International Journal of Engineering & Technology, *7 (4.38) (2018) 893-897*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Reliable and Secure AODV Protocol for MANETs

Ajit Kumar Singh Yadav1, Rajesh K. Yadav2

1Department of Computer Science & Engineering, NERIST, Itanagar, India
aky@nerist.ac.in
2Department of Computer Science & Engineering, DTU, New Delhi, India
**Corresponding author E-mail: rkyadav6711@gmail.com*

Abstract

In recent years, Mobile ad hoc networks ((MANETs) have generated great interest among researchers in their implementation under several computing environments. However, MANETs are highly susceptible to various security attacks due to their inherent characteristics. The ad hoc on demand distance vector (AODV) is most suitable routing protocol for mobile adhoc networks in which resource consumption attacks are frequent if it is not detected timely. In this paper, we have proposed a scheme to detect as well as overcome black hole attacks using an Intrusion Detection System (IDS). The proposed scheme is implemented using network simulator 2(NS2) to compare its performance against the standard AODV with and without attack. The results of the simulation show that proposed scheme optimizes the end-to-end delay, normalized routing load, packet delivery fraction and average throughput in comparison with AODV protocols under black hole attack.

Keywords: *Mobile adhoc Network, AODV, relative velocity, black hole attack and Intrusion Detection System.*

1. Introduction

As there is no fixed infrastructure between MANETs for communication, routing becomes an issue in large number of mobile nodes deployed along with other challenges of these networks. Proposed AODV protocol is able to reduce the communication overhead due to mobility. A black hole attack in which a node drops the packet instead of relay them. This is a type of denial of service attack [1][2][3]. The proposed scheme calculates the parameters like packet delivery ratio, throughput in the network without black hole and with many black hole nodes. The proposed protocol operates in two steps namely black hole attack detection and recovery. If a black hole node is detected it is bypassed by discovering a new route to the destination. The network parameters can be computed and compared in following scenarios, namely one in which no black hole nodes are present, the second in which black hole nodes are present but no attempt is made to detect them, and the last one being an implementation of our proposed protocol which aims to recover from black hole attack.

This paper is organized in following sections Background and related work of black hole attack is described in section 2. Section 3 describes the proposed scheme. Section 4 explains results and analysis. The Conclusion of proposed scheme is highlighted in section 5.

2. Background

2.1 AODV Protocol

In the AODV protocol [4] on demand approach is used for establishing a route when data transmission is required by a source node. It finds out the most recently used route from the destination sequence number. The source node sends the Route request Packet to all when it does not finds a rout for the destination. When a node receives a RouteRequest either it setup a reverse path to the source to establish a path to the destination if it is having valid route to the destination or setup forward path to forward the RoutRequest of previous node with its BcastID. There are many researchers have been attempting to optimize the AODV protocol [5][6][7][8][9].

2.2 Black hole attack

A black hole attack also called packet drop attack in a network, in which a node discards the packets instead of relay them, is a type of denial of service attack. These types of attacks are more complex to prevent and detect. In a lossy network the packets are frequently dropped because of a node compromised by a different number of causes.

A wireless ad hoc network is more vulnerable to packet drop attack in comparison to a wired network because of different architecture. Compromised node can broadast false information about the shortest route and all the packets can choose the compromised node as relay node towards the destination. Now the compromised node can discard the packets. Hosts in a mobile ad hoc network are also vulnerable to collaborative packet drop attacks, where multiple nodes can be compromised.

2.3 Drawback of already proposed solutions to black hole attack

Many authors [10][11][12][13][14] have tried this problem. Djenouri & Badache[15] proposed a scheme that prevents false accusation attacks vulnerability and reduces the false positives caused by mobility of nodes and channel conditions. This scheme can detect the attacker node which is dropping the packets. Here the random two hope ACK can be taken as the normal two hop ACK in detection of high true and low false with less overhead. This scheme is based on cooperatively witness based verification. This approach cannot detect the multiple compromised nodes and collaborative black hole attacks.

Deng [16] proposed a scheme to avoid the black hole attacks. In this scheme an intermediate node cannot reply a message. Only destination node can reply all the messages. This way by avoiding black hole attacks a secure AODV protocol can be implemented. However this scheme has two disadvantages. One is the increased routing delay in large networks and second an attacker node can reply a message pretending itself as destination node.

In SAODV scheme [17] the author proposed a cryptographic approach to prevent the black hole attack. To secure the hop count information a digital signature is used to authenticate hash chains and non-mutable fields of messages. Here key management is difficult in this scheme as MANET does not have centralized infrastructure which is mostly required in a cryptographic protocol.

2.4 Intrusion detection system

In intrusion detection system (IDS) all inbound and outbound network activities and doubtful manipulations are checked and alert the network administrator. In this it collects the information analyses about attacks within computer or network. Intrusion may be attacks from outside or within the organization. The IDS can be implemented in two ways one is host based IDS(HIDS) and the other is network based IDS(NIDS).

3. Proposed work

3.1 Proposed AODV Protocol

In original AODV protocol set up routes are set up on demand but it requires more time to establish a connection and initial broadcasting of packets puts a heavy load on the network during the route set-up phase. Secondly, in AODV protocol whether a route should be chosen or not depends on route update logic which is based on the path with lower hop count or higher sequence number.

Modifications

The modifications done in the original protocol are as follows:

1. For the initial broadcasting phase we have used an expanding ring search.

- In this method increasingly larger neighbourhoods searched by sending out successive RREQ's each with a larger TTL that limits how far a RREQ can traverse from source.
- If the initial search fails then increase the search area until either we get the next hop or reach the maximum admissible value of TTL.
- If the final search also fails then use the process of flooding the network with RREQ packets.

2. For route update logic in place of number of hops as a parameter, we have taken

a new parameter which is a metric of dr^2/dt.

- This particular metric is chosen as it tells the relative stability of nodes with one another on the basis of position and velocity.
- The metric dr^2/dt is equal to 2*(relative position of nodes)*(relative velocity of nodes).
- In addition to this we have a predefined threshold value for this metric. If the node receives a RREQ packet, it calculates the value of the metric.
- If the value of metric is greater than threshold, packet is discarded else it is forwarded.
- if unable to get a route to the destination then increase the value of threshold by a predefined amount and repeat the process.
- This process is repeated until we get a route or threshold is lesser than maximum threshold value set.In this way the route which has a lower value for the metric dr^2/dt is selected for transmission of packet.

3.2 Black hole detection and recovery

3.2.1 Basic principle

Since, data and RREP packets are unicast so they will be received by/ forwarded to from exactly one neighbouring node, so neighbouring nodes can keep record of packets received and sent by each node. By this way the number of packets dropped can be computed in the network. This parameter can then be used to estimate if a given node drops too many packets to be classified as a black hole node or not.

Following rules for a rule based IDS formulated to detect intrusion in the network:

1. A node is considered as honest node if it forwards many data packets.
2. A node can be considered as misbehaving node if it is receiving many packets and forwarding less no of packets.
3. There is a high possibility of a node being compromised when it sends RREP packets and rule 2 is correct for it.

3.2.2 Neighbourhood Maintenance

The proposed scheme requires all nodes in the network to maintain a list of neighbours. For this purpose, HELLO packets used, which are periodic beacons broadcasted by a node to inform its neighbours about its presence. If a node *j* receives a HELLO packet broadcasted by node *i*, then *j* adds *i* to its list of neighbours, *Neighbour_List[i]*.

3.2.3 Dealing with Black hole nodes

To deal with black hole nodes, each node *i* in the network maintains the following data structures:

1. ***Neighbour_List[i]*** : A list of nodes maintained by node *i*, using HELLO packets as described above such that if node *j ϵ Neighbour_List[i]*, then node *j* is a neighbour of node *i*.
2. ***Black_List[i]*** : A table of entries maintained by node *i* such that the entry for node *j* in *Black_List[i]* consists of the following fields:
   a. ***Black_List[i][j].num_data_received*** :Number of data packets received by node *i* from node *j*.
   b. ***Black_List[i][j].num_data_sent*** : Number of data packets sent from node *i* to node *j*.
   c. ***Black_Llist[i][j].num_rrep_sent*** : Number of RREP packets received by node *i* from node *j*.

d. ***Black_List[i][j].is_blackhole*** : A boolean flag which if set true indicates that node *i* perceives node *j* to be a black hole node, and not otherwise.

Using the above table entries, we can compute the following for a node *i:*

1. **NUM_DATA_RECEIVED[i]** : Total number of data packets received by a node *i*

$$NUM\_DATA\_RECEIVED[i] = \sum_{k} BLACK\_LIST[k][i].num\_data\_sent$$

∀k, such that i ϵ Neighbour_List[k]

2. **NUM_DATA_SENT[i]** : Total number of data packets sent/forwarded by node *i*

$$NUM\_DATA\_SENT[i] = \sum_{k} BLACK\_LIST[k][i].num\_data\_received$$

∀k, such that i ϵ Neighbour_List[k]

3. **NUM_RREP_SENT[i]** : Total number of RREP packets sent/forwarded by node *i*

$$NUM\_RREP\_SENT[i] = \sum_{k} BLACK\_LIST[k][i].num\_rrep\_received$$

∀k, such that i ϵ Neighbour_List[k]

3.2.4 Detection of black hole node

In order to detect the presence of black hole nodes in the network, the nodes operate as follows:

1. Whenever a node *i* receives a data packet from node *j*, it increments *Black_List[i][j].num_data_received* by 1
2. Whenever a node *i* forwards a data packet from node *j*, it increments *Black_List[i][j].num_data_sent* by 1
3. Whenever a node *i* receives a RREP packet from node *j*, it increments *Black_List[i][j].num_rrep_received* by 1
4. Whenever a node *i* has to forward a data packet to node *j*, it determines if *j* is a black hole node by querying its neighbors for the information they maintain about node *j*, and thereby computing parameters *NUM_DATA_SENT[j]* and *NUM_DATA_RECEIVED[j]* and applying the threshold function as described above.

3.2.5 Recovery

1. If a node *i* detects that node *j* is a black hole node, it sets *Black_List[i][j].is_blackhole* as true and broadcasts an ALARM packet to all other nodes in the network which respond by setting this Boolean flag to true
2. Now if some intermediate node has a packet to forward to a destination node such that the next hop in its routing table for the destination is listed as node *j*,
   i. It erases that route entry
   ii. It initiates route discovery to the destination by broadcasting RREQ (Route Request) Packets.
   iii. If in response to the Route discovery phase, a node receives a RREP Packet from node *j*, then it is simply dropped and a new path to the destination is discovered rather than the current one which goes via the black hole node

The detailed scheme is:

1. Initialize the neighbor list and black list which has the following fields (Number of received data, number of sent data, number of sent RREP, Boolean flag is_blackhole).
2. If the packet is a HELLO packet
   a. If a node j receives a HELLO packet broadcasted by node i, then j adds i to its list of neighbours , Neighbour_List[i].
3. If the packet is a data packet then:
   a. Forward opinion request packet to the neighbors of the next hop stored in the routing table.
   b. Check the blacklist to determine if the next hop recorded in the routing table is a black hole node or not.
   c. If the node is not a black hole node, then increment the number of sent data to next node and forward packet to next node.
   d. Else remove the next hop information from the corresponding routing table entry and reinitiate route discovery phase to discover a new route to the destination.
4. If the packet is a RREP then
   a. Increment the number of received RREP for sender of the packet.
   b. If blacklist[i][sender].is_blackhole=0 for the sender of RREP, where i is the current node then the packet is forwarded.
   c. Else the packet is ignored.
5. If the packet is an opinion request packet then
   a. If the node has any opinion about the requested node then extract the activities of the requested node from black list table (including number of received data, number of sent data, and number of sent RREP) and create a response packet including the required information.
   b. Forward the response packet.
   c. Else forward the opinion request packet.
6. If the packet is a response packet then
   a. If the node is sender of the opinion request packet then extract the information from the packet (including number of received data, number of sent data, number of sent RREP, is_blackhole).
   b. If the (packet drop ratio for the node>=Threshold (for blackhole node detection)) and (sum of received RREP>0) then set the value of is_blackhole=1.
   c. Else forward the packet.

4. Simulation and Result Analysis

The proposed protocol is simulated and evaluated in the Network Simulator 2(NS2). In this simulation a network with 10, 20, 30,40,50,60,70,80,90, and 100 nodes has been considered that moves in an area of 500 meters × 500 meters for 100 seconds. The simulation is done over the following parameters and settings shown in table-1.

Table-1: Simulation Parameters

Parameter	Simulation Value
Antenna type	Omni Antenna
Channel Type	Wireless channel
Radio-propagation model	Two Ray Ground
MAC layer	IEEE 802.11
Simulation area	500*500 m^2
node velocity	10ms^{-1} to 30 ms^{-1}
node movement model	Random Waypoint
Traffic type	CBR(UDP)
Packet Size	512 bytes
Pause time	5 s
Simulation time	100 s

4.1 Evaluation Metrics

The performance evaluation involves:

i. Packet Delivery Ratio: It is the rate of packets successfully delivered.
ii. Average End to End Delay: This parameter represents the average time for transmitting a data packet from source to destination.
iii. Normalized Routing Load: The quantity and size of control packets generated by the protocol to find and hold a route. It is defined as the ratio of the number of generated control packets to the number of generated data packets.
iv. Average Throughput: It is the rate of successful message delivery over a communication channel.

4.2 Graphs for network parameters

The simulation was also used to plot various network parameters as a function of time and the results obtained are summarized as follows:

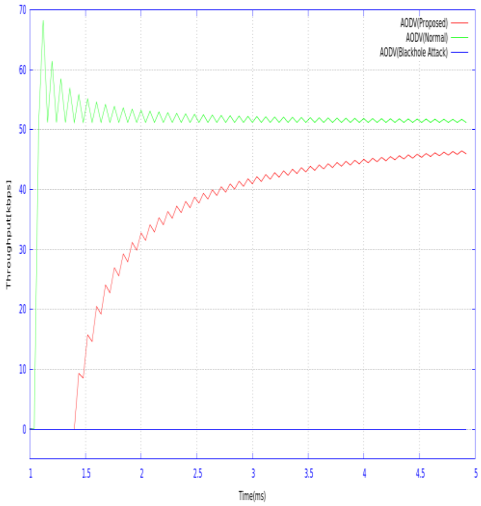

Figure 1. Average Throughput vs. Time

The above Figure 1 depicts that in the network with black hole attack the data packets do not reach the intended destination and hence the throughput remains zero at all times. In proposed IDS scheme after the black hole attack is detected, the throughput rises and tends to the value for the normal network.

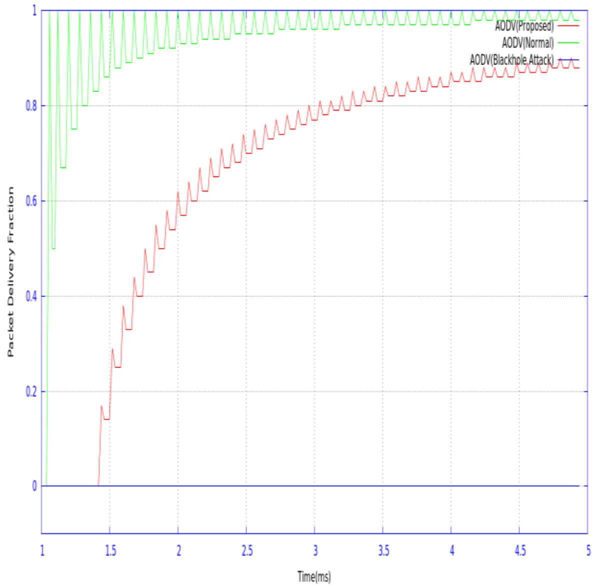

Figure 2. Packet Delivery Fraction vs. Time

The above Figure 2 depicts that in the network with black hole attack the data packets do not reach the intended destination and hence the packet delivery ratio remains zero at all times. In proposed scheme after the black hole attack is detected, the packet delivery ratio rises and tends to the value for the normal network

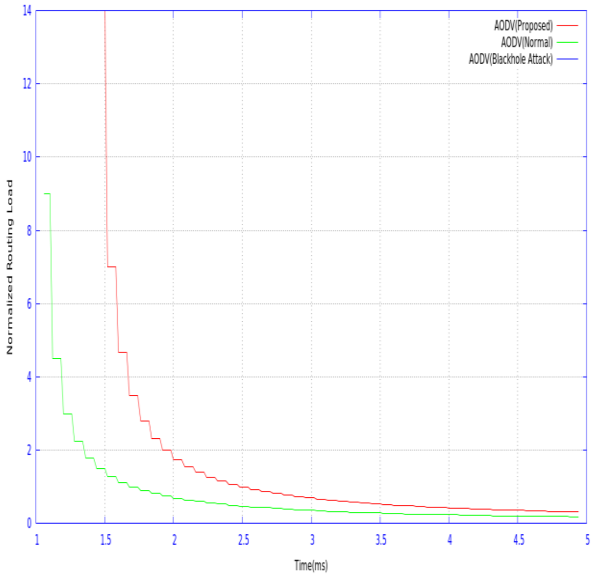

Figure 3. Normalized Routing Load vs. Time

Figure 3 shows that normalized routing load is far better than with black hole attack, but it is higher than the case in which no black hole nodes are present because in the network with black hole attack the more effort in terms of routing packets is required to deliver packets and hence the normalized routing load increases.

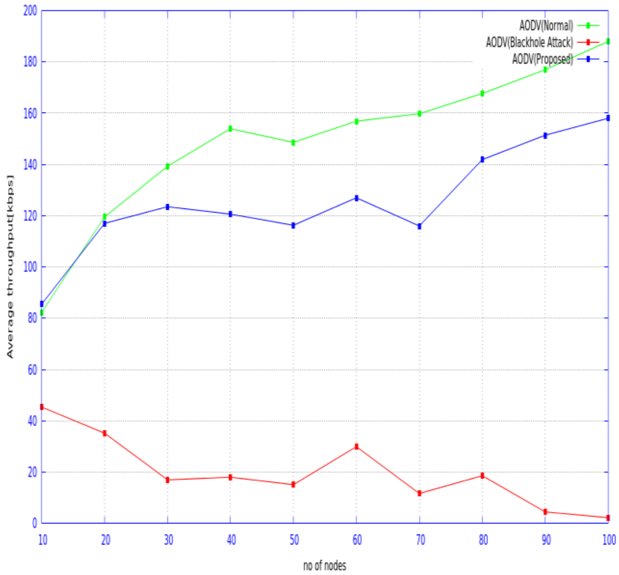

Figure 4. Average Throughput vs. no. of nodes

In AODV with black hole attack, fewer packets reach the destination and hence average throughput decreases. The Figure 4 shows that proposed protocol solves the issue and thus throughput tends to the value for normal network without any attack.

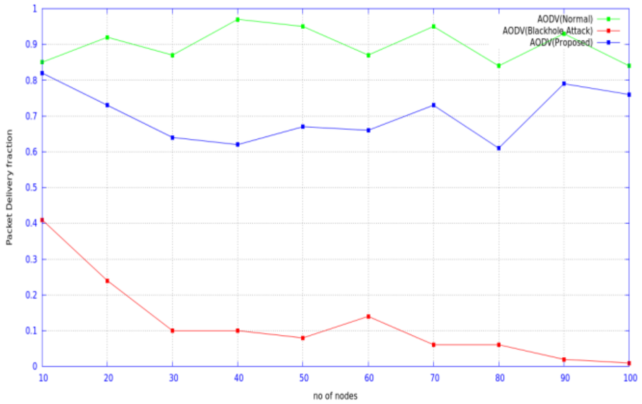

Figure 5. Packet delivery fraction vs. no. of nodes

In AODV protocol with black hole attack, less number of packets reaches to the destination and thus packet delivery fraction decreases while figure 5 shows that proposed protocol increasing the packet delivery fraction and thus minimizing the effect of attack.

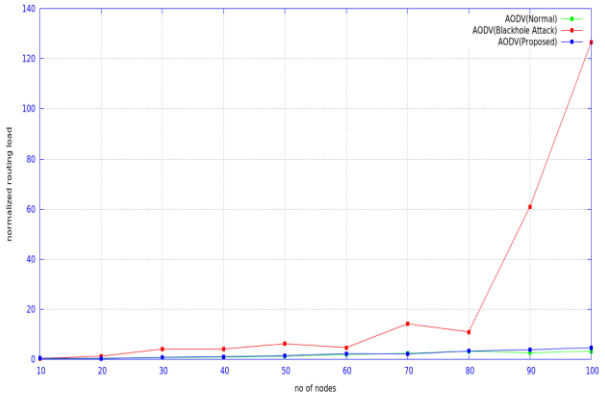

Figure 6. Normalized routing load vs. no. of nodes

In the network with black hole attack the more effort in terms of routing packets is required to deliver packets and hence the normalized routing load increases. Figure 6 shows that proposed scheme detects the black hole attack but requires an additional route discovery phase to find a path to the destination bypassing the malicious node, hence it incurs more routing overhead than the normal network but less than the network with no solution.

5. Conclusion

We propose a scheme **to detect as well as overcome black hole attacks using an Intrusion Detection System (IDS)** on the AODV routing protocol. The proposed protocol is optimized by preventing the recursive flooding using a metric based on relative mobility with expanding ring search. The performance of proposed AODV improves over the original protocol for the networks with more number of nodes in which path stability plays a dominant factor with respect to route length. The packet delivery ratio; throughput improves although being less than the case in which no black hole nodes are present. Normalized routing load is far better than with black hole attack, But it is higher than the case in which no black hole nodes are present.

References

[1] Salehi, M., Darehshoorzadeh, A., & Boukerche, A. On the Effect of Black-hole Attack on Opportunistic Routing Protocols. In Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks ,pp. 93-100. ACM. (2015)

[2] Hiremath, P. S., and T. Anuradha. "Performance Comparison of Cluster based and Threshold based Algorithms for Detection and Prevention of Cooperative Black Hole Attack in MANETs." International Journal of Advanced Networking and Applications 6.3: 2352. (2014)

[3] Thachil, F., Shet , K. C.: A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET,Computing Sciences (ICCS), 2012 International Conference on, Phagwara,pp. 281-285(2012)

[4] Perkins, C.E., Royer, E.M. "Ad-hoc on-demand distance vector routing," Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, New Orleans, LA, pp. 90-100.(1999)

[5] Jambli, M. N., Wan Mohd Shuhaimi, W. B., Lenando, H., Abdullah, J., & Suhaili, S. M. : Enhancement of AODV routing protocol in MASNETs. In IT in Asia (CITA), 2015 9th International Conference on,pp. 1-6.(2015)

[6] Zou, Y., & Chakrabarty, K. "Distributed mobility management for target tracking in mobile sensor networks," IEEETrans. Mob. Comput. vol. 6, no. 8, pp. 872–887. (2007)

[7] Li, W., Chen, M., & Li, M. M. (2009). An enhanced aodv route protocol applying in the wireless sensor networks. In Fuzzy Information and Engineering Volume 2,pp. 1591-1600.(2009)

[8] Murthy, C. Siva Ram, and B. S. Manoj. :Ad Hoc Wireless Networks: Architectures and Protocols, Portable Documents. Pearson education.(2004)

[9] Dhurandher, S.K., Isaac W., Mathur, R., & Khurana, P.: GAODV: A Modified AODV against single andcollaborative Black Hole attacks in MANETs." In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, pp. 357-362.(2013)

[10] Chen, H., Wu, H., Hu, J., & Gao, C. Event-based trust framework model in wireless sensor networks. In Networking, Architecture, and Storage, 2008. NAS'08. International Conference on (pp. 359-364). IEEE. (2008)

[11] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. IJ Network Security, 5(3), pp.338-346.(2007)

[12] Ehsan, H., & Khan, F. A.: Malicious AODV: implementation and analysis of routing attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on ,pp. 1181-1187.(2012)

[13] Rathore, H., Badarla, V., Jha, S., & Gupta, A. Novel approach for security in wireless sensor network using Bio-inspirations. In Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on ,pp. 1-8.(2014)

[14] Khandelwal, V., & Goyal, D.: Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs. IJARCET, 2(4), 1555-9. (2013)

[15] Djenouri, D. and Badache, N.: Struggling against selfishness and black hole attacks in MANETs. Wirel. Commun. Mob. Comput., 8: 689–704. (2008)

[16] Deng, H., Li, W., & Agrawal, D. P. Routing security in wireless ad hoc networks. Communications

[17] Magazine, IEEE, 40(10), 70-75. (2002)

[18] Zapata, M. G. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing

[19] and Communications Review, 6(3), 106-107.(2002)

[20] Introduction to Network Simulator NS2(2nd Edition) by Teerawat Issariyakul, Ekra Hossain

[21] The Network Simulator (NS-2); http://nsnam.isi.edu/nsnam/index.php/User_Information

[22] Tcl Tutorial - Tcl/Tk; https://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[23] Generating sensor node-movement and traffic-connection files for large wireless scenarios,

[24] http://www.isi.edu/nsnam/ns/tutorial/nsscript7.html

[25] Post processing NS2 Result using NS2 Trace — New Wireless Trace file format,

[26] http://ns2ultimate.tumblr.com/post/32176398101/post-processing-ns2-result-using-ns2-trace-new