© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

GNB-AODV: Guard Node Based –AODV to Mitigate Black Hole Attack in MANET

A. R. Rajeswari, K. Kulothungan, A. Kannan

College of Engineering, Gunidy, Anna University, Chennai, Tamil Nadu India

ABSTRACT

In multi-hop wireless ad hoc network, the packets are transmitted through intermediate nodes to reach the destination. In this topological structure, there is no centralized co-ordinating, monitoring or control point. Due to this type of network environment, an intermediate node can act as either selfish or malicious to drop packets. The primary objective of such an untrustworthy behavior of the node is to preserve its own resource such as energy. In this paper, Guard Node Based Ad hoc On Demand Distance Vector Routing scheme has been proposed to detect and prevent the black hole attack on AODV, in Mobile Ad hoc networks. A black hole attack refers to an attack by a malicious node, which forcibly acquire the route from a source to a destination by the falsification of the sequence number and hop count of the routing message. In the proposed system, fixed guard nodes are deployed in the network environment to mitigate black hole attack. These guard nodes are set in promiscuous mode to listen about the transmission within its transmission range. This also calculates the Trust Value of a node, depending upon the abnormal difference between the routing packets transmitted from the node. If the trust value falls below the specified range, guard node will broadcast an alert message, informing all the nodes in the network to isolate the malicious node. The performance and effectiveness of the proposed system outperform the existing protocol in terms of Packet Delivery Ratio, Throughput and Delay.

Keywords : Malicous Nodes, Black Hole Attacks, Trust Value, AODV, GNB-AODV, MANETs.

I. INTRODUCTION

In the "Ad Hoc" topology, the node does not rely on a fixed infrastructure where the nodes are self–configured and self-managed. On the other hand, in "infrastructure" topology, the nodes are under the control of a centralized authority called base station. An ad hoc network is a self-organizing multi-hop wireless network, which is dependent neither on fixed infrastructure nor on predetermined connectivity. It is a collection of nodes, which communicate with each other using radio transmissions. MANETs are generally used for communication during natural disasters on the battlefield and business conference. Thus, secure routing protocols **[1]** are required to enhance the secure transmission between the nodes. Because, MANET lacks a centralized monitoring or centralized control point, due to this open architecture MANET are threatened by many attacks. These attacks include message tampering, identity spoofing, eavesdropping, black hole attack, wormhole attack, and sinkhole. The detection and countermeasure to these attacks are more challenging task because of the resource constrained network environment, which includes self-fish nodes and malicious nodes. In this paper, a guard node based secure mechanism is proposed by extending the traditional AODV to mitigate the black hole attack. By forging the falsified sequence number and hop count the black hole node can forcibly obtain the route from the source node.

The remaining of this paper is organized as follows, section 2describes the related work. Section 3 describes the AODV Protocol. Section 4 illustrates the black hole attack scenario in AODV. Section 5 presents the proposed system section 6 describes the experimental data set and result analysis using ns2 and conclusions and future work are presented in Section 7.

II. METHODS AND MATERIAL

1. Related Work

Many works have been proposed by various researchers in this direction in the past [2] [6] [11] [13] [14] [15] [16]. Among them, A Dynamic Learning method to detect a black hole attack was proposed by Kurosawa et al **[2]**. Tamilselvan et al**. [3] [4]** introduced a revised AODV routing protocol namely Prevention of a Co-operative Black Hole (PCBHA) to isolate co-operative black hole nodes. An authentication mechanism is added into the AODV routing Protocol by Luo et al **[5].** Djahel et al **[6]** also proposed a routing mechanism based on OLSR to mitigate the black hole attack by using two special control packets namely 3 hops ACK and hello rep. Dokurer et al. **[7]** revised the AODV routing protocol to isolate the black hole node. To acquire a route in this mechanism the source node will drop the first returned RREP or the first two returned RREPs and select the subsequent RREP packets because RREP replied by a black hole are generally the first or the second one to arrive at the source node. Mahmood and Khan[8] in their survey work have analyzed a previous work involving black hole attack in MANET. Energy efficient routing protocols are proposed by various researchers for wireless sensor networks, mobile ad-hoc networks and fault tolerant networks [11] [12] [13] [14] [15] [16].

2. AODV

Adhoc on-demand distance vector (AODV) Charles E. Perkin et al. **[9]** proposed Ad Hoc On-demand Distance Vector Routing (AODV) which is classified under on–demand routing protocol. The objective of AODV is to provide loop- free routes even under the condition of repairing the failure routes. The aim of AODV is to broadcast discovery packet only on demand by using local connectivity management, each node in the network can detect its neighbour and topological maintenance. By using AODV, the number of route advertisement message which are broadcasted throughout the network is reduced by discovering the path on–demand rather than using the global periodic routing advertisement. AODV is developed by taking features from DSR and DSDV. AODV consists of the following phases [16]:

Route Discovery Phase In AODV, when a source node tries to seek a route with another node to have communication, it will initiate the path discovery process. However, this process is initiated only when the source node has no routing information in its table. The source node being a route discovery process by broadcasting a route request (RREQ) packet to all its on hop distance neighbors. Each of the neighbor nodes broadcast further to their neighbors until the request reaches an intermediate node with a route to the destination. This RREQ packet contains the IP address of the source, Source Sequence Number, Broadcast–ID, Destination sequence number and hop count. Source address together with the broadcast id uniquely used to identify a RREQ. Broadcast –ID is incremented when the source node initiates a new RREQ. The source sequence number is used to ensure the freshness information about the reverse route to the source. The destination sequence number tells about the freshness of the route to the destination before it can be used by the source. The reverse path is automatically set-up when the RREQ propagates from the source to the destination. Figure 1 illustrates the route discovery phase of AODV [16].

Route Maintenance Phase The source node can initiate the route discovery process to re-establish a new route to the same destination when the source node is moving from the current position during the active session. Under this condition when either the destination or an intermediate node navigate from their current active position, a new RREP is sent to the source node that will carry the information about the new route depending on the current position of the destination and intermediate nodes [16].

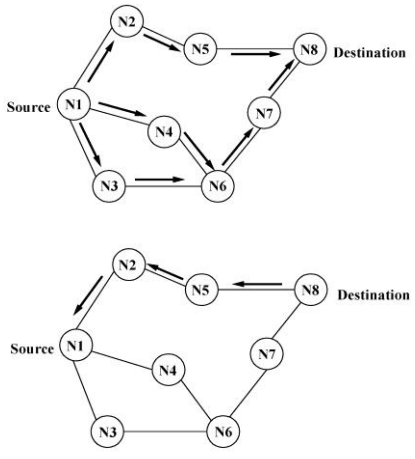
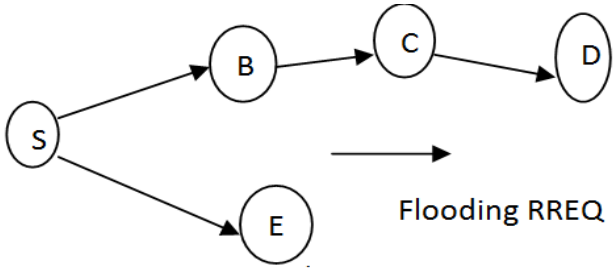


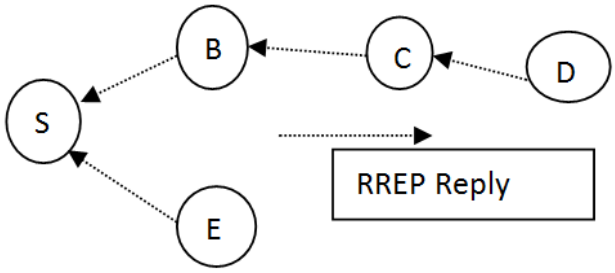
Figure 1. AODV Route Discovery Phase

4. Black Hole Attack in AODV

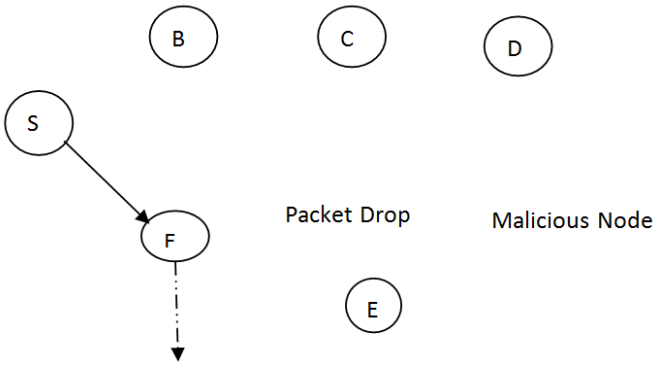
In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and makes another good nodes to route packets through the malicious nodes. In AODV, the attacker can send a fake RREP to the source node, claiming that it has a sufficient fresh route to the destination node. Thus, the source node will select the route that includes the malicious node. Therefore, all the packets will be routed through the attacker. If a malicious node gets the packet, it will simply drop the packet. Fig. 2 illustrate the Black hole attack in AODV.



(a) RREQ Flooding



(b) RREP Reply



(c) Black Hole Attack

Figure 2. Illustrate Black hole attack in AODV

III. RESULTS AND DISCUSSION

5. Proposed System

The objective of this work is to detect and isolate the malicious node that performs the black hole attack in the network.

Assumptions

The following assumptions are taken in order to design the proposed system

1. Guard nodes are fixed and set in promiscuous mode in order to listen all routing packets within its transmission range.
2. Guard node can overhear each other's transmission if they lie within each other transmission range (one – hop neighbor).

In this proposed system, a special kind of node, namely Guard nodes is placed to cover the transmission area and to ensure message transmission takes place between Guard nodes. Every Guard node is assumed to be in promiscuous mode to listen all routing packets within its transmission range. Each Guard node will maintain two tables, namely Packet Monitoring Table (PM) and Malicious Node Table (MN). Guard node constructs the PM table as shown in Table 1 to maintain a record about the RREQ packets, showing that it has overheard within its transmission range. MN table as shown in Table 2 is employed by the Guard node to keep track about the Trust Value (TV) of a node.

A guard node 'G' monitors the traffic of each one hop neighbor node say X and estimate the Trust value TV (G, X), defined as the trust value given by G to X. RREQ and RREP packets transmitted by the node are considered as the primary metrics by the guard node for calculating the TV (G, M).

TV (G, M) =

$$\frac{\text{Total number of Route Replies(RREP)Sent by X}}{\text{Total number of Route Request(RREQ) Received by X}}$$

Trust Value can take values from 0 to 1 wherein 1 means fully trusted and 0 means un-trusted. A node 'X' is considered to be trusted if its Trust Value TV (G, M) estimated by guard node 'G' ranges from 0.5 to 1, whereas the node is considered to be 'malicious' if the

value is less than 0.25. The Trust Value (TV) of a node act as an important criteria to isolate the node as a malicious node. According to the proposed system, any intermediate node, which is not a destination node for a route is classified as a malicious node if it never involves itself in broadcasting a RREQ but forwards a RREP for the specified route. The overhearing guard node will estimate the TV of an intermediate node. Thus, if the TV (intermediate node) falls below the specified value then the state of node will change from " Unblocked" to "Blocked" indicating that the node is isolated and blocked from the network. An alert message will be broadcasted by a guard node to all its one-hop nodes within its transmission range to isolate the malicious node. On receiving the alert message from the Guard node, the normal nodes will update their own Black List Table (BLT) as shown in Table 3. Each node will maintain a Route Information Table (RIT) as shown in the Table 4, while processing the RREQ packet an intermediate node first checks with its RIT to find the availability of fresh and shortest reverse route entry. If found, then the intermediate node will send the 'RREP' otherwise the node will create an entry for a reverse route.

Table 1. Packet Monitoring Table

Source_ID	Destination_ID	Broadcasting Node

Table 2. Malicious Node Table

Node_ID	TV	Condition

Table 3. Black List Table (BLT)

Guard Node	Malicious Node

Table 4. Routing Information Table

Destination IP Address
Destination Sequence Number
Hop Count
Next Hop

Detection of Black Hole Node

Figure 3, illustrates the proposed guard node based mechanism to detect the black hole attack. Source node 'S' intends to forward data to destination node D, broadcast RREQ packet based on the traditional AODV routing protocol. In this scenario, node X that is defined as a malicious node sends 'RREP' to node S as a reply to the RREQ with the highest sequence number and a hop-count of 1.

Hence, X captures the route from S to D.

Guard node G2 will overhear node X's 'RREP' packet. G2 will check whether node X is the destination node. If so, then node X is a normal node. If not G2 will perform the below described procedure Fig 4 to detect the node 'X' as a malicious node by using the following two conditions as illustrated in Fig 5. which shows the procedure to detect a node as Malicious Node.

C1 is a condition that RREQ information corresponding to X's RREP is available in PM Table;

C2 is a condition that X_ID is available in the "broadcasting_nodes" field of PM Table.

Case 1: if C1 and C2 are satisfied, then node X is a normal node.

Case 2: if C1 is satisfied and C2 is not satisfied, then, RIT (X) is checked to find whether there is a fresh and shortest route entry to reach the destination 'D' available in the table. If so, then X is a normal node else node X is identified as a malicious node.

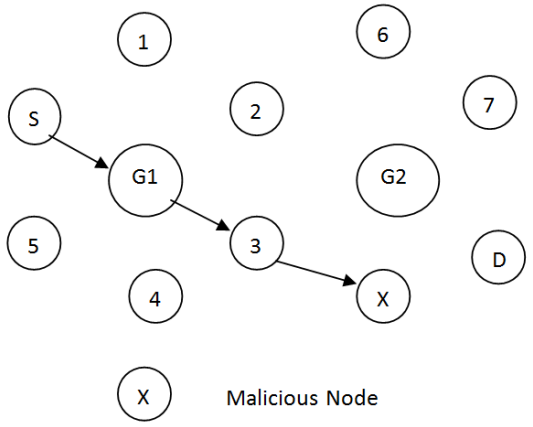


Figure 3. Black Hole node 'X' Detection by guard Node 'G'

Procedure

G is a Guard node that listens to RREP packet transmitted by Node 'X'

C1 is a condition that RREQ information corresponding to X's RREP is available in PM Table

C2 is a condition that X_ID is available in the "broadcasting_nodes" field of PM Table.

1) Source node S broadcast RREQ packet based on AODV routing protocol.
2) G checks If (RREQ. Destination_id == RREP. Source_id) then
3) X is the destination node // X is the normal node
4) Else
5) If X is not the destination
6) Case 1:
7) In G if (C1 == True and C2 == True) then
8) Drop the RREP Packet // X is a normal node
9) Case 2:
10) In G if (C1== True and C2 == False) then
11) Search RIT (X) for availability of fresh and shortest path to reach D
12) X is Normal Node
13) Else
14) X is Malicious Node

Figure 4. Procedure to Identify a Node 'X' as Malicious Node

Steps involved in the isolation of malicious node and transmission of "Alert Message"

1) If guard node G2 detect any node ' X ' within its transmission range as a malicious node. G2 will isolate 'X', if Trust Value TV (G, X) of that node is less than 0.5. Figure. 6 illustrates the procedure to isolated of the Malicious node from the network.
2) G2 will broadcast alert message holding the identity of X (X_ID) to alert the one-hop neighbors, namely 2,4,6,7 and D to update their respective Black List Table (BLT) Fig.6. depicts the operation of Guard Nodes in the network.
3) The G1 that lies near to G2 will also receive the Alert Message broadcasted by G1.
4) If the Alert Message received by G1 is a new message, then G1 will also broadcast this message to all its one-hop neighbor nodes, namely S, 1,4 and 3 to update their BLT.
5) All the nodes in the network added X_ID into their BLT and none of them will include X in Route Discovery Phase. Thus, X is isolated from the Network. Figure 7. illustrate the proposed system to detect and isolate the malicious node from the network.

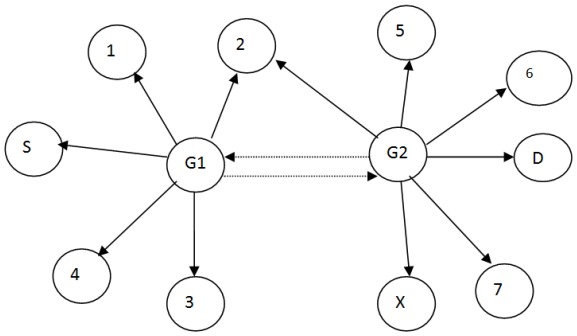


Figure 5. Operation of Guard Nodes

Procedure:

// Isolation of Malicious Node

1. Search (X information in Malicious Node table)
2. If exists and the status is 'blocked'
3. G broadcast 'Alert message'
4. Else
5. Calculate TV (G, X)
6. If (TV (G, X) < 0.5)
7. G changes X. Status = 'Active ' and broadcast ' Alert message '
8. Else
9. Store X (Node_ID, TV, Status) in Malicious Node table
10. End if

Figure 6. Procedure for Isolation of Malicious Node

6. Experimental setup and Result analysis:

A simulation study has been done in NS2.34 [10] to analyze the detection and isolation efficiency of the proposed Guard Node based system against the black hole attack. In the simulation model, there are 100 nodes deployed in a 1000 X 1000 m^2 field all the nodes are set a static node. The routing protocol namely AODV is used in this simulation. Table 5 shows the experimental parameters of ns2. 34 used in the simulation.

Table 5. Parameters

Parameter	Value
Coverage area	1000mX1000m
Normal Nodes	100
Malicious Nodes	35
Guard Nodes	9
Packet Size	512 bytes
Transmission range	250m
Pause Time	15 s
Speed	20m/s

Performance Metrics:

The performance of the proposed system has been measured by using the following parameters namely:

1. Packet Delivery Ratio
2. Throughput
3. End-end delay

Packet Delivery Ratio: Packet Delivery Ratio is measured in terms of the number of packets received successfully by the destination for those generated by the constant source and the total amount of packet bit rate transmitted.

Throughput : It is a measure of the number of packets successfully transmitted to their final destination per unit time. The throughput is usually measured in bits per second or data packets per second. In general, term throughput denotes the amount of traffic in the entire network.

End–End: End-to-End Delay: This parameter is defined as the time elapsed between the moment of sending off a bit by the source node and the moment of its reception by the destination. It indicates the time taken for a packet to travel from CBR constant bit rate source to destination. It represents the average data delay that an application experience while transmitting data.

The performance of the proposed scheme is compared with AODV. The proposed GNB-AODV yields better results. Figure 7, shows an improvement in packet delivery ratio of GNB-AODV scheme.

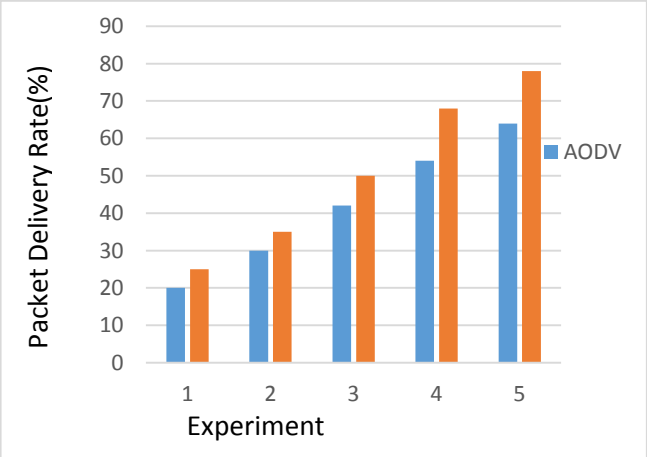


Figure 7. Packet delivery Ratio

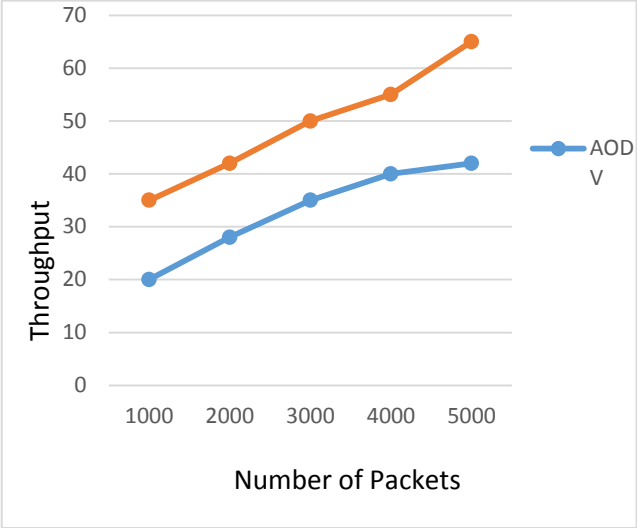


Figure 8. Throughput

Figure 8. shows that the proposed algorithm improves the throughput of the network even in the presence of black hole attack. GNB-AODV yields less delay when compared to AODV as shown in Figure 9.

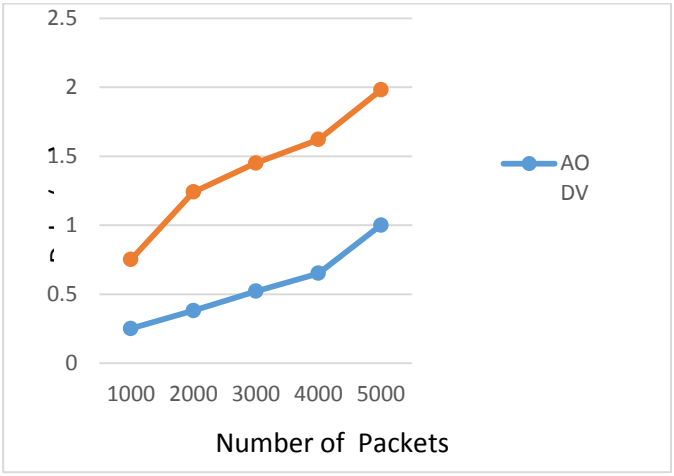


Figure 9. Delay

From the figure 10. Depicts the malicous node detecion rate . form this figure, it is obsedrved that the detection rate in the proposed work GNB-AODV is higher when compared to traditional AODV.

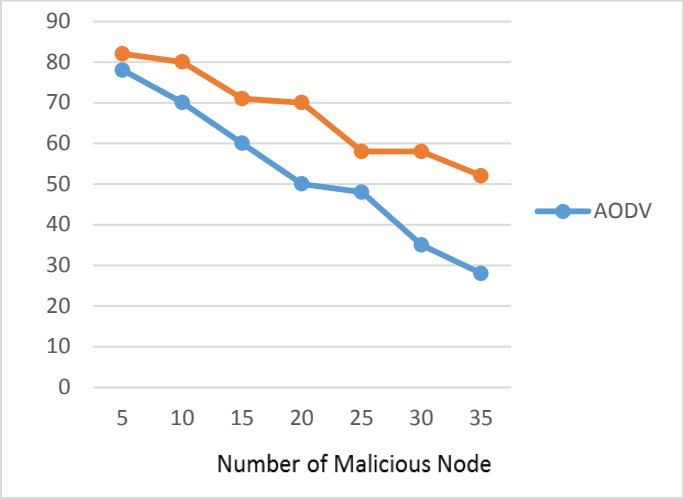


Figure 10. Detection Accuracy Rate

IV. CONCLUSION

In this work, a new protocol is proposed to detect the malicious node and to isolate it by deploying fixed Guard nodes in the network environment. The guard nodes will estimate the Trust Value (TV) of a node, when TV falls below the specified range an alert message will be broadcasted by the guard node to all nodes in the network to isolate the malicious node. The simulation results show that the percentage of data packet loss in the proposed system is better than that in AODV in presence of black hole attack. Further works in this direction can be the use of intelligent agents for performing more effective decision making onattack detection.

V. REFERENCES

[1] Zapata Manel G, Asokan N. Securing ad-hoc routing protocols. In: Proc. of the ACM workshop on wireless security (WiSe), 2002.

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Detecting blackhole attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method, International Journal of Network Security 5 (3) (2007) 338–34

[3] Latha Tamilselvan, V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", in: Proc. of the International Conference on Wireless Broadband and Ultra Wideband Communication, 2007.

[4] Latha Tamilselvan, V Sankaranarayanan, Prevention of co-operative black hole attack in MANET, Journal of Networks 3 (5) (2008) 13–20.

[5] Junhai Luo, Mingyu Fan, Danxia Ye, "Black Hole Attack Prevention Based on Authentication Mechanism", in: Proc. of the IEEE Singapore International Conference on Communication Systems (ICCS), pp. 173–177, 2008.

[6] Soufine Djahel, Farid Nait-Abdesselam, Ashfaq Khokhar, "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol", in: Proc. of the IEEE International Conference on Communications (ICC), pp. 2780–2785, 2008.

[7] Semih Dokurer, Y.M. Erten, Can Erkin Acar, "Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148–153, 2007

[8] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks", in: Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), pp. 1–6, 2007.

[9] C.E. Perkins, E. Beliding-Royer, S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF Internet Draft, MANET working group, Jan. 2004

[10] The Network Simulator - ns-2.34, http://www.isi.edu/nsnam/ns/.

[11] S Jerusha, K Kulothungan, A Kannan, "Location aware cluster based routing in wireless sensor networks",International Journal of Computer and Communication Technology, Vol.3, No.5, pp. 1-6, 2013.

[12] K Kulothungan, JAA Jothi, A Kannan, "An Adaptive Fault Tolerant Routing Protocol with Error Reporting Scheme for Wireless Sensor Networks", European Journal of Scientific Research, Vol. 16, No.1, pp. 19-32, 2011.

[13] K Kulothungan, S Ganapathy, S Indra Gandhi, P Yogesh, A.Kannan, "Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach", International Journal of Soft Computing, Vol.6, No.5, pp. 210-215, 2011.

[14] S Muthurajkumar, M Vijayalakshmi, S Ganapathy, A.Kannan, "An Intelligent Energy Efficient Cluster based Routing Protocol for Wireless Sensor Networks", Transylvanian Review, Vol. 24, No.6, 2016.

[15] R. Logambigai, S. Ganapathy, A. Kannan, "Energy Efficient Mid Position Opportunistic Routing for Wireless Sensor Networks", International Journal of Scientific Research in Science, Engineering and Technology, Vol. 2, No.2, pp. 99-102, 2016.

[16] Perkins, C.; Belding-Royer, E.; Das, S. (July 2003). Ad hoc On-Demand Distance Vector (AODV) Routing. IETF. RFC 3561. Retrieved 2010-06-18.