A Survey on Security Solutions of AODV Routing Protocol against Black Hole Attack in MANET

Mohamedi M. Mjahidi
College of Informatics and
Virtual Education
The University of Dodoma

ABSTRACT

Ad Hoc On-Demand Distance Vector (AODV) routing protocol is among the efficient routing protocols in Mobile Ad Hoc Network (MANET). Because of its routing features AODV has gained popularity compared to other routing protocols, but this protocol lacks a security features which make it more vulnerable to malicious attack particularly black hole attack. A single or cooperate black hole attacks when present in a network can deny any packet from source to reach the destination. This paper aims at presenting the current existing security techniques that are used to prevent and detect the black hole attacks in MANET.

General Terms

Black Hole, Routing Protocols, Security.

Keywords

AODV, RREP, RREQ, MANET,

1. INTRODUCTION

Ad hoc networks are wireless networks formed spontaneously between certain mobile devices like computers, sensors, mobile phones and others with limited resources like battery life time, low memory, weak security, devices size limitation, bandwidth constrained, slow data transfer rate and low processing power that do not have a central routing device like router and so each node must ensure the functionality of routing. In addition, the network structure changes dynamically as needed, possessing features like adaptively, auto-configuration and ability to operate in an environment where no previous infrastructure exists for communication. This allows the MANETs to meet communication needs in situations like military operations, disaster relief, emergency rescue, etc.

In ad hoc networks, routing protocols are categorized in two traditional groups; *the reactive routing protocols* and *proactive routing protocols*. Among the MANET routing protocols, reactive routing protocols have gained more attention; a reactive routing protocol discovers a route only when needed. This enables a reactive routing protocol to achieve better performance than the other routing protocols, which discovers and maintains all possible routes in the network even though they may never be used [1].

AODV routing protocol is an improvement of DSDV, it typically minimizes the number of required broadcast by creating routes on demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm [2]. AODV does not specify any special security measures and is vulnerable to many types of attacks that manipulate its routing control mechanism. Among the attacks to AODV routing protocol is the black hole attack, so the black hole node can disrupt network operations and disobey the AODV routing specifications.

2. AD-HOC ON DEMAND DISTANCE VECTOR (AODV)

AODV is a reactive routing protocol in MANETs. Route discovery is not initiated until it is required (on-demand), the protocol operates in two phases: *Route Discovery* and *Route Maintenance* [3]. Route discovery is used when a source node want to send message to a target node without the routing, it sends/broadcast RREQ first. When the adjacent node received RREQ with the addresses of source node and target node, before forwarding, it keeps a reverse path to the source node in its routing table. The routing table records the route information of the next hop, the distance and the current highest sequence number it has seen then it judges if it was the same with the target node's address. If it was, then it sends the RREP to source node, otherwise, checking the routings in the rout table that could reach the target node, then it sends RREP to source node, or continue to flooding sent RREQ. Source node receives multiple RREP packets via different paths. Source node selects fresher and shorter path among them to send the application data. AODV protocol maintains routing nodes through broadcasting hello message regularly. If one link breaks, it sends ERROR message to nodes, meanwhile deleting broken records or repairing the routing.

In addition to AODV, The sequence number is a 32-bit unsigned integer, it helps in comparing the freshness of the information of the other node. Higher sequence number indicates more accurate information and whichever node sends the highest sequence number, its information is considered for route establishment over the other nodes. So, the higher the sequence number, the more the freshness of the route. A destination node updates its own sequence number whenever a node initiates a route discovery process and whenever a destination node responds to RREQ with a RREP [1].

3. BLACK HOLE ATTACK

It should be noted that the source node can receive several RREPs from different nodes. However, it chooses the one with higher sequence number for the intended destination. If RREPs containing the highest sequence number for the same destination are reported by more than one node, then the path with smaller hop counter will be selected. In this regard, in [3], [4], [5] the black hole attack in AODV can be summarized in the following points:

- When the black node receives a RREQ, it takes note of the destination address, and prepares a RREP, in which the destination address is set to the spoofed destination address, the sequence number is set to a highest value (2^{32} -1) and the hop counter is set to a smallest value(1 in this case).

- If the black hole node does not communicate directly to the source node, it sends RREP to the closest intermediate node belonging to the actual active route. RREP received by the intermediate node will be relayed through the reverse path towards the source node.
- The source node updates its routing table according to the received RREP, and uses the new route to send data.
- When intercepted, data is dropped by the black hole node.

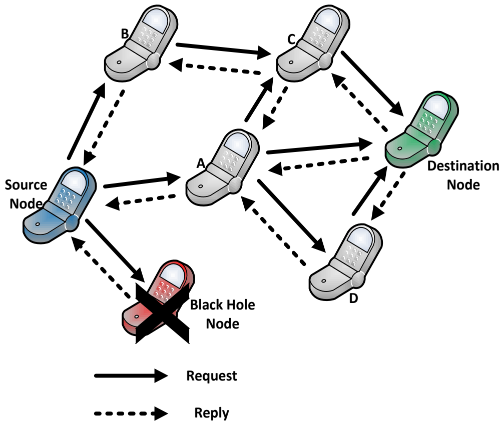

Fig 1: Black hole attack

In Fig 1, the Source Node wants to send data to destination node, at first it needs to initialize a route. Once the Black Hole Node received a RREQ message, which would claim that, it had routing to the Destination Node, and send a RREP response to the Source Node. Destination Nodes and other intermediate nodes (A, B etc.), with available other routing may also send a RREP response to the Source Node. If a legitimate response reaches the source node at first, the network will operate normally, but if Black Hole Node is close to the Source Node, the response information sent by it may reach the Source Node at first, and then the network's security will suffer threat at this time.

However, when a Black Hole Node send wrong message, it doesn't check the routing table, its response information will be more easily to reach the Source Node. In this way, the Source Node will find that the searching routing process has ended, then neglects all the other response information, and begins to send data message. The entire message arriving at Black Hole Node will be discarded simply. Therefore, Black Hole Node can attack the network at a very low price by leading great network traffic to its own.

4. DIFFERENT AODV SECURITY SOLUTIONS AGAINST BLACK HOLE ATTACK IN MANET

4.1 Minimum Modification in AODV

In [6] proposes algorithm to prevent black hole attack at the cost of only marginal processing overhead. The proposed algorithm is simple and does not affect working of either intermediate or destination node. It does not even modify the working of normal AODV but calls a process called Process_RREP. The Process continues to accept RREP packets and calls a process called Compare_RREP (RREP R1, RREP R2) which actually compares the destination sequence number of two route reply and selects the route reply with higher destination sequence number if the difference between two numbers are not significantly high. If the Route reply containing exceptionally high destination sequence number is suspected to be a black hole node and an ALERT message containing the node identification is generated which is broadcasted to neighbor nodes so that any message received from such black hole node is discarded. Then a list of black hole node maintained by the nodes participating in communication which can be used to prevent black hole attack.

In other side, [7] and [8] proposes approach to wait for all routes from the destination or intermediate node so as to find more than one route to the destination (redundant routes, at least three different routes). Then, the source node may unicast a ping packet to the destination using these three routes. Since any packet can arrive to the destination through many redundant paths, Two or more of these nodes must have some shared hops. This solution can guarantee a safe route to the destination, but the main drawback is that there is time delay. Many RREP packets have to be received and processed by the source.

In addition, [7] proposes a second approach, if there are no shared nodes or hops between the routes, the packets will never be sent. The second proposed solution exploits the packet sequence number included in any packet header. The node in this situation needs to have two extra tables; the first table consisting of the sequence numbers of the last packet sent to every node in the network, and the second table is for the sequence number received from every sender. Once the source receives this RREP, it will extract the last sequence number and then compare it with the value saved in its table. If it matches or a slight difference occurs, the transmission will take place. If not, the replied node is a black hole node, so an alarm message will be broadcasted to warn the network about this node.

Also in [9] proposes a mechanism in which the source node initially works in the same way as in AODV routing protocol. When source node receives RREP messages from different intermediate nodes, it just discards the first RREP message coming from any intermediate node for the avoidance of black. In this mechanism, source selects second shortest route for transmission of data packets to destination rather than selecting the first optimal route. But there is a possibility to multiple black hole nodes working in the network so that it might be possible for a black hole node to be part of second optimal route. For identification of the black hole node in the second optimal route, they propose to apply a hash function on the message that has to be sent. But Hash function is cost effective than other authentication techniques.

4.2 Modified RREP (MRREP) Message

In [10] makes use of the destination's unique identifier to detect the black hole in the network. When destination node receives route request, it replies by using MRREP. MRREP is a modified message in normal AODV to include the unique ID of the destination itself to find the black hole node RREP. This can be done easily because the black hole node will not have any knowledge of the unique ID of the destination. Taking into consideration the fact that a black hole node always tries to send a fake RREP with highest sequence number and also that it cannot fake the unique ID of the destination, it is easy to find out the black hole node using the comparison method. The identified Black hole entries are then removed from the Reply Collect Table (RCT) and it is rearranged in the decreasing order of sequence number. The highest sequence number route in the filtered RCT is used to send the data. The disadvantage of this methodology is that, in large scenarios, collecting of all MRREP is time consuming and has memory constraints.

4.3 Intrusion Detection Systems (IDS)

The IDS approach for detecting black hole attack in MANET was introduced in [11]. Intrusion detection can be done in two types: network based intrusion detection and host based intrusion detection. Basically network based intrusion detection works on switches, routers etc. In the mobile ad-hoc networks, there is no central coordinator that monitors the traffic flow among the mobile nodes. They proposes the technique based on the anomaly detection by using host based Intrusion detection system. In this system every activity of a user is monitored and anomaly activities of a malicious node are identified from normal activities. To detect a black hole, this system needs to be provided with a pre¬-collected set of anomaly activities called audit data. The system compares every activity with audit data. Hence, if it finds that any activity of a host is looking like out of the activity provided in the audit data, it isolates that particular node from the network.

In addition, [12] proposed Source Intrusion Detection (SID) approach. This SID approach is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is extended, the SID solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is extended, the delay in the detection period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

4.4 Data Routing Information (DRI)

In [13], [14], [15] introduces the Data Routing Information (DRI) and cross checking method to recognize the cooperative black hole attack, and exploits modified AODV routing protocol to attain this methodology. Each node needs to establish an extra DRI table, where" 1" represents for true and "0" for false. All entry in table is made of two bits, "From" and "Through" which is set for information on routing data packet from the node and through the node likewise. As given in Table 1: the entry (1 1) indicates that node 1 has successfully routed data packets from or through node 3 and the entry of (0 0) means that node 1 has not routed any data packets from or through node 5. The process of proposed solution is merely depicted as: the source node (SN) sends RREQ to each and every node, and then forwards packets to the node which gives reply by the RREP packet. The intermediate node (IN) expressed as the next hop node (NHN) and DRI table to the source nodes (SN) after that the SN cross checks its own table and the received DRI table to verify the IN's sincerity. After that, the SN sends the more request to IN's NHN for asking about its routing information, together with the current NHN, the DRI table of NHNs and its delicate DRI table. At last, the SN evaluates the above information by cross checking to identify the black hole nodes in the routing path. The advantage of this technique is that, it can recognize the multiple collaborative black hole nodes. The main weakness of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of sustain their routing table.

Table 1. DRI for node 1

Node Id	DRI From	DRI Through
3	1	1
5	0	0
2	0	1
4	1	0

4.5 Enhanced Route Discover AODV (ERDA)

In [16] proposes a solution to employ minimum modification to existing AODV algorithm. Three new elements introduced to improve the existing AODV in recvReply() function namely are; a) the *rrep_table* to store incoming RREP packet, b) *mali_list* to keep the detected black hole nodes identity and c) the *rt_upd*, parameter to control the routing table update. Generally, the proposed method is divided into two parts; i) securing routing table update, ii) detecting and isolating black hole node. The source node before receiving any RREP it set rt_upd parameter as 'true' until it receive all the reply. After that it checks on the route reply with the high destination sequence number and discard it, then it keep the detected black hole node in mali_list and notify all the neighbor nodes.

In [17] Extended Enhanced AODV (EEAODV) or extend ERDA by revise the logic and parameters was introduced. The rt_upd parameter is maintained with logic AND. A new condition parameter for checking the RREP packet for better filtering mechanism. Also [18] proposed a Modified Enhanced AODV (MEAODV), where there is a revision of logic as described in EAODV but with few different condition parameters for checking the RREP message for better route discovery mechanism. The MEAODV method works similar to EAODV method except redundancy in the process of detecting black hole node if it exist in intrud_list is prevented.

4.6 Peak Value, Reliable-AODV and Modified Reliable AODV

The peak value approach was introduced in [19], where an intermediate node dynamically calculates a PEAK value after every time interval. It uses three parameters for calculation: RREP sequence number, routing table sequence number and number of replies received during the time interval. The PEAK value is the maximum possible value of sequence number that any RREP can have in the current state. When an intermediate node receives RREP having sequence number higher than the calculated PEAK value, the RREP received is marked as DO_NOT_CONSIDER and is assumed to come from black hole node. Meanwhile, each node receiving the forwarded RREP updates route entry for the black hole node. Source node sending RREQ also appends a list of black hole nodes to inform other nodes in the network about the existence of attackers. Thus, black hole nodes remain isolated from normal nodes. In [20] introduce Modified RAODV, in MR-AODV, when an intermediate node detects a black hole node, it updates the routing table with black hole node entry and discards the RREP to go through source node (it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag). Thus, all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior.

4.7 Trust based Approach

In [21] proposes that every node keeps a trust value on its neighbors and the trust value is calculated as a ratio of number of packets dropped to the number of packets forwarded. In this method every node listens to its neighbor promiscuously. Each node confirms packets sent to neighboring nodes are further forwarded, provided the packet is not destined to that node. Each node monitors the transmission of data packets, not the control packets, so that it can prevent even selective dropping where black hole drops not all packets but only a few selected packets. To verify that packets are forwarded by a neighboring node, a caching mechanism is implemented at every node to collect the packets being forwarded to a neighbor but not destined. If the node cannot tap the same packet from a neighbor node, then a neighbor node further forwards the packet, node will assume the neighbor as black hole node. To determine if it is the same packet, node verifies the tapped packet with the cached packets. If cached packets are not able to be tapped from its neighbor, then those packets are considered to be dropped. When the trust value of a neighbor goes below a threshold value (which is 0.5), then the node will be considered as black hole and will be removed from route and further route selection.

Trust value = 1- (Dropped Packet/Forwarded Packet)

4.8 Utilization of the Gratuitous RREP (G-AODV)

In [22], the AODV protocol has a provision of sending a gratuitous RREP packet to the destination node. Whenever an intermediate node has a route towards destination, in addition to sending the RREP to the source, it also unicasts a gratuitous RREP to the destination node. The gratuitous RREP is conceptualized and simulated as the CONFIRM packet. Thus, a CONFIRM packet is uni- casted/routed by the RREPN (The node that sends an RREP to source node) to the destination. It is only after the receipt of CONFIRM the destination await for packets (i.e. CHCKCNFRM) from the source. Thus, the source unicasts a CHCKCNFRM to the destination. Upon CHCKCNFRMs receipt the destination replies by broadcasting a REPLYCONFIRM to the source. The destination broadcast REPLYCONFIRM only if it received a CONFIRM and a CHCKCNFRM.

4.9 Secure Route Discovery AODV (SRD-AODV)

In [23] proposes three threshold in three environments; for small environment (THs) (THs = [MAXseq * 94]/100), medium environment (THm) (THm = [MAXseq * 96]/100), large environment (THl) (THl = [MAXseq * 98]/100). First, the source nodes use the defined thresholds to verify the multiple RREP messages from their neighbor nodes as given in Fig 2 below.

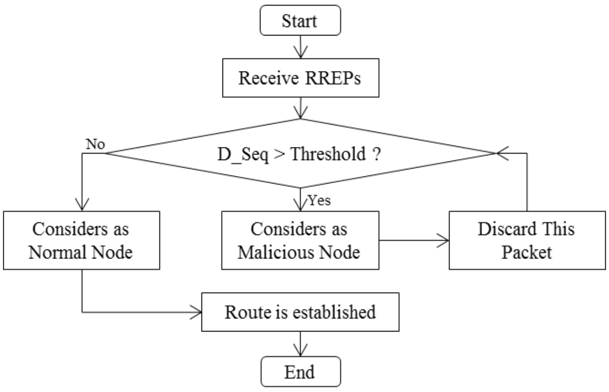

Fig 2. Source node process to verify multiple RREP messages from their neighbor

The source node after receiving multiple replies including one from black hole node based on what is known about fake RREP messages from black hole nodes, the additional function starts by requiring the source node to use the defined threshold to verify the destination sequence number (D_Seq) in each RREP message. If the D_Seq in the RREP message is greater than the defined threshold (TH), the source node considers the message as a fake message generated by a black hole node and discards the packet. Otherwise, a route is established between the source node and the destination node. Second, the destination nodes use the defined thresholds to verify the RREQ messages from the source nodes as given in Fig 3 below.

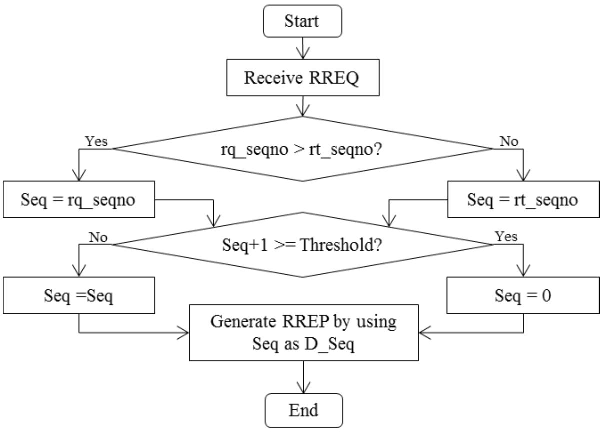

Fig 3. Destination node process to verify multiple RREQ messages from the source node

After an RREQ message has been sent by source node, the destination node gets the sequence number (Seq) from that RREQ message and compares it with the Seq in its routing table. If the Seq value in the RREQ message is greater than the Seq value in its routing table, the destination node selects the Seq from the RREQ message. If otherwise, it selects the sequence number from its routing table. Additionally, the Seq value that is selected by the destination node must be incremented by one and must be verified using the defined threshold. If the Seq value is greater than or equal to the defined threshold, the Seq value is updated to zero (0). If otherwise, the destination node will use the Seq value to generate the RREP message.

4.10 Opinion AODV (OAODV)

In [1] proposes algorithm that makes assumption about the black hole node having the ratio of number of RREQs transmitted to the number of RREPs transmitted. If it is less, then the black hole node can be detected in this way. Two extra fields are used in opinion AODV (OAODV) - *request weight* and *reply weight*. Request weight in routing table indicates the number of RREQs that are forwarded by the corresponding node. Similarly Reply weight indicates the number of RREPs forwarded. Proposed method has two modules-*updating request/reply weights* and *collecting feedback*.

Updating weights; in the normal process of route discovery of AODV whenever a node receives RREQ/RREP, Request weight/Reply weight is incremented in its routing table. Weights are updated against the routing entry from which RREQ/RREP received. These values reflect the participation of nodes in the routing process. Also the weights are updated only if forwarded node is not the originator of the corresponding control packet. If forwarded node is originator, then it implies that it is forwarding for its own purpose not for others. For a node and all its neighbors know the participation of node in routing. Neighbors can give feedback for the node.

Collecting Feedback; for the source node to verify multiple received RREP, two new control packets are used; Opinion Request (OREQ) and Opinion Reply (OREP). Source node calculates the ratio of request weight to reply weight for each path. If the weights ratio is very low then there might be black hole node in that path. Otherwise route with highest destination sequence number is chosen to transfer application layer data.

5. SUMMARY

Table 2: Summary of different AODV security solutions against black hole attack in MANET

Techniques	Proposed Protocol	Types of Attacks	Publication Year
Minimum Modification in AODV Protocol	AODV	Single and multiple black hole attack	2012 and 2013
Modified RREP (MRREP) Message	AODV	Two black hole attack	2013
Intrusion Detection Systems (IDS)	AODV	1, 2 and multiple black hole attack	2010, 2011
Data Routing Information (DRI)	AODV	Cooperative black hole attack	2011, 2013 and 2014
Enhanced Route Discover AODV	ERDA	1, 2 and 3 black hole attack	2011 and 2013
Peak Value, Reliable-AODV and Modified Reliable AODV	RAODV, M-RAODV	Single and multiple black hole attack	2012 and 2013
Trust Based Approach	AODV	Single black hole attack	2012
Utilization of the Gratuitous RREP	G-AODV	1 and 2 black hole attack	2013
Secure Route Discovery AODV	SRD-AODV	Single black hole attack	2013
Opinion AODV	OAODV	Single black hole attack	2012

6. CONCLUSION

Most of the discussed research papers were focused on improving the security of AODV routing protocol against black hole attack. In many cases the proposed improvement were done by modifying the existing AODV routing protocol with the cost of routing overhead and delay. Without any attack, AODV is a convenient routing protocol to use in MANET. But when single, multiple or cooperate black hole attack exist in network using AODV as a routing protocol, most of the packet would be dropped as a result the network performance will dramatically fall.

In MANET there is no central devices for controlling the network traffic which makes it so hard to decide where to put the security mechanism. However, putting a security mechanism at every node in the network will affect the network performance by increasing the network overhead. In this case, detecting and preventing a black hole attack remain the challenging task. So the need to improve the security of AODV routing protocols so as to increase the performance in the presence of black hole attack while reducing the cost is vital.

7. REFERENCES

[1] R. Yerneni and A. K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc," in Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, 2012, pp. 1-5.

[2] N. Jadeja and R. Patel, "Performance evaluation of aodv, dsdv and dsr routing protocols using ns-2 simulator," Performance Evaluation, vol. 3, pp. 1825-1830, 2013.

[3] M. Roopak and B. Reddy, "Blackhole Attack Implementation in AODV Routing Protocol," International Journal of Scientific & Engineering Research, vol. 4, pp. 402-406, 2013.

[4] K. K. Varshney and P. Samundiswary, "Performance analysis of malicious nodes in IEEE 802.15. 4 based wireless sensor network," in Information Communication and Embedded Systems (ICICES), 2014 International Conference on, 2014, pp. 1-5.

[5] A. Gurjar and A. Dande, "Black Hole Attack in Manet's: A Review Study," International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN, pp. 2319-4413, 2013.

[6] K. S. Chavda and A. V. Nimavat, "Removal of black hole attack in AODV routing protocol of MANET," in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-5.

[7] N. Sharma and A. Sharma, "The black-hole node attack in MANET," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, 2012, pp. 546-550.

[8] S. Agrawal and S. Jaiswal, "Study to Eliminate Threat of Black Hole of Network Worms in MANET." International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.

[9] M. Amaresh and G. Usha, "Efficient malicious detection for AODV in mobile ad-hoc network," in Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, 2013, pp. 263-269.

[10] S. S. Narayanan and S. Radhakrishnan, "Secure AODV to combat black hole attack in MANET," in Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, 2013, pp. 447-452.

[11] Y. F. Alem and Z. C. Xuan, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," in Future Computer and Communication (ICFCC), 2010 2nd International Conference on, 2010, pp. V3-672-V3-676.

[12] M. Abdelhaq, S. Serhan, R. Alsaqour, and R. Hassan, "A local intrusion detection routing security over MANET network," in Electrical Engineering and Informatics (ICEEI), 2011 International Conference on, 2011, pp. 1-6.

[13] G. Wahane, A. M. Kanthe, and D. Simunic, "Technique for detection of Cooperative black hole attack using true-link in Mobile Ad-hoc Networks," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on, 2014, pp. 1428-1434.

[14] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, 2011, pp. 338-343.

[15] A. Mishra, R. Jaiswal, and S. Sharma, "A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network," in Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013, pp. 499-504.

[16] K. Abd Jalil, Z. Ahmad, and J. Manan, "Securing Routing Table update in AODV routing protocol," in Open Systems (ICOS), 2011 IEEE Conference on, 2011, pp. 116-121.

[17] Z. Ahmad, K. Abd Jalil, and J. Manan, "Black hole effect mitigation method in AODV routing protocol," in Information Assurance and Security (IAS), 2011 7th International Conference on, 2011, pp. 151-155.

[18] A. Gupta, "Black hole attack mitigation method based on route discovery mechanism in AODV protocol," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, 2013, pp. 1-6.

[19] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, 2012, pp. 556-560.

[20] R. H. Jhaveri, "MR-AODV: a solution to mitigate blackhole and grayhole attacks in AODV based MANETs," in Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on, 2013, pp. 254-260.

[21] F. Thachil and K. Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET," in Computing Sciences (ICCS), 2012 International Conference on, 2012, pp. 281-285.

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

[23] S. Tan and K. Kim, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs," in ICT Convergence (ICTC), 2013 International Conference on, 2013, pp. 1027-1032.