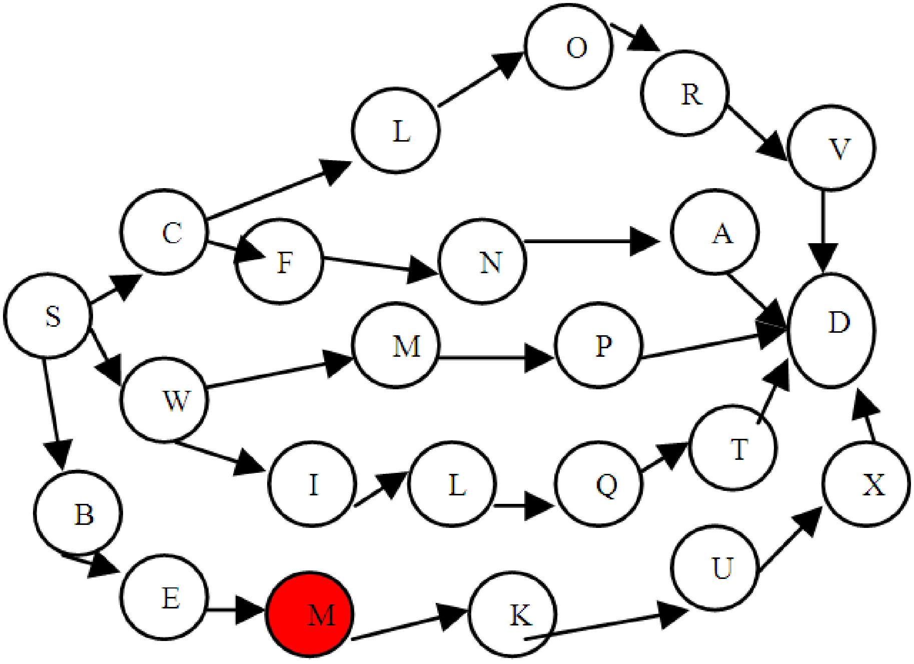
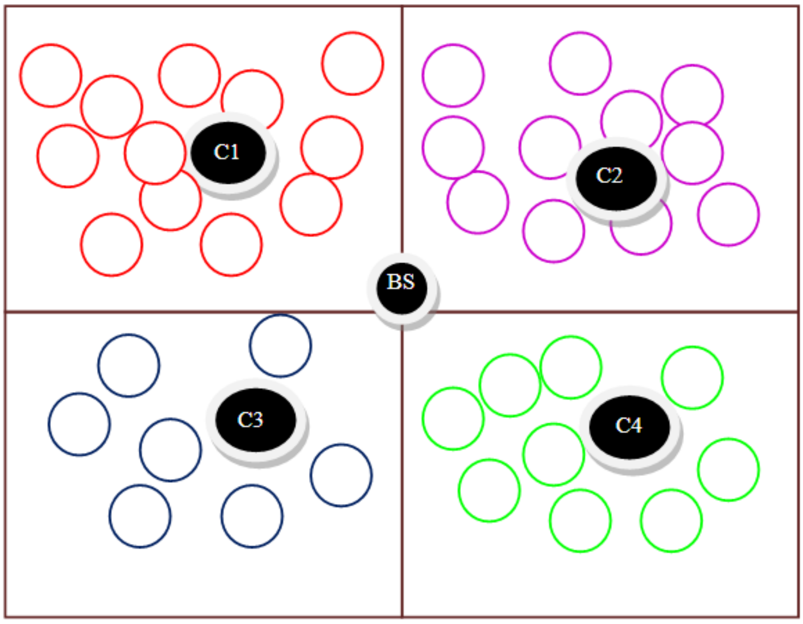


Fig. 1. Sinkhole attack



Node ID	N1	N2	N3	N4	..	..	Ni	..	Nm
Location	1,2	34,45	5,6	76,56	43	5,87	88,98	34,13	43,44

Fig. 2. WSN Region wise leader and Node ID table for nodes

Phase I: Leader Election Algorithm

```
1.  Start procedure leader_election_model()
2.  G = {N, E}, network G with N number of nodes are connected with edges E.
3.  G = {{$G_1$},{$G_2$},{$G_3$},....{$G_i$},....{$G_m$}}
4.  Find centre of G and elect a leader in that place as C
5.  for i= 1 to m
6.  N = {$n_1$,$n_2$,$n_3$...$n_i$,...$n_n$ } // number of nodes in group $G_i$
7.  Assume $E_o$ = 100, $T_o$ =0; // initial energy to all nodes and time starts from 0.
8.  At every time $t_i$, calculate $e_i$ for all the nodes
9.  Elect the cluster  $C_i$ = e($n_i$) > e($n_1$,$n_2$,$n_3$...$n_m$)
10. Repeat step 7 and 8 for all the $G_i$
11. Call LBIDS()
12. End procedure
```

Phase II: Algorithm For Avoid Malicious

```
1.  Start procedure LBIDS()
2.  $n_i$ <- source node
3.  $n_j$ <- destination node
4.  Find route from $n_i$ to $n_j$
5.  Let route R = {$n_i$, $n_a$,$n_b$,$n_c$,....,$n_j$}
6.  Call checkIDS(R)
7.  End if
```

Phase III: CheckIDS Algorithm

```
1.  Start procedure checkIDS(R)
2.  Route <- get nodes of R
3.  Compare ID and location of route nodes
4.  if ID, location exists in the info table
5.    return " continue"
6.  else
7.    return "change the path"
8.  end if
```

2.2. Existing Sinkhole Attack and its Remedies

Figure 3 shows the sinkhole attack. Here, the screen shot shows that, in the route 0->3->5->6, 0 is source node and 6 is the destination node, when 0 starts transmitting the data to 6 through 3, 5 the node 3 is getting all the information and not transmitting to the other nodes. It is behaving like a sink and holding all the data by itself.

There are a number of nodes in a wireless sensor network, where the node 0 is considered as source node and the node 6 is considered as destination node. While transferring the data from source to destination, the source node is sending request and getting response from the other nodes and finding the route. In this scenario, the node 3 is sending response to the source node first and it will get the data from source node and keeps all the data by itself. The source node is waiting for the acknowledgement from the destination node and not getting it. So, after sometime the source node suspecting the node 3 is the sinkhole node and displaying. There are many ways to avoid the sinkhole attack. One of the remedies for sinkhole is given below.

Figure 4 shows the remedy for the sinkhole node, the source node follows the remedy [Routing Algorithm], i.e., in each stage all the source nodes getting the next neighbor node by applying the relation Equation 1:

$$T_{AB} = \frac{(R-d)}{V} \quad (R > d) \tag{1}$$

It is seen from the above that ∀ Nodes A and B, node A and node B are neighbors if they are within each Other’s transmission range R. They are also called neighboring nodes. ∀ Nodes A and B, node A and node B are eighboring nodes, if the distance between them is T_{AB}, which is T_{AB} = (R-d)/V(R>d), where R is the transmission range; d is the distance between the node A and node B; V is the average speed of the node.

In sinkhole remedy it will choose the other node to send the data packets because in wireless sensor network most of the nodes are alive nodes or beacon nodes. During the remedy process for sinkhole attack when the path size will be increased, the packet loss will occur and also we will not able to monitor the intruder clearly in each region when the node will get change. So we go for newly derived approach known as LBIDS.

2.3. Routing Algorithm for Sinkhole Attack and Remedies

Description and definitions related to the sinkhole attack and routing algorithm.

Definition 1:

∀ Nodes A and B, node A and node B are neighbors if they are within each other’s transmission range R. They are also called neighboring nodes.

Definition 2:

∀ Nodes A and B, node A and node B are neighboring nodes, if the distance between them is T_{AB}, which is T_{AB} = (R-d)/V(R>d), where R is the transmission rang; d is the distance between the node A and node B; V is the average speed of the node.

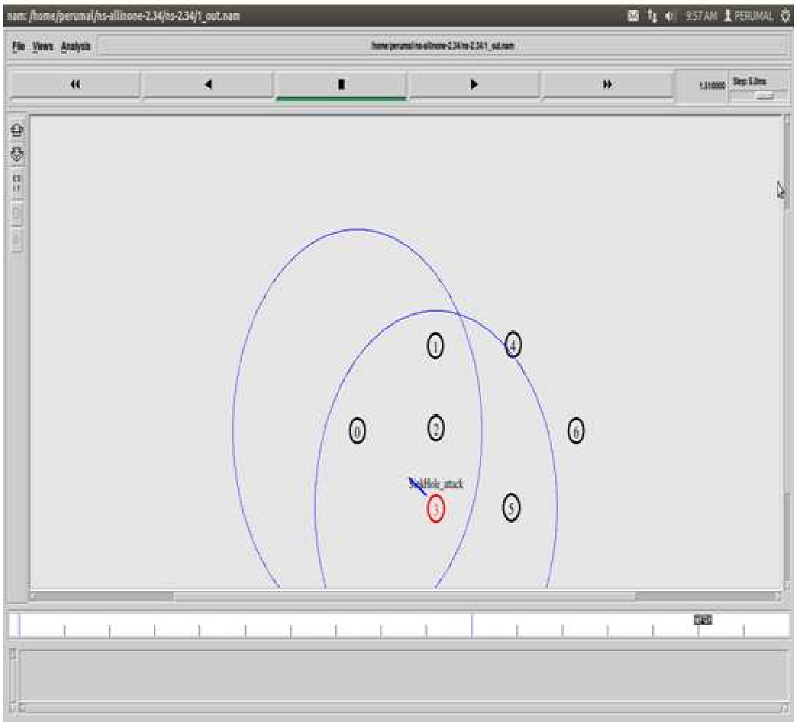
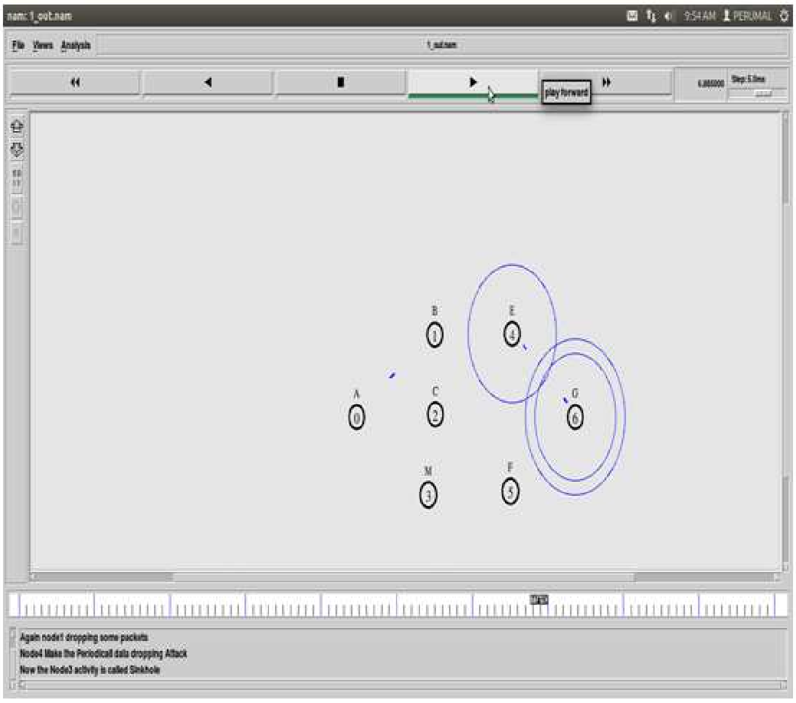

nam: /home/perumal/ns-allinone-2.34/ns-2.34/1_out.nam
File
Views
Analysis
/home/perumal/ns-allinone-2.34/ns-2.34/1_out.nam
1.510000
Step: 5.0ms
9:57 AM
PERUMAL
1
4
0
2
6
Sinkhole_attack
3
5

Fig. 3. Sinkhole node attack



```
Again node1 dropping some packets
Node4 Make the Periodicall data dropping Attack
Now the Node3 activity is called Sinkhole
```

Fig. 4. Remedy for Sinkhole attack

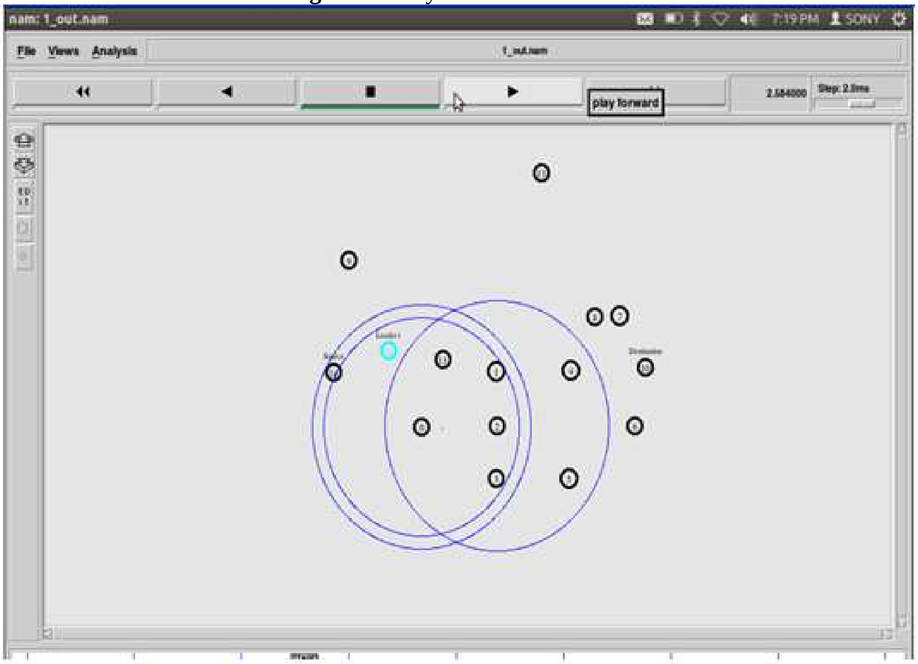
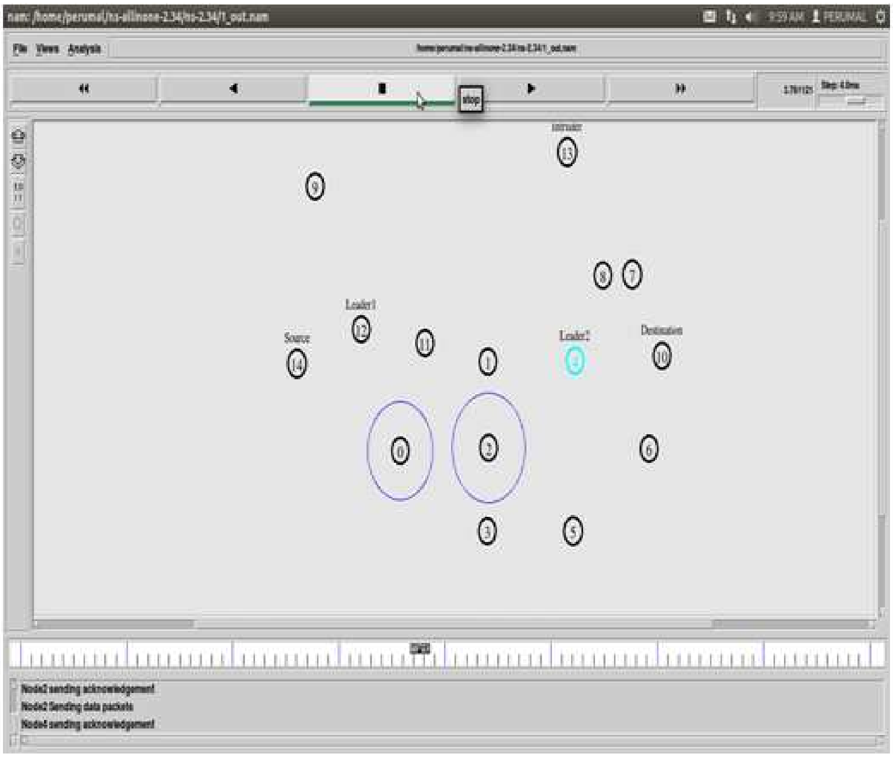


Fig. 5. Election of Leader 1



```
Node2 sending acknowledgement
Node2 Sending data packets
Node4 sending acknowledgement
```

Fig. 6. Election of Leader 2

Definition 3:

Every node has a counter, initially is set zero. Agent collects the information from one node to another. When the agent leaves the node, the counter of the node will be added one. Obviously, the number of counter indicates the frequency visited by agent and if two agents have the information of the same node (node A), the information of node A contained in the agent which has bigger counter will be updated.

Definition 4:

Each node contains ID, Program and agent packet. Here, the agent packet contains some condition parameters, such as T_{AB}, counter and so on. Agents can share the information in agent packets with other agents. These condition parameters should be updated before agents leave.

2.4. Algorithm for Check IDS

The steps to be followed for the proposed CheckIDS Algorithm are described below:

Step1: Check the connection between the node A and B. whether the T_{AB} is equal to zero start procedure, if no, then, go to step2.

Step2: Check the column, T_B of node B and find T_B is not equal to zero if T_B is equal to zero there is valid route.

Step3: Compare ID and location of the route nodes.

Step4: If the ID location exists in the information table. The route will continue if not exists then change the path. In LBIDS, leader node will check the Current ID, location of the nodes with in its region. Whenever the data is going to transfer from source node to destination node it will inform its states to the leader node. The leader scans the nodes, if the ID is wrong or the location x, y of the node current position is wrong it suggests all other nodes about that node as intruders and stop transfer the data.

2.5. Leader Election Based IDS

LEVEL 1: Node-12 is act as a Leader

The above **Fig. 5**. Shows the Leader Election Based IDS in Wireless Sensor Network and it have three levels in a spare of time. Each level is nothing but a period of time where within a period how the leader is getting elected; detect the intruder in the network. From the above figure, it is seen that in the level-1, node 12 is elected as the leader due to its high energy level in the particular time. The leader node 12 will know all the information about the neighbor node. Here, 14 is the source node and 10 is the destination node. At first we send the request to the nearest node and node 0 will give response and the data packet will start to transmit through node 0 and through node 2 and reaches the destination node 10. As there is no intruder in this region, the leader remains calm.

LEVEL 2: Node-4 is act as a Leader 2

In **Fig. 6** shows the level 2, same like the previous level at the time of 40, node 4 is having the highest energy level; node 4 will be elected as a Leader 2 and the leader is very near to the node where data is getting passed. The data from the node 2 is passed through the node 4 itself. Now the node 4 starts monitoring the other nodes ID and location. No intruder is found in level 1 and 2 monitored by node 12 and node 4. The intruder is checked with the constraints explained in the proposed approach LBIDS, which always checks the ID and Location of the nodes which are very fundamental to enter into a network. Till the level 2 all the nodes which are in the Route are perfect nodes and belong to the same network.

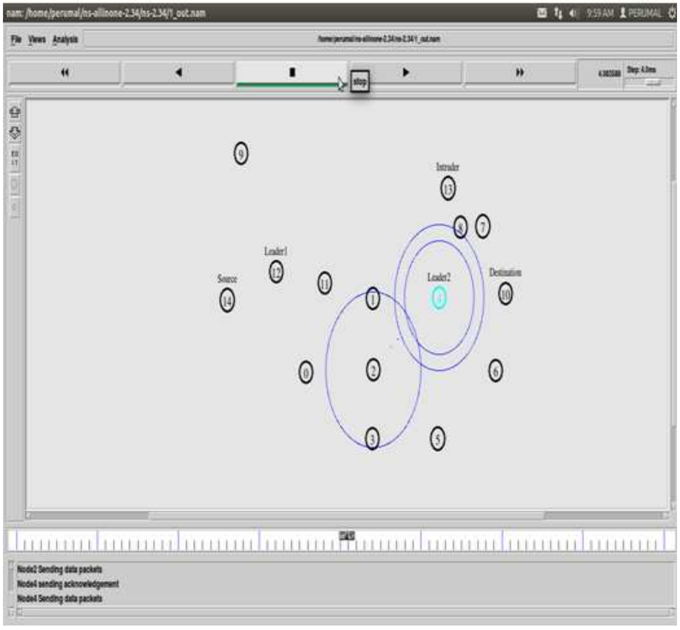
LEVEL 3: Node-7 is act as a Leader 3

In **Fig. 7** shows the level 3; at the time of 60 the node 7 is having the highest energy level. Hence, it will elect as a Leader 3. Now the node 4 is trying to pass the data to the nearest node 8. Here, we have a node 13 as unknown new node entering the network. The Leader 3 node will monitor the entire node and also the unknown node entering into the region and the leader3 finds the node 13 as abnormal node by analyzing the node ID and Location of the node. After analysis, the leader 3 declare the node 13 as an intruder and it will intimate to all other nodes in the region about the node 13.after that the node 4 which is source node stops transferring packets to the node 13 at the time of 70.

It is seen from the **Fig. 8** that the leader 3 detects the intrusion node 13 in the network.

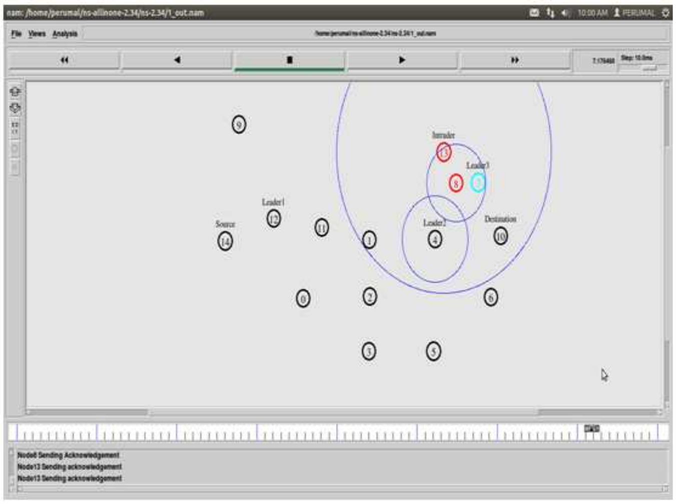
LEVEL 4: Node-13 and 8 Finds as an Intruder

In **Fig. 8**. Shows variation of number of attackers with the detected attackers for the proposed and the existing systems in the WSN environment. In the proposed, the routing protocol predicts 14 attackers out of 200 nodes in the network. It is clearly shown in the above **Table 1** that proposed approach of the total number of nodes and total number of attacks happen using LBIDS.



```
Node2 Sending data packets
Node4 sending acknowledgement
Node4 Sending data packets
```

Fig. 7. Election of Leader 3



```
Node8 Sending Acknowledgement
Node13 Sending acknowledgement
Node13 Sending acknowledgement
```

Fig. 8. Identification of intruder

3. RESULTS AND DISCUSSION

The above algorithm is implemented in NS2 with some number of nodes. In order to detect the sinkhole node in the route by applying timer or by not getting any acknowledgement from any other node in the route. Since the middle node is the sinkhole node it doesn't pass the data to the next node and source node never gets any data acknowledgement from the destination node. So it will suspect the intermediate node as the sinkhole node and it select the alternative, smallest path in the same region and transfer the data.

The performance of the proposed approach is proved by a number of iterative simulations done in Network Simulator 2, by changing the number of nodes in the network and deploying the proposed approach and compared.

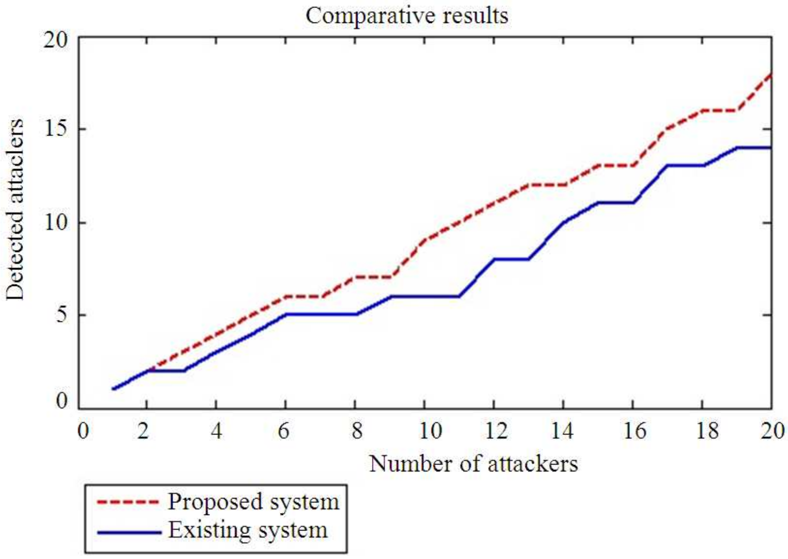


Fig. 9. Comparison of existing and proposed algorithm on detection of attacker node within the network

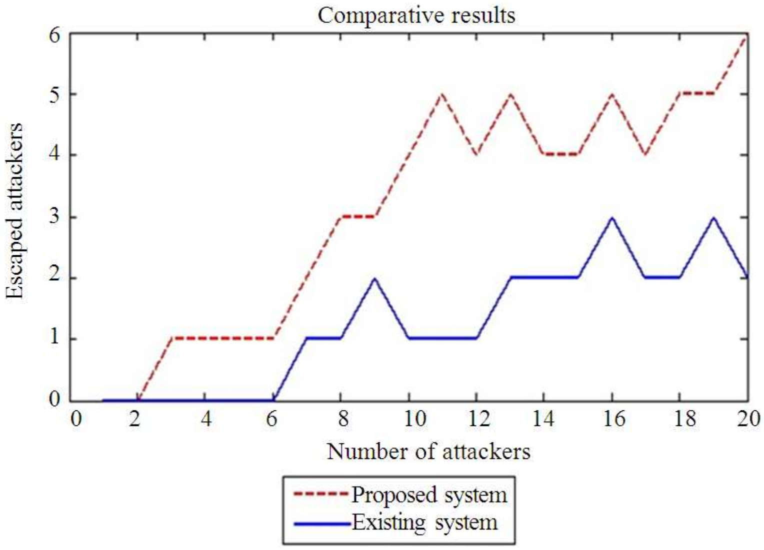


Fig. 10. Comparison of escaped attackers with attackers

The nodes in the network are grouped according to the distance from the base-station where the BS is assumed as located in the origin (0,0) in the plane. According the distance from BS in ASTC method-all silver tea cup method {(+, +), (-, +), (-,-), (+,-)} the nodes are placed. And the leader node is elected, which is located in the center of the region, so that all the nodes in the group can communicate easily and directly to the leader node. Here we have simulated our proposed algorithm by assigning one attacker for each TEN number of regular nodes and 20 attackers for the 200 nodes and are shown in **Table 1**.

The number of detected attackers in the existing system as well as in the proposed LBIDS based protocol is given in **Table 2**. From the **Table 1**, there are 20 attackers available for the network of 200 nodes. For the existing case without using LBIDS, the protocol can identify only 14 attackers out of 20. But in the case of proposed algorithm using LBIDS, a total of 18 attackers can be identified.

Table 1. Regular node and Attacker node

No. of nodes	No. of Attacker
10	1
20	2
30	3
40	4
50	5
60	6
70	7
80	8
90	9
100	10
110	11
120	12
130	13
140	14
150	15
160	16
170	17
180	18
190	19
200	20

Table 2. No of detected attacker in the WSN for the proposed and existing

Proposed	Existing
1	1
2	2
3	2
4	3
5	4
6	5
6	5
7	5
7	6
9	6
10	6
11	8
11	8
12	10
13	11
13	11
15	13
16	13
16	14
18	14

The identifying of attackers in the existing system as well as proposed system is shown in **Table 2**.

Figure 9 shows the comparison between the existing and proposed algorithm on detection of attacker node within the network in the WSN environment. It is seen from the figure that the existing system, the routing protocol predicts only 14 attackers out of 200 nodes in the network. But in proposed protocol based on LBIDS, predict 18 attackers for a network consist of 200 nodes.

Table 3. Shows no of escaped attacker

Proposed	Existing
0	0
0	0
0	1
0	1
0	1
0	1
1	2
1	3
2	3
1	4
1	5
1	4
2	5
2	4
2	4
3	5
2	4
2	5
3	5
2	6

3.1. Performance by Number of Escaped Attackers

Table 3 shows the comparison of escaped attacker from the existing as well as from proposed system. In the existing system out of 20 attackers, 6 attackers are escaped. But in the proposed system when we are using the LBIDS for a 20 attackers, only 2 attackers are escaped as shown in the following **Table 3**.

Figure 10 shows the escaped attacker in the existing system and the proposed system. In the proposed protocol for a network of 60 nodes, no escaped attacker can be found but for the network of 200 nodes only 2 escaped attackers are found. In the existing system for a network of 60 nodes, 1 escaped attacker is found, but in the case of a network with 200 nodes, 6 escaped attackers are found. Number of leader nodes and the attacker nodes are depending upon the IDS which are deploying in the network. Since all the leaders are acting as a monitoring nodes, the number of attacker getting reduced.

4. CONCLUSION

In this study, we have described some of the previous efforts to measure IDS and we have outlined some of the difficulties that have been encountered. Hence we have proposed the Leader Based Intrusion Detection System that detects the sinkhole threat attackers inside the Wireless Sensor Networks. In our approach we improved the performance of the system by means of energy efficiency and intrusion detection rate. In future, we will study some efficient ways to improve the performance of the system by characterizing the node attackers in WSN's.

4.1. Future Enhancement

In future the leader election mechanism can be improved in the way of energy efficiency, where the group nodes are treated as cluster and the leader is the Cluster Head (CH) elected by the energy value, where the maximum energy node is taken as the CH and the IDS is deployed in the CH. Where the functionality of the current work and the future work are same and the scope of the work is improving the energy of the network and lifetime of the network.

5. REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2011. A survey on sensor networks. IEEE Commun. Mag., 40: 102-114. DOI: 10.1109/MCOM.2002.1024422

Anastasi, G., M. Coti, M.D. Frrancesco and A. Passarella, 2009. Energy conservation in wireless sensor networks: A survey. Ad Hoc Netw., 7: 537-568. DOI: 10.1016/j.adhoc.2008.06.003

Anjum, F. and P. Mouchtaris, 2007. Security for Wireless Adhoc Networks. 1st Edn., John Wiley and Sons, Hoboken, ISBN-10: 0470118466, pp: 316.

Chang, Y.C. and J.P. Sheu, 2009. An energy conservation MAC protocol in wireless sensor networks. Wireless Personal Commun., 48: 261-276. DOI: 10.1007/s11277-008-9521-2

Edith, C.H., N. Jiangchuan, L. Michael, R. Lyu and E.C.H. Ngai, 2007. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Comput. Commun., 30: 2353-2364. DOI: 10.1016/j.comcom.2007.04.025

EI-Khatib, K., 2010. Impact of feature reduction on the efficiency of wireless intrusion detection systems. IEEE Trans. Parallel Distrib. Syst., 21: 1143-1149. DOI: 10.1109/TPDS.2009.142

Fessant, F.L., A. Papadimitriou, A.C. Viana, C. Sengul and E. Palomar, 2011. A Sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Comput. Commun., 35: 234-248. DOI: 10.1016/j.comcom.2011.09.005

Kalita, H.K. and A. Kar, 2009. Wireless sensor network security analysis. Int. J. Next-Generation Netw., 1: 1-10.

Li, G., J. He and Y. Fu, 2008. Group-based intrusion detection system in wireless sensor networks. Comput. Commun., 31: 4324-4332. DOI: 10.1016/j.comcom.2008.06.020

Mohammed, N., H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, 2011. Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE Trans. Dependable Secure Comput., 8: 89-103. DOI: 10.1109/TDSC.2009.22

Perrig, A., J. Stankovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57. DOI: 10.1145/990680.990707

Rezaei, Z. and S. Mobininejad, 2012. Energy saving in wireless sensor networks. Int. J. Comput. Sci. Eng. Survey, 3: 23-37. DOI: 10.5121/ijcses.2012.310

Rong, C.M., S. Eggen and H.B. Cheng, 2011. A novel intrusion detection algorithm for wireless sensor networks. Proceedigns of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Feb. 28-Mar. 3, IEEE Xplore Press, Chennai, pp: 1-7. DOI: 10.1109/WIRELESSVITAE.2011.5940938

Sharma, K. and M.K. Ghose, 2010. Wireless sensor networks: An overview on its security threats. IJCA Special Issues "Mobile Ad-hoc Netw".

Werner-Allen, G., K. Lorincz, M. Welsh, O. Arcillo and J. Johnson *et al*., 2006. Deploying a wireless sensor network on an active volcano. IEEE Int. Comput., 10: 18-25. DOI: 10.1109/MIC.2006.26

Zhao, F. and L.J. Guibas, 2004. Wireless Sensor Networks-An Information Processing Approach Elsevier. 1st Edn., Morgan Kaufmann, San Francisco, ISBN-10: 1558609148, pp: 358.