Black hole detection using improved Hierarchical Detection algorithm in MANET

[1]Ramakanth Reddy Malladi, [2]Prof.A.Govardhan

[1]Research Scholar, Achrya Nagarjuna University, Andhra Pradesh, India.
[2]Professor & Rector, JNTUH, Telangana, India.

Abstract: **In they recommended an intrusion detection mechanism to detect the black hole attack which is vitality inefficient. We proposed an intrusion detection system which is vitality efficient, to secure network nodes from black hole attacks. Our approach is simple and is based on the exchange of control packets between sensor nodes and base station. Therefore, BS takes the part of monitor node to detect any black hole attack. Our proposal mitigates significantly the effect of the black hole attack. Simulation effects show that the recommended methodology has a improved performance in the IDs in terms of security and vitality consumption. As a future work, sensor nodes can also be simulated as black hole nodes along with the CH and an efficient mechanism can be devised.**

Keywords**: Black hole attack, intrusion detection, security, sensor nodes.**

I. INTRODUCTION

A WSN comprises of spatially dispersed sensor nodes, which are unified deprived of the use of any wires [1, 2]. In a WSN, sensor nodes intellect the situation and use their communication modules in order to transmit the sensed data over wireless channels to other nodes and to a selected sink point, denoted to as the Base Station (BS). BS gathers the data transmitted to it in order to act either as a administrative control processor or as an access point for a human interface or even as a gateway to further networks [3,4].Through the cooperative use of a great number of sensor nodes, a WSN is capable to accomplish simultaneous data acquisition of present conditions at several points of interest situated over widespread areas. Despite of the advantages of a WSN their use is severely restrained by the vitality limitations posed by the sensors.

The vitality disbursement of the sensor nodes arises during wireless communication, environment sensing and data processing. Therefore, power conservation is the main criteria for many routing protocols. Since a large number of protocols developed for routing in wired networks follow the achievement of a good Quality of Servic, they are not practically feasible for application in WSNs. Maximum number of the protocols makes use of clusters so as to offer vitality competence and to extend the lifetime of the network. A WSN is also exposed to several attacks; therefore security is a significant factor in the deployment of WSNs. However, sensor nodes possess restricted memory, power, computational ability, and transmission range. So when developing security algorithms the restricted resources have to be considered.

Due to the specific characteristics, Wireless Sensor Networks are severely unsafe and are open to malicious attacks. One of the most malicious threats to WSN is in the form of black hole attack that target the routing protocols. This genre of attacks can have a very serious impact on hierarchical routing protocols. A variety of security solutions have been put forth to safeguard WSNs from black hole attacks. However, a majority of the solutions are cumbersome and vitality inefficient. In this paper an improvised hierarchical vitality efficient intrusion detection system is proposed, to protect sensor Network from black hole attacks. Our proposed approach is simple and is based on exchange of control packets between sensor node and base station. The results show that our proposed algorithm is effective in detecting and preventing efficiently the
black hole attacks.

The attacks which are a threat to the network layer are routing attacks. These malicious attacks happen while routing messages. One of the routing attacks is black hole attack. One of the most devastating attacks that aim for the cluster heads is the black hole attack. A malicious node can be selected as cluster head, and absorbs all received data from its cluster members. Also, black hole attack can be created by a sinkhole attack. The adversary node can position itself in the range of sink node, and draws the complete traffic to be routed through it by presenting itself as the shortest route. Thus, the assailant absorbs any received message by rejecting and not forwarding it. Selective forwarding is a particular type of black hole attack. Instead rejecting all received packets, adversary node selects randomly or maliciously packets that will be rejected.

II. RELATED WORK

The Black hole attack has been addressed by several researches in wireless sensor network. In this unit we present a survey of these researches. To detect a single as well as a group of Black Hole attacks, Karakehayov Z. has recommended a technique with the aid of two broadcast messages; MISS and SAMBA to recognize Black Hole nodes. This technique works well for different levels of security.D S. et al. [9] have suggested an innovative approach to progress data distribution in the occurrence of a Black Hole attack that uses concept of several base stations organized in WSN by means of mobile agent. The purpose of several base stations is to certify high packet distribution in the presence of attack. Atakli I. M., Hu and H. et al.[10] have developed a Weighted Trust Evaluation mechanism for ordered sensor network architecture. This mechanism is applied to Cluster Head at each sequence to detect unspecified activity.

Virmani D. et. al. [11] recommended an exponential trust based mechanism to identify malicious node.Trust factor droops down exponentially with each successive packet being dropped which aids in sensing the adversary. Janani C et. al. [12] introduced TARF a strong trust aware routing framework for WSNs mainly protects a WSN against the replay attacks and also, demonstrated to be potent against several strong attacks. A hierarchical secure routing protocol called HSRBH has been put forth in [14] to identify and discover a secure path against black hole attacks. Symmetric key cryptography is used to determine a innocuous route against black hole attacks. Most of black hole attacks except the group leader collude with other nodes to mark black hole attack. So, it is much quicker in identifying the black hole attacks, and the message overhead is very low.

III. METHODOLOGY

Our simple idea is to detect and prevent black hole attacks, by implementing an intrusion detection system based on a simple strategy. In our proposal, each sensor node sends a control packet to one of agents and the Cluster Head among them at the end of transmission phase. Each control packet contains the node identifier [id], and the number of packets sent to CH. Then, base station compares the Nbrpk of each node with the amount of packets received from its agent and the CH. The mismatch in Nbrpk allows base station to detect an eventual black hole attack.

In this case, base station will broadcast an alarm packet to all network nodes. The alarm packet contains identifier of black hole node. All sensor nodes maintain a black hole table, which contains identifiers of detected black hole nodes. Then, each sensor node checks its black hole table before the selection of its next CH, which prevents that attacker node from being selected one more time as Cluster Head. The node with the maximum vitality backup and neighbor to more number of nodes will be selected as a second CH.

3.1 Phases

1. Selection of Agent Node
2. Determination of Neighborhood Nodes
3. Choosing a Cluster Head
4. Transmission of Control Packets
5. Detection and Elimination of Black Hole Node

3.2 Selection of Agent Node

The agent node is selected centered on its aloofness to the base station. The agent with least distance to the base station is selected or preferred than agent with maximum distance to the base station. The foremost aim of our work is to conserve vitality resources. The vitalityconsumed by the node to transfer a packet depends on the distance. Hence we conserve large amount of vitality by minimizing the distance between the agent and base station.

3.3 Determination of Neighborhood Nodes

The neighborhood nodes are designated based on the coverage. The nodes are considered to be the neighbor to each other when they are in a particular coverage area or range to the other.

3.4 Choosing a Cluster Head

Cluster Head is nominated based on the residual vitality. The node with maximum residual vitality and neighbor to more number of nodes is nominated as the Cluster Head. The role of cluster head is vitality consuming since it is continuously switched on and in control for the far-off transmissions. If a fixed node has this role, it would lose its vitalityrapidly, and after it died, all its adherents would be “headless” and so useless. If the Cluster Head is detected as a black hole node then the Cluster Head is discarded.

3.5 Transmission of Control Packets

First the control packets are transmitted from all the nodes to the Head of the Cluster and the agent node. Then the agent node and Cluster Head will send those control packets to the base station for detection of black hole attack.

3.6 Detection and Elimination of Black Hole Node

When the packets are sent from the agent and Head of the Cluster to the base station the comparison of number of packets is done by base station. If there is a black hole attack then number of packets sent by the agent and the Cluster Head will differ. In case of absence of black hole then number of packets sent by the agent and the number of packets sent by the Cluster Head will be equal. In case of detection of black hole node, the CH is discarded from the network. fig 3.1 shows the scenario of proposed work.

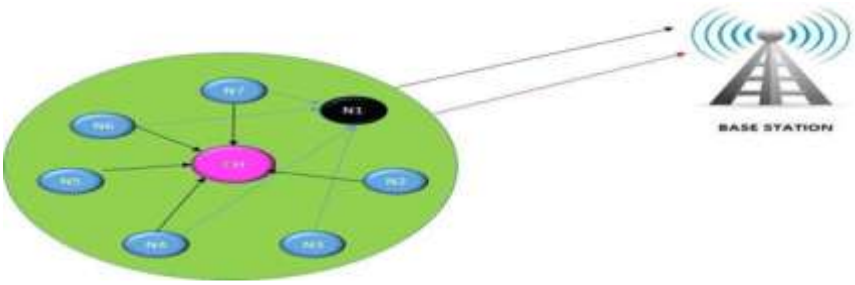


Figure 1 Scenario of proposed work

The proposed model is explained in the flow chart as shown in fig 3.2

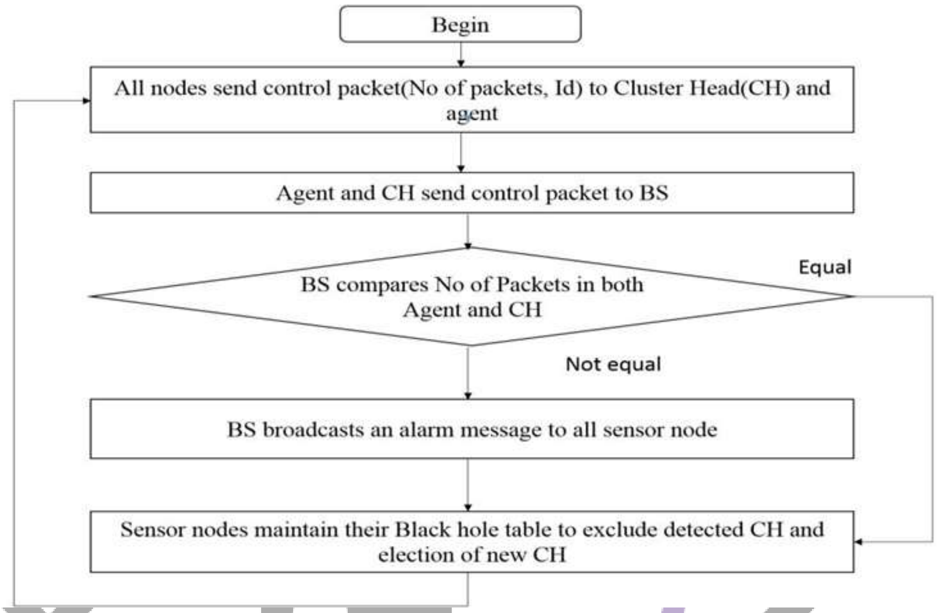

Begin
All nodes send control packet(No of packets, Id) to Cluster Head(CH) and agent
Agent and CH send control packet to BS
BS compares No of Packets in both Agent and CH
Equal
Not equal
BS broadcasts an alarm message to all sensor node
Sensor nodes maintain their Black hole table to exclude detected CH and election of new CH

Figure 2 Flow Chart of Proposed Algorithm

3.7 Vitality Calculation

A maintask in constructing a WSN is to enhance the network life time. Nodes in a WSN are usually highly vitality-constrained and estimated to operate for longer periods. Accurate prediction of sensor network lifetime requires an accurate vitalityingesting model. In this paper, a comprehensive vitality model is adopted that includes sensing, logging and switching energies apart from the processing and communication vitality values. The network set up shown in consumes vitality by transmitting packets, receiving packets, overhearing, switching vitality, and sensor logging. The nature of the sensor nodes determine the processes involved in consuming vitality. For example, the sink node need not involve in overhearing and hence, it does not consume vitality in overhearing of packets from neighbouring nodes.

Sensor logging consumes vitality used for reading „*b*" bit packet data and writing it into memory. Sensor logging vitality consumption for a node per round is evaluated by [15], [16]:

$$E_{loggn}(b)=E_{write}+E_{read}=\frac{b\times V_{sup}(I_{write}\,T_{write}+I_{read}\,T_{read})}{8}$$ (1)

Where , $I_{read}$is vitality consumption for writing data, E_{read} is vitality consumption for reading „*b*" bit packet data, $I_{write}$and are current for writing and reading 1 byte data. Communication of neighboring sensor nodes is enabled by a sensor radio. Vitality dissipation by a sensor node can be attributed to transmitting and receiving data. According to [s], the vitality dissipation due to transmitting „*b*" bit packet, in a distance d_{ij} from sensor node to the neighbor is given by (2)

where, E_{elec} is the vitality dissipated to transmit or receive electronics, E_{amp} is the vitality dissipated by the power amplifier, and n is the distance-based path-loss exponent. Here, free space spading is assumed and so n takes the value 2.Vitality dissipation due to receiving „ b, bit packet from the sensor node is given by:

$$E_2=h_4\times b\times V_{sup}(I_{write}\times T_{write}+I_{read}\times T_{read})$$ (2)

The switching vitality component [10] is the vitality consumed for switching the radio state between states, including normal, power down and idle modes. The following equation determines the vitality consumed for switching the radio from sleep mode to active mode:

$$E_{switch} = \frac{(I_{active} - I_{\alpha}) \times T_{\alpha} + V}{2} \tag{3}$$

$$E_6 = T_{CH} \times V_{sup}[C_{CH} \times I_A + (1 - C_{CH})I_S] \tag{4}$$

where T_{α} is the current draw of the radio in active mode, I_{α} is the current draw of the radio in sleep mode α, and is the time required for the radio to go from sleep mode to active mode.

In the vitality model [16] that incorporates overhearing, the total vitality expenditure due to a transmission from node to is given by,

$t \quad f$

$$E_{ij}(b, d_{ij}) = b \times E_{elec} + b d_{ij}^{\varepsilon} \times E_{amp} + N_{ij}^{(q)} \times E_{rxn}(b)$$

(5)

Hence, the total vitality consumed by a node is given by vitality consumed by each and every node, E_{mcu} is the vitality consumed due to processing of packets, E_{switch} is the switching vitality.

The total vitality consumed by the Cluster, CH$_j$ per round is given by equation (6)

$$E_{CH}(j) = E_1 + E_2 + E_3 + E_4 + E_5 + E_6 + E_7 \tag{6}$$

where,

$$E_1 = h_3 \times b \times V_{sup} \times I_{sense} \times T_{sense}$$

stands for vitality due to sensing,

is the data logging vitality,

$$E_3 = h_1 \times b_1 \times N_{cyc} \times C_{avg} \times V_{sup}^2 (n_j + 1) \tag{7}$$

is the vitality spent due to switching,

$$E_4 = h_1 \times b_1 \times V_{sup}\left(I_0 \times e^{(V_{sup}/N_p VT)}\right)\left({}^{N_{cyc}}\!/_{f}\right)(n_j + 1) \tag{8}$$

Stands for the leakage vitality

$$E_5 = h_2 \times b_2 \times (1 + \gamma) \times d_j^n \times E_{amp} \tag{9}$$

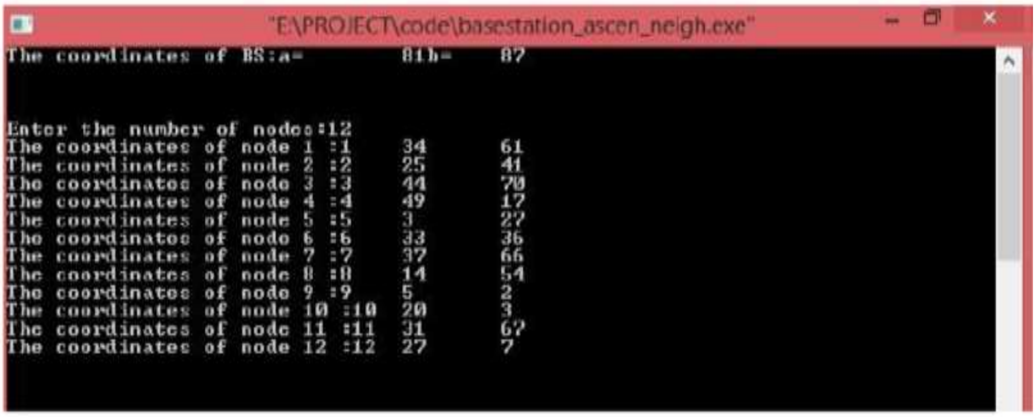
is the transmitting vitality consumed by the nodes to the CH, is the vitality spent during transient

$$E_7 = E_{actu} \times N_{actu} \tag{10}$$

is the actuation vitality.

VI. EXPERIMENTAL RESULTS AND COMPARISONS

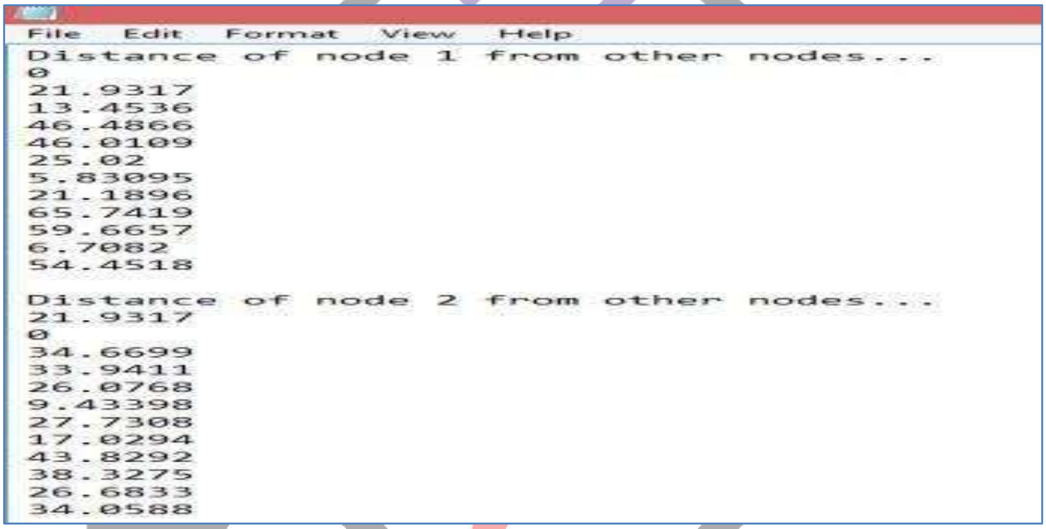
We assume a network of 12 nodes to recognize the black hole attack. The simulation is done in c++.The vitality spent for transmission, reception of packets is also calculated



```
The coordinates of BS:a=        81b=     87


Enter the number of nodes:12
The coordinates of node 1 :1    34      61
The coordinates of node 2 :2    25      41
The coordinates of node 3 :3    44      70
The coordinates of node 4 :4    49      17
The coordinates of node 5 :5    3       27
The coordinates of node 6 :6    33      36
The coordinates of node 7 :7    37      66
The coordinates of node 8 :8    14      54
The coordinates of node 9 :9    5       2
The coordinates of node 10 :10  20      3
The coordinates of node 11 :11  31      67
The coordinates of node 12 :12  27      7
```

Figure 3 Coordinate Generation for all the Nodes

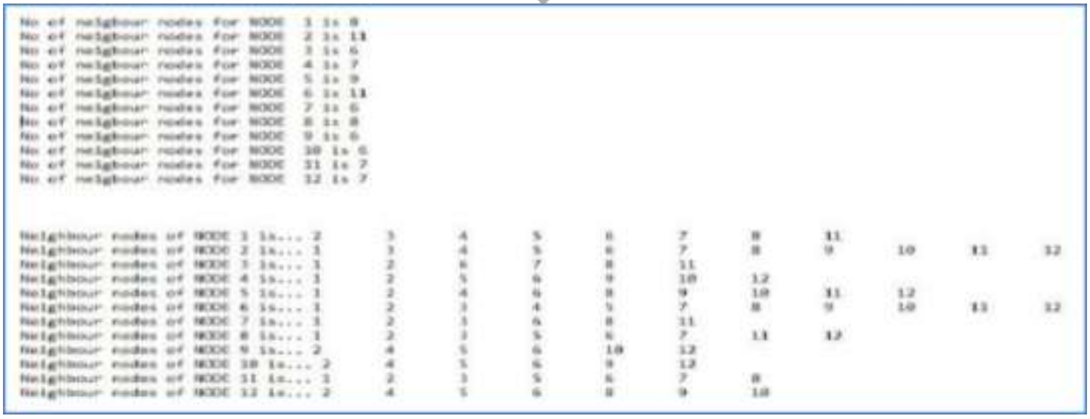
The neighborhood node detection phase includes two steps one is coordinate generation and the distance calculation. Coordinate generation includes the generation of the coordinates for each and every node in the network. Our simulation results produce coordinates for all the nodes.Fig3.1.shows the coordinates for a network of 12 nodes. Distance calculation is an important metric in the neighbourhood detection. The nodes which are in a particular coverage are said to be the neighbour nodes. Fig 3.2 shows the distance of each node from other nodes. This distance calculation of each node to other nodes is helpful to find the neighbourhood nodes.



```
Distance of node 1 from other nodes...
0
21.9317
13.4536
46.4866
46.0109
25.02
5.83095
21.1896
65.7419
59.6657
6.7082
54.4518

Distance of node 2 from other nodes...
21.9317
0
34.6699
33.9411
26.0768
9.43398
27.7308
17.0294
43.8292
38.3275
26.6833
34.0588
```

Figure 4 Distance calculation of neighbourhood nodes

The Fig 3.2 shows the number of neighbour nodes to a particular node and indicate their node name along with them.from the it is known that the number of neighbourhood nodes for node 1 is 8.

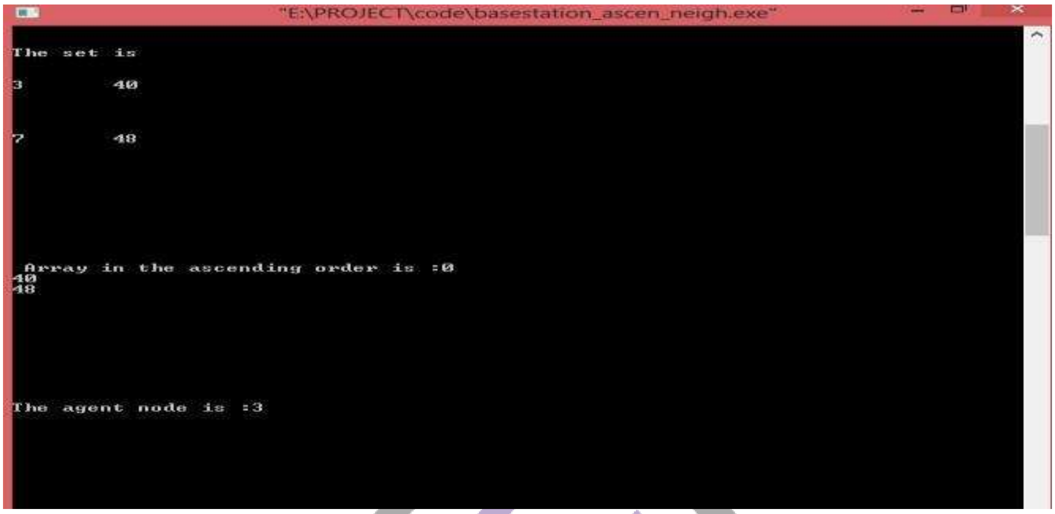


```
No of neigbour nodes for NODE  1 is 8
No of neigbour nodes for NODE  2 is 11
No of neigbour nodes for NODE  3 is 6
No of neigbour nodes for NODE  4 is 7
No of neigbour nodes for NODE  5 is 9
No of neigbour nodes for NODE  6 is 11
No of neigbour nodes for NODE  7 is 6
No of neigbour nodes for NODE  8 is 8
No of neigbour nodes for NODE  9 is 6
No of neigbour nodes for NODE  10 is 6
No of neigbour nodes for NODE  11 is 7
No of neigbour nodes for NODE  12 is 7


Neighbour nodes of NODE 1 is... 2     3     4     5     6     7     8     11
Neighbour nodes of NODE 2 is... 1     3     4     5     6     7     8     9     10    11    12
Neighbour nodes of NODE 3 is... 1     2     6     7     8     11
Neighbour nodes of NODE 4 is... 1     2     5     6     9     10    12
Neighbour nodes of NODE 5 is... 1     2     4     6     8     9     10    11    12
Neighbour nodes of NODE 6 is... 1     2     3     4     5     7     8     9     10    11    12
Neighbour nodes of NODE 7 is... 1     2     3     6     8     11
Neighbour nodes of NODE 8 is... 1     2     3     5     6     7     11    12
Neighbour nodes of NODE 9 is... 2     4     5     6     10    12
Neighbour nodes of NODE 10 is... 2    4     5     6     9     12
Neighbour nodes of NODE 11 is... 1    2     3     5     6     7     8
Neighbour nodes of NODE 12 is... 2    4     5     6     8     9     10
```

Figure 5 Neighborhood node detection

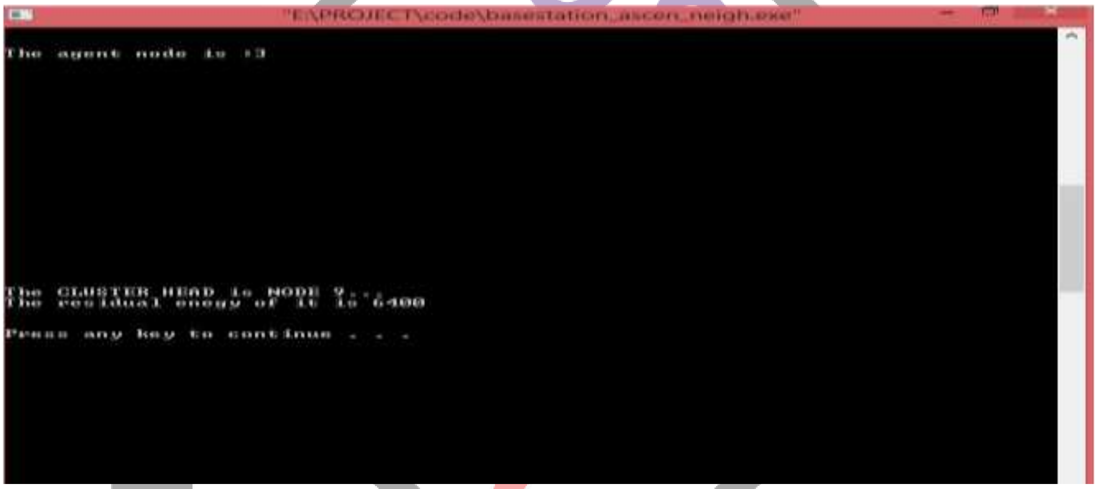
4.1 Selection Of Agent Node

The selection of agent node phase includes the distance calculation and comparison. The agent node selection will be centered on their aloofness to the base station. Hence it is the first and foremost reason to calculate the distance between each and every node and the base station.



```
The set is

3         40


7         48





 Array in the ascending order is :0
40
48




The agent node is :3
```

Figure 6 Comparison



```
The agent node is :3








The CLUSTER HEAD is NODE 9...
The residual enegy of it is 6400

Press any key to continue . . .
```

Figure 7 Cluster Head Detection

The Head of the Cluster is elected based on the residual vitality. The node with maximum residual vitality and the node which is neighbor to more number of nodes is considered to be the Cluster Head.

4.2 Vitality consumption

The vitality required for transmission, reception of packets is calculated for all the nodes and the Cluster Head. The Fig 1.8 shows the result of comparing both existing algorithm and proposed algorithm for different number of nodes. It is proved that the proposed algorithm provides a large amount of vitality consumption. Hence our proposed work is said to be vitality efficient.

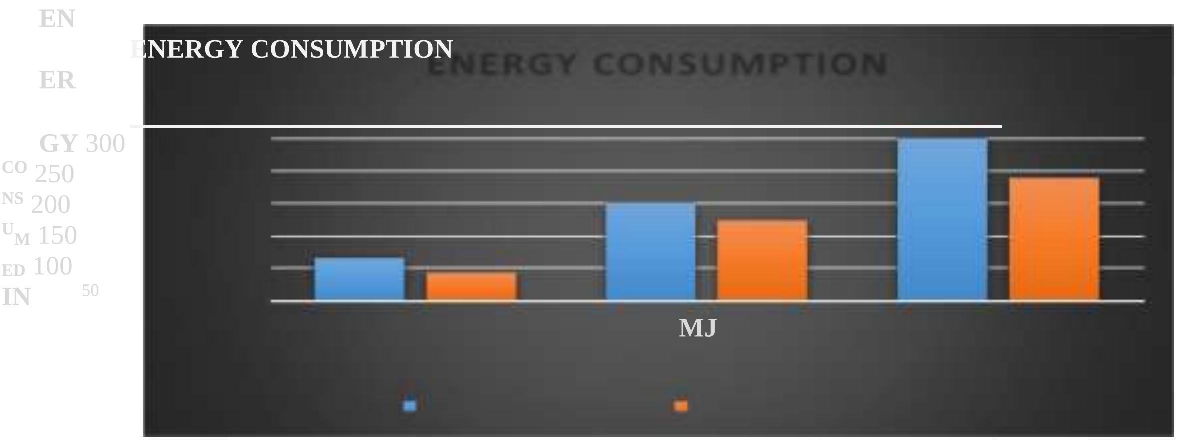


Figure 8. Vitality Consumed for Different Number of Nodes

V. CONCLUSION

In they recommended an intrusion detection mechanism to detect the black hole attack which is vitality inefficient. We proposed an intrusion detection system which is vitality efficient, to secure network nodes from black hole attacks. Our approach is simple and is based on the exchange of control packets between sensor nodes and base station. Therefore, BS takes the part of monitor node to detect any black hole attack. Our proposal mitigates significantly the effect of the black hole attack. Simulation effects show that the recommended methodology has a improved performance in the IDS in terms of security and vitality consumption. As a future work, sensor nodes can also be simulated as black hole nodes along with the CH and an efficient mechanism can be devised.

REFERENCES

[1] A. Mehran, and W. Tadeuz, "A review of routing protocols for mobile ad hoc networks", International Journal on Ad hoc Networks, Vol. 2, No.1, pp.1–22, 2004.

[2] D. B. Johnson, D. A. Maltz, and C. Y. Hu, "The dynamic source routing protocol for mobile ad-hoc network (DSR)", IETF Internet Draft, 2004.

[3] R. K. Bar, J. K. Mandal, and M. Singh, "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", International Conference on Computational Intelligence: Modeling Techniques and Applications, India, pp. 530-537, 2013.

[4] H. Deng, P. Agarwal, "Routing security in wireless ad hoc networks", IEEE Communication Magzine, Vol. 40, No. 10, pp. 70–75, 2002.

[5] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks", In: ICPP Workshops, pp. 73-79, 2005.

[6] S. Dokurer, Y. Erten, and C. Erkin, "Performance analysis of ad-hoc networks under black hole attacks" In: Proc. of the IEEE South-east Conference, pp. 148–53, 2007.

[7] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of black hole attack in MANET", In: Proc. of the international conference on

[8] C. Chao, and T. Yuh, "A context adaptive intrusion detection system for MANET', international journal on Computer Communications, Vol. 34, No. 4, pp. 310–318, 2011.

[9] M. Mohanapriya, and L. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", International Journal on computers and electrical engineering, Vol. 40, No. 2, pp. 530-538, 2014, Elsevier.

[10] Y. Yao, L. Guo, X. Wang, and C. Liu, "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks", IEEE Journal on Computer Network, Vol. 5, No. 4, pp. 1460-1469, 2010.

[11] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks" International Journal in Parallel Distributed Computer networks, Vol. 67, No. 11, pp. 1218–1230, 2007, Elsevier.

[12] X. Gao and W. Chen, "A novel gray-hole attack detection scheme for mobile ad-hoc networks". In: International Conference on network and parallel computing workshops, , pp. 209–14, 2007.