IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 23-31
www.iosrjournals.org

The Novel to Preventing Black Hole Attack in Wireless Sensor NetworkUsing Hidden Markov Model

J. Kolangiappan1 and A. Senthilkumar2

[1]*Ph.D., Research Scholar, Department of Computer Science, Periyar University, Salem*
[2]*Assistant Professor, Department of Computer Science, Arignar Anna Government Arts College, Namakkal*

***Abstract**: Secure routing is a difficult task because of the limited nature of wireless sensor network resources. This paper provides a Hidden Markov Model solution to identify malicious nodes in wireless sensor networks through prevention of black hole attack. Our proposed approach based on a new routing algorithm which analyses shortest pathin order to avoid malicious node path. Our results demonstrate the success and the efficiency of our proposed routing algorithm.*

***Keywords**: WSN; HMM; Black Hole; Malicious; Shortest path;*

I. Introduction

A sensor network is a compound, of sensing, processing, communication ability to observe and react to events ina specified environment. WSN is usually composed of tens to thousands of nodes. Which collect process and transmit cooperatively information to a central location [1].

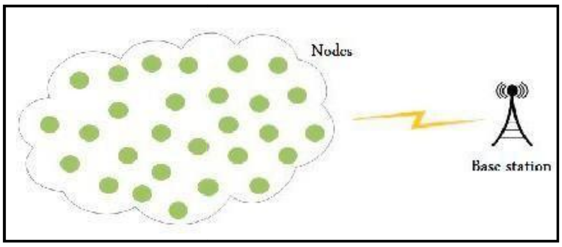


Fig. 1. Wireless sensor network

WSN technology offers many advantages compared to conventional networking solutions such as reducing costs, reliability, scalability, flexibility, accuracy and ease of deployment. The rapid Advance of technology makes the sensors smaller and cheaper while billions of them are being deployed in different applications. Some of the potential applications domains are military, environment, healthcare and security [2]. The design of such a network is influenced by many factors such as: fault production costs, operating environment, sensor network topology, hardware constraints, transmission media and power consumption. These factors are used as a guideline to design protocols and algorithms for manufacturing efficient sensor network [3-4-5].

Moreover, security in WSNs is an important challenge, especially if they have critical tasks. Sensor networks are deployed in applications where they interact physically with the environment, people and other objects making them more vulnerable to security threats [6]. The objective of security in WSN is to protect information and resources against attacks and misbehavior [7].

WSN can be affected by several types of attacks damaging and making the network unreliable for communication and proper working. Various attacks on network layer such as wormhole, sinkhole, selective forwarding, hello flood, false routing attacks and acknowledgement flooding have recently attracted considerable attention [8-10]. The black hole attack is one of the most severe attacks on WSNs. In this work we present our experience to detect a Black Hole attack in WSNs usingHidden Markov Model technique.

II. Black Hole Attack

Black Hole attack occurs under Dos (Denial of service) attack in the network layer of OSI Model. In this kind of attacks the malicious node forgery other nodes by announcing a shortest false route to the destination then attracts additional traffic and drops continually the packets. During data transmission the source node sends a Route REQuest (RREQ) message to all the nodes including malicious node. Given that a malicious node may become active by receiving RREQ message and replies using Route REPly (RREP) message. It attracts additional traffic by falsely claiming the shortest route to the destination [16]. This causes blocking and increasing the energy consumption in each node, leading to the formation of routing holes which disturb or stop the network functionality [17, 18].

The Fig. 2 illustrates the Black hole attack: while the source node A broadcasts an RREQ messages to discover the route for sending packets to destination node C. An RREQ broadcast from node A is received by neighboring nodes B, D and the malicious node E. The RREP message sent by the malicious attacker node E is the first message reaching the source node. This last updates its routing table for the new route to the intended node destination, discarding any RREP message from other neighboring nodes including the actual node destination and starts sending the buffered data packets immediately. In the same time the Black hole node drops all coming data packets rather than forwarding [19].

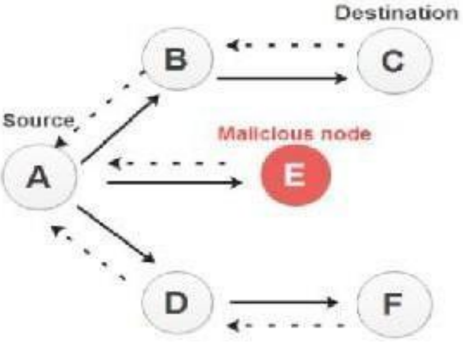


Fig. 2. Black hole Attack schematic illustration using RREQ and RREP Packet

III. System Architecture and Network Structure

An overview of our proposed attack preventing system architecture is given in this section, in which the detection mechanisms, the system framework and the algorithms used are discussed. In particular, the benefits and relevance of using Hidden Markov Model in detecting attacks.

System Architecture

The proposed system consists of a detection module and a decision-making module. The detection module analyzes all the shortest paths between the source and the destination using the Hidden Markov Model in order to find the most likelymalicious path. The decision module is used to eliminate from the routing table all the shortest path contains the untrusted node.

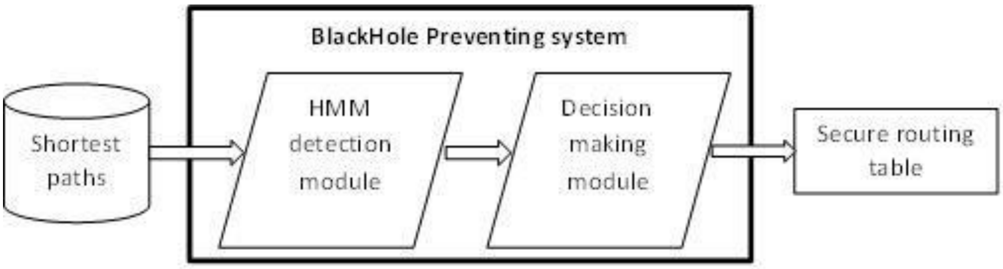


Fig. 3.The preventing system is consists of two modules. First, the Detection

module is used to filter all shortest paths .The shortest path identified as an abnormal are passed to the decision making module to find the malicious node.

The detection module is based on HMM in order to detect the Black Hole attack. A Hidden Markov Model (HMM) [20,21] is a statistical Markov model in which the modeled system is supposed to be a Markov process with unobserved (hidden) states S and sequence of the observation V. An HMM λ is defined by a set of N states, K observation symbols and tree probabilistic matrices λ = {Π, A, B}, where A is NxN transition matrix, storing the probability of state j following state I and B is MxN observation matrix, storing the probability of observation k being producedfrom the state j, independent of t.

In our system HMM was applied to model the shortest path sequence decisions made by a source node to reach destination node. We consider the number of HMM states is the set of all shortest paths weights, while the shortest paths corresponds to symbol observations V, and a number of the shortest paths decisions taken by the source node correspond to M of an observation sequence time T length. This step consists in modeling a behavior to determine the HMM parameters for the calculation of the maximum state transition probabilities via the Viterbi algorithm [22]. The Viterbi algorithm was used in this work to find the optimal state sequence of a given observation sequence M, for a T time sequence. The calculated state sequence is based on the maximum probabilities calculated at each sequence step to figure out which state is already-met at that given step.

There are two standard ways to deal this task, depending on the examples form, namely supervised and unsupervised training [23]. When the training examples contain both the inputs and outputs of a process, we will perform supervised training by associating the inputs with the observations and the outputs with the states, however if only the inputs are provided in the training data, we should use unsupervised training to guess model which will have made these observations.

In in our case we have unsupervised training so the key idea is to make an iterative improvement of the model parameters. Unsupervised learning estimates matrices A (transition matrix) and B (emission matrix) based solely on traces of activities, so there is almost no prior knowledge of the strategies defined by S. The process of unsupervisedtraining is as a follow:

- Assume an HMM with N states.
- Suppose HMM parameters λ= (A,B) (making sure they represent legaldistributions).
- Until converge (i.e. λ no longer changes) do:
- E Step: Use the forward/backward [24] procedure to determine the probability ofvarious possible state sequencesfor generating the training data.
- M Step: Use these probability estimates to re-estimate values for all of theparameters λ.

Network Structure

In this proposed model, we use a multichip flat routing topology where typically all nodes are assigned equal roles or functionality [25]. We performed the attack and its detection method on a widely used WSN routing protocol known as the Ad Hoc Distance Vector (AODV) [26] routing protocol.

AODV routing protocol is a reactive, distance vector routing protocol. AODV requests a route when needed and uses sequence numbers to avoid routing loops and indicates the "newness" of routes. An input of the routing table essentially contains the address of the destination, the address of the next node, the distance in number of hops (i.e. the number of nodes needed to reach the destination) destination sequence number, time expiration of each entry in the table. When a node needs to find a route to a destination whose input in the routing table does notexist or has expired, it broadcasts a Route Request message (RREQ) to all its neighbors. The RREQ message is broadcast through the network to reach the destination. Over its course through the network, the RREQ messages makes creating temporary records routing table for the reverse route nodes through which it passes. If the destination or a route to it is found, a road is made available by sending a Route Reply message (RREP) to the source node. The response follows the reverse path of the temporary RREQ message. In its way back to the source, RREP introduced creating entries for the destination in the intermediate nodes routing tables. Routing entries expire after a certain period of time (time-out). Note that the AODV protocol supports only symmetric links in the construction of reversepaths.

IV. Our proposed attack prevention system implementation

In this paper, we have implemented a Black Hole attack and provide its prevention technique on AODV routing protocol over WSNs. Our preventionapproach uses the shortest paths between a source and a destination as seen in figure. We assume that the source and the destination are not compromised or malicious. Our method suggests that the process of finding a malicious path integrated in the route discovery phase of routing protocols AODV.

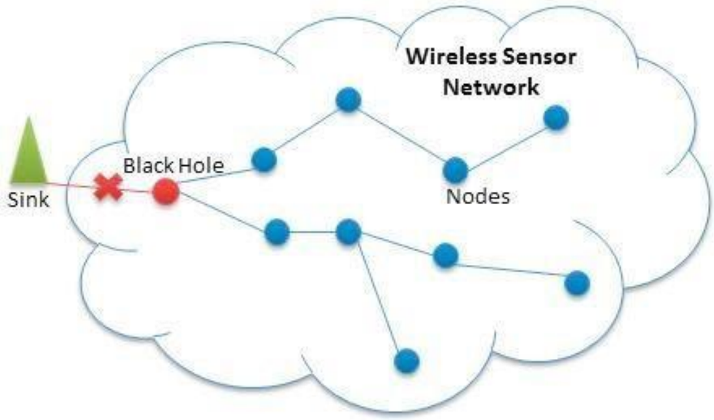
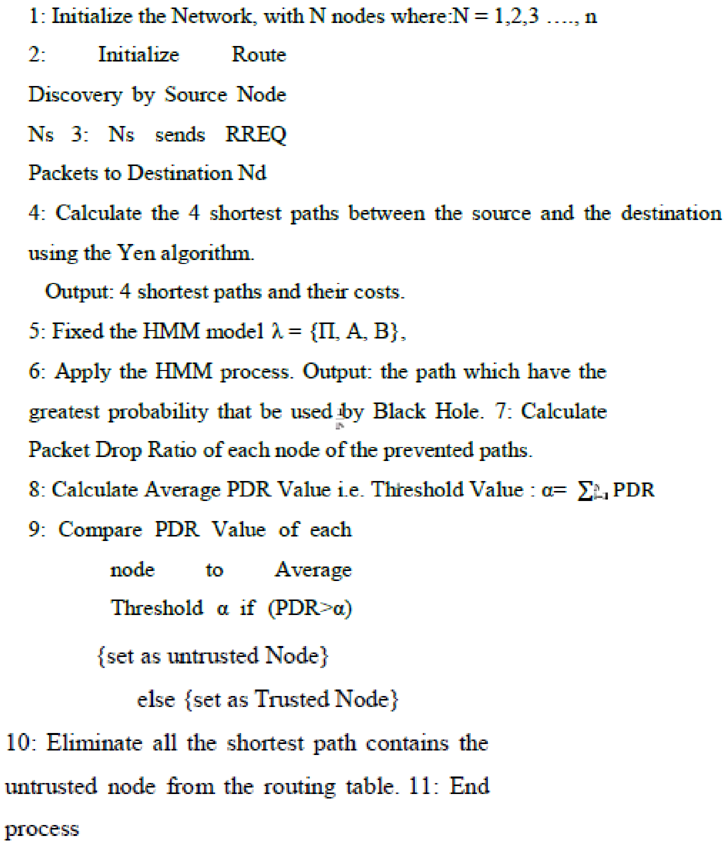


Fig. 4. Black hole Attack

The prevention of black hole attack can be assured using tree main stage (add more details). First stage, the topology marked by deploying nodes in the network. Then in the second stage our algorithm performs a calculation of 4 shortest between source and destination using the Yen algorithm [27, 28]. The black hole attack use the shortest path between source and destination as a factor to attack the network, for this reason, the weight of each path is considered as HMM state of our model. In the last stage a Viterbi algorithm is performed to calculate the path with highest probability to be malicious. Since the black hole node receives all the data packets and drop them maliciously, the nodes in selected path are packet dropped analyzed to find out the malicious node, in order to prevent all next routing paths to avoid this node.

Table 1. The proposed attack prevention algorithm The proposed attack prevention algorithm



```
1: Initialize the Network, with N nodes where:N = 1,2,3 …., n
2: Initialize Route
Discovery by Source Node
Ns 3: Ns sends RREQ
Packets to Destination Nd
4: Calculate the 4 shortest paths between the source and the destination
using the Yen algorithm.
  Output: 4 shortest paths and their costs.
5: Fixed the HMM model $\lambda = \{\Pi, A, B\}$,
6: Apply the HMM process. Output: the path which have the
greatest probability that be used by Black Hole. 7: Calculate
Packet Drop Ratio of each node of the prevented paths.
8: Calculate Average PDR Value i.e. Threshold Value : $\alpha = \sum$ PDR
9: Compare PDR Value of each
        node to Average
        Threshold $\alpha$ if (PDR>$\alpha$)
      {set as untrusted Node}
         else {set as Trusted Node}
10: Eliminate all the shortest path contains the
untrusted node from the routing table. 11: End
process
```

V. Simulation

Experimental Setup

In this work we have used NS2 (Network Simulator 2) [29] which is an object oriented, discrete event driven network simulator targeted at networking research. It provides support of TCP, routing and multicast protocol simulation on all wireless networks. In this paper Ubuntu 14.10 LTS is used as operating system.

The network model used in this work is as follows: All the sensor nodes in the network are fixed, homogeneous (All sensor nodes have the same capabilities, the same radio-transmitter devices and constrained power resources), uniformly deployed, and they have the same initial energy. The base station is fixed and located far from the sensor node. The weight model is symmetric. This means link transmission weight from node i to node j is the same than inthe opposite direction.The rest of simulation parameters are shown in Table 2.

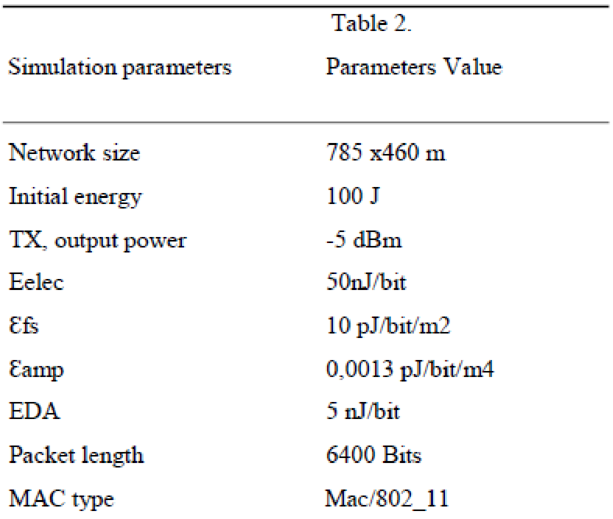


Table 2.

Simulation parameters	Parameters Value
Network size	785 x460 m
Initial energy	100 J
TX, output power	-5 dBm
Eelec	50nJ/bit
Ɛfs	10 pJ/bit/m2
Ɛamp	0,0013 pJ/bit/m4
EDA	5 nJ/bit
Packet length	6400 Bits
MAC type	Mac/802_11

Simulation results and analysis

In this section, the results obtained from simulation on various scenarios arepresented and discussed in detail.

We implemented our attack model under a network of 50 nodes in area of 785 x460m.

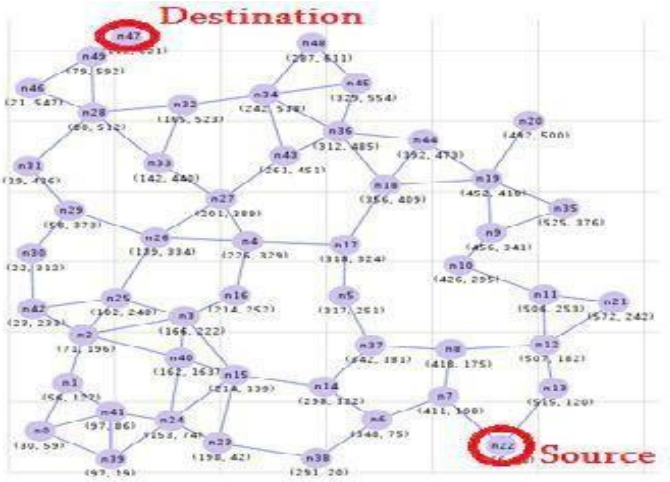


Fig. 5. The WSN topology used in our system.

Our black hole attack model is with a single malicious node. Then we evaluated the network performance while preventing attacks is established to approve our approach.

The 4 shortest paths between a source node 22 and the destination node 47, with minimal weight according to thepaths taken as indicated below:

Weight 1= 12 hop counts of Path1= {22, 7, 8, 37, 5, 17, 18, 36, 34, 32, 28, 49, 47}
Weight 2= 12 hop counts of Path2= {22, 7, 8, 37, 5, 17, 4, 27, 33, 28, 46, 49, 47}
Weight 3= 12 hop counts of Path3= {22, 7, 6, 14, 15, 3, 25, 26, 27, 33, 28, 49, 47}
Weight 4= 11 hop counts of Path4= {22, 7, 8, 37, 5, 17, 4, 27, 33, 28, 49, 47}The adopted HMM model is as

follow:

S state set is S= {Weight1, Weight3, Weight3, Weight 4} V observation set is V= {Path1, Path2, Path3, Path4}

The transition matrix is:A = $\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

The emission matrix is: B= $\begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.7 \end{bmatrix}$

$\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

$\begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.7 \end{bmatrix}$ $\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

The initial probability matrix: $\pi = \begin{bmatrix} 0.2 \\ 0.2 \\ 0.2 \\ 0.4 \end{bmatrix}$

$\begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.7 \end{bmatrix}$ $\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

$\begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.7 \end{bmatrix}$ $\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

$\begin{bmatrix} 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.7 \end{bmatrix}$ $\begin{bmatrix} 0.3 & 0.2 & 0.2 & 0.3 \\ 0.2 & 0.3 & 0.2 & 0.3 \\ 0.2 & 0.2 & 0.3 & 0.3 \\ 0.2 & 0.2 & 0.2 & 0.4 \end{bmatrix}$

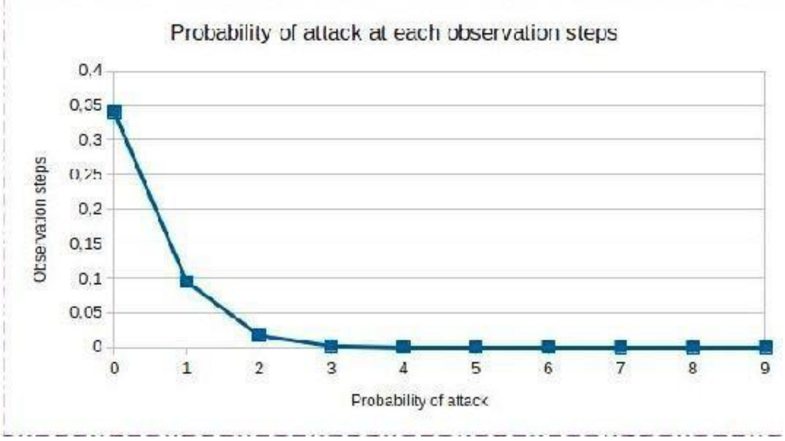
Than we launched observation sequence steps O randomly, for the time T = 10, and each entity in the sequences of observation sequences represents the random path decision made at that time.

O= {Path4, Path4, Path3, Path2, Path3, Path3, Path2, Path3, Path4, Path1}

For example, at time t=1 the random path decision made was a path number 4 meaning the hidden state computed for this sequence step is the weight of this random path 4.

The computed hidden states δ, as shown below, for a random observational sequence steps for a total of time, T= 10Hidden states δ = {weight 4, weight 4, weight 3, weight 3, weight 2, weight 3, weight 4, weight 1, weight 4, weight 2}.

Fig. 6. The prevention results, for a random observational sequence steps for a total of time, T= 10.



From the graph, at the observation sequence step t=1, a random path decision of path 4 was made and for this path, the hidden state is cost=11 hops, which is the least cost meaning the path decision could be a malicious path. Since at t=1 the probability is the greater, the path 4 decision was a path which contains Black Holenode.

In the next step we have calculate Packet Drop Ratio of each node of all paths and Threshold PDR Value in order to prevent malicious node. We can illustrate from fig.7 below that node 4 is malicious node because its packets dropped ratio exceeds threshold value.

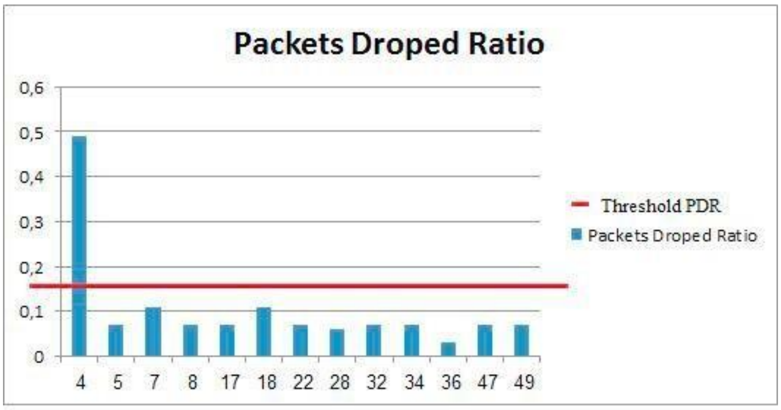


Fig. 7. Dropped Ratio packets of malicious path nodes.

END to END Delay, when our proposed approach is deployed network performance is improved and large number of packet is delivered to the destination. We have evaluated the END2END Delay the Packets Delivered Ratio and the throughput of the network, then we have compared the result obtained for our proposed approach and the normal Black hole attack.

End to end day on network refers to the time taken, for a packet to be transmittedacross a network from source to destination device, this delay is calculated using the below given formula.

E2E Delay= Receiving Time – Sending Time.

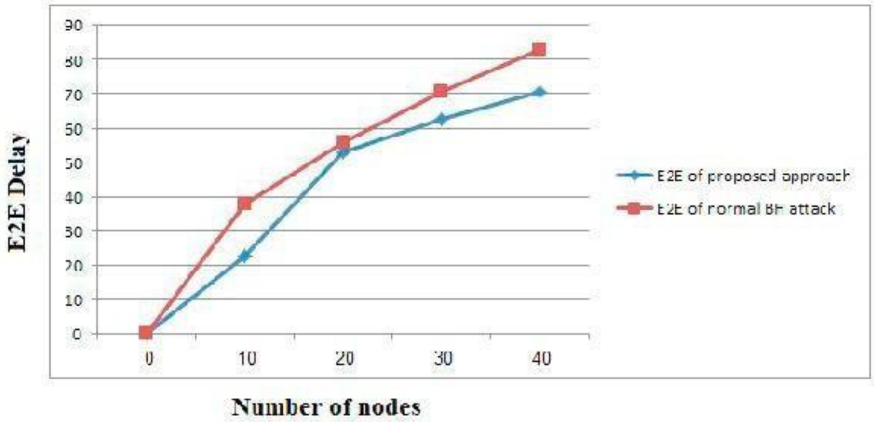


Fig. 8. The end-to-end delay comparison between normal black hole attack andproposed solution.

According to the obtained results obtained in the graph above the proposed solution is produces less end to end delay as compared to traditional routing technique under Black Hole attack conditions. Therefore the proposed solution is and efficient technique and produces less amount of time.

Packet delivery ratio, the performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given:

Packet delivery ratio= Total Delivered Packets / Total Sent Packets.

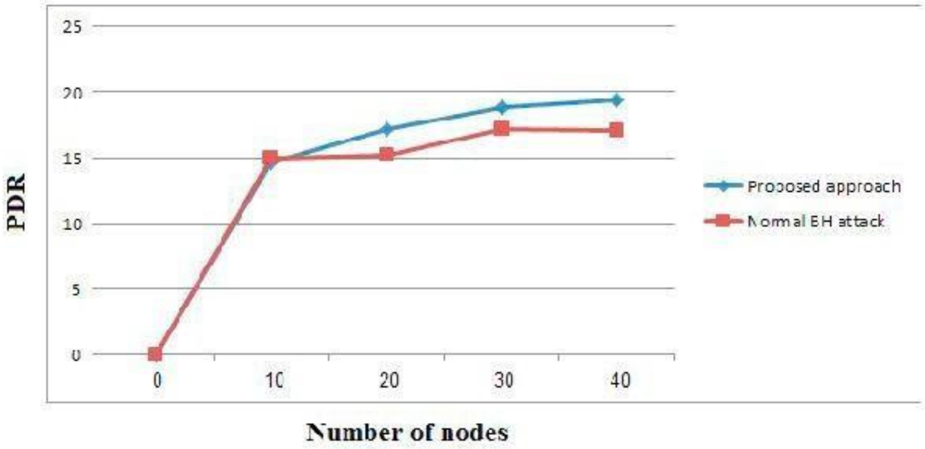


Fig. 9. Packets delivered ratio comparison between normal black hole attack andproposed solution.

The comparative packet delivery ratio of the networks is given in figure 9, in this graph the X axis shows the number of nodes in the network and the Y axis shows the amount of packets successfully delivered in terms of the percentage. According to the obtained results the proposed solution delivers more packets as compared to the traditional technique even when the network contains the Black hole attacker node therefore the proposed solution able to escape the attack effect and improve the network performance.

VI. Conclusion

In this paper, we gave an approach to prevent the Black Hole attack in wireless sensor network using HMM. Our experience measurements and in the basis of metrics like end-to-end delay and packets delivered ratio. An HMM based algorithm has been used to model the sequence of the shortest path decisions selected by a source node to communicate with a destination node. Our approach has allowed preventing the malicious path and node, and our experimental results demonstrate the efficiency of our proposed approach to prevent the malicious nodes.

References

[1]. Filippini, Massimo, and Lester C. Hunt. (2011) "Energy demand and energy efficiency in the OECD countries: a stochastic demand frontier approach." *Energy Journal***32** (**2**): 59–80.

[2]. Sohraby, K., Minoli, D., and Znati, T. (2007) "Wireless sensor networks: technology, protocols, and applications." John Wiley and Sons.

[3]. Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M.(2014)"Wireless sensor networks: a survey on recent developments and potential synergies." The Journal of supercomputing 68(1): 1–48.

[4]. Kalkha, H., Satori, H., and Satori, K.(2016) "Performance Evaluation of AODV and LEACH Routing Protocol." Advances in Information Technology: Theory and Application.

[5]. Kalkha, H., Satori, H., and Satori, K. (2017)"A Dynamic Clustering Approach for Maximizing Scalability in Wireless Sensor Network."

[6]. Transactions on Machine Learning and Artificial Intelligence Akyildiz, I. F., Su, W., S Sankarasubramaniam, Y., and Cayirci, E. (2002) "Wireless sensor networks: a survey." Computer networks, 38(4):393–422.

[7]. Zia, T., and Zomaya, A.(2006) "Security issues in wireless sensor networks." In Systems and Networks Communications. ICSNC'06. International Conference IEE. 40.

[8]. Sunitha, K., and Chandrakanth, H. (2012) "A survey on security attacks in wireless sensor network." International Journal of Engineering Research and Applications (IJERA), 2(4), 1684–1691.

[9]. SARVARI, S., et al.: Wireless Local Area Network. (2017) "A Comprehensive Review Of Attacks And Metrics." Journal of Theoretical & Applied Information Technology. 95, no. 13.

[10]. Abraham, A., Falcon, R., and Koeppen, M.(2017) "Computational Intelligence in Wireless Sensor Networks: Recent Advances and Future Challenges". Vol. 676. Springer .