

## IMPROVED MCBDS FOR DEFENDING AGAINST GRAY HOLE AND BLACK HOLE ATTACKS IN MANETS

Ahmad Haghighi<sup>1</sup>, Kiarash Mizanian<sup>1</sup>, Ghasem Mirjalily<sup>1</sup>

<sup>1</sup> Faculty of Electrical and Computer Engineering, Yazd University, Yazd, Iran, e-mail: haghighi.ahmad@gmail.com, k.mizanian@yazd.ac.ir, mirjalily@yazd.ac.ir

Received: 2016.03.01  
Accepted: 2016.04.25  
Published: 2016.06.01

### ABSTRACT

Mobile Ad-hoc Networks (MANETs) are widely used nowadays. Because of their characteristics as open media, dynamic topology, being infrastructure-less and lack of centralized monitoring, MANET is vulnerable to a wide range of attacks like blackhole and grayhole. Blackhole and grayhole attacks refer to the attacks that breach the security by performing packet forwarding and routing misbehavior and cause denial of service in MANETs. In this paper we improved our previous work on MCBDS, we reduced false-positive rate more than before and on average it dropped to zero. The proposed method employs Network Simulator-2 (NS-2) to validate the effectiveness under different scenarios. Simulation results show that improved MCBDS has same performance as CBDS in terms of throughput and end-to-end delay and as much as the presence of malicious nodes increased, improved MCBDS performs better than CBDS.

**Keywords:** mobile ad hoc network, cooperative bait detection scheme(CBDS), modified CBDS (MCBDS), black hole, gray hole, MANET.

### INTRODUCTION

Mobile ad-hoc networks have become increasingly popular in recent years because of their characteristics like, infrastructure-less architecture, dynamic topology, self-configuring and cheaper price. Due to these characteristics they are used in military operations, rescue operations that there is not a communication infrastructure or existing infrastructures are destroyed, voting systems and local applications like conferences, classrooms and homes for connecting devices [1].

One of the most obvious indicators of mobile ad-hoc networks is lack of infrastructure, So that each node in the network, in addition to being a host, acts as a router and for transmitting a packet from source to destination, nodes must cooperate with each other. Dynamic topology, lack of central monitoring and need for cooperating makes this network more vulnerable. For example, in

blackhole and grayhole attacks, malicious nodes can disrupt routing function and cause decrease of network performance.

In blackhole attacks, a malicious node sends fake information and claims it has a valid shortest route to reach the destination node, so the source node seduced and sends packets to the specified path. After that when data packets received by malicious node, it drops all of them. In grayhole attacks, malicious node acts like blackhole, but in dropping packets behaves differently, for example sometimes acts like normal nodes and forward packets and in specific times drop receiving packets or drop certain (e.g. based on type or destination) packets and forward others [2]. This variable and flexible behavior of grayhole attackers mislead most of the detection mechanisms and make its detection harder than blackhole.

Dynamic Source Routing (DSR) [3] is a common routing protocol for MANET. The DSR protocol contains two main mechanisms, Route

Discovery and Route Maintenance, which work together to allow the discovery and maintenance of source routes. In Route discovery when a sender wants to send some packets to a destination, if it does not have a route to destination, it broadcast a route request (RREQ) packet, when this packet is received by intermediate nodes, they search their route cache for a valid route to destination; and if found, inform the source node by unicasting a Route Reply (RREP) packet otherwise inserts its own address in RREQ and broadcast it. Route request broadcasted in the network and if it received by destination node, destination would use the stored path in RREQ and sends a RREP to source node, also intermediate nodes on the path, store path in their route cache. When the source node received some RREPs, it chooses the best path and sends packets through it.

There are several different mechanisms for detection and combat against blackhole/grayhole attacks, with each one having its own advantages, weaknesses and usages. For example some mechanism works based on Intrusion Detection Systems (IDS) [4] and some nodes in the network play IDS role which is based on MANET specifications, IDS with dynamic hierarchical structure is a good choice [5]. Some other mechanisms are Trust Based [6–9], which is based on nodes' history and observation each node earns a trust level that is used for routing and detection. Usually these methods are more vulnerable to grayhole attacks. Some mechanism improves the existing routing protocols and decreases vulnerabilities.

In this paper we improved our previous work MCBDS[10], the CBDS [11] suffers from false-positive in detection, so in previous MCBDS we modified detection phase to increase accuracy and decrease the false-positive rate, also we reduced processing load and the size of routing packets by removing and summarizing some transferred data and some operations so the performance increased and accuracy is preserved. Also in previous MCBDS false-positive decreased, but still in some scenarios one or two safe node has been detected as malicious; so in improved MCBDS we changed implementation of MCBDS to increase its accuracy.

## RELATED WORKS

Many studies have been proposed for detection and combat against malicious nodes in MANETs. The existing studies can be catego-

rized based on their specifications and applications, for example: which kind of attack can be detected (blackhole, grayhole or both), what number of malicious nodes can be detected simultaneously (in each operation), the detection mechanism (Proactive [12, 13]/Reactive [14, 15] detection) and usability in all environments or exclusive to specific environments (requires specific assumption and conditions).

In [16] the authors propose a method based on AODV routing protocol to defend against blackhole attacks. They add another table with three columns to AODV named DRI. In the DRI table, 1 stands for 'true' and 0 for 'false', first column is "Node number", second is "From" and value 1 means we received data packet(s) from respective node, third column is "Through" and values 1 means we have sent the data packet(s) through a respective node. Therefore, when RREP is received, if needed the source node sends a further RREQ and in response relevant node(s) sends its/their DRI table, finally the source node compares DRI tables and decides whether a node is malicious or not. After them in [17] Singh Bindra et al. improved DRI and name it EDRI table and afterwards in [18] authors improved EDRI table and name it Modified EDRI.

In [19] Jhaveri improved their previous work (R-AODV [20, 21]) and named it MR-AODV. In MR-AODV each node based on its own observations and received RREP and RREQ packets, calculate a 'PEAK' value, then for each received RREP, node compares its sequence number with PEAK value. If PEAK is less than a sequence number, the node detects the sender of RREP as a malicious node, and so informs all other nodes by sending a RREQ with an attached list of malicious nodes. It is worth mentioning that PEAK is the biggest value which a RREP can have, so as a malicious node usually uses a big number for its RREP packets (to cheat the source node), the malicious node can be detected by MR-AODV.

In [22] Mohanapriya and Krishnamurthi proposed an approach to combat grayhole attacks by improving DSR routing protocol. They send data in some blocks, and the receiver is aware of size of blocks; therefore, if the receiver observed a considerable decrease in size of received blocks, it would initiate a malicious detection phase. First, it sends a Query Request (QREQ) packet to the node in the source route at a 2-hop distance from it, in

response to QREQ; node sends the number of data packets which forwarded to its next hop neighbor in the source route. When QREP received, the destination node it verifies whether its previous hop is correctly forwarding all the data packets it receives from its previous node or not. If not correct, the destination node considered both one hop and two hop previous nodes as suspect nodes and asks IDS nodes to monitor them. If correct, it means that those two nodes are normal and repeat the procedure for 4-hop distance from it and so on.

In [11] the authors improved their previous work (CBDS [23]). CBDS is based on DSR routing protocol and can prevent and detects blackhole and grayhole nodes. In CBDS before sending RREQ, the source node cooperates with one of its one-hop neighbors and uses its address as destination address (bait destination address) for a RREQ packet known RREQ'. As the malicious node responds to any RREQ, bait RREQ (RREQ') used to bait the malicious node(s) to send a RREP message, thus based on mechanisms proposed in CBDS, source node can detect the sender of fake RREP, so mark it as a malicious node and inform other nodes to will not be participated in the Route Discovery. The CBDS has a threshold for packet loss which if packet loss in the network exceed the value, the algorithm starts the detection phase again. The CBDS is both Proactive and Reactive, because it initiates a bait phase independently (regardless of existence of malicious nodes) to detect malicious nodes (Proactive) and is able to trigger detection phase while node detects a significant drop in the packet delivery ratio (Reactive).

## PROPOSED METHOD

### The CBDS

The Cooperative Bait Detection Scheme (CBDS) has three steps:

- 1) Initial Bait Step,
- 2) Initial Reverse Tracing Step,
- 3) Shifted to Reactive Defense Phase.

#### Initial Bait Step

The source node selects an adjacent node stochastically i.e.  $n_r$  within its one-hop neighborhood nodes and uses the address of this node as

bait destination address to bait malicious nodes to send a reply (RREP) message. The bait setup step initiated whenever the bait RREQ' is sent earlier for seeking the initial routing path. The analysis procedures of follow-up bait phase, are as follows:

- If the  $n_r$  node had not launched a blackhole attack, then after the source node had sent out the RREQ', there would be other nodes' reply RREP in addition to that of the  $n_r$  node. This indicates that the malicious node existed in the reply routing. Therefore, the reverse tracing program in the next step would be initiated in order to detect this route.
- If only the  $n_r$  node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase.
- If  $n_r$  had been the malicious node of the blackhole attack, then after the source node had sent the RREQ', other nodes (in addition to the  $n_r$  node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. In this case, the reverse tracing program in the next step would be initiated to detect this route.
- If  $n_r$  deliberately gave no reply RREP, it would be directly listed on the blackhole list by the source node
- If only the  $n_r$  node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that  $n_r$  had provided; in this case, the route discovery phase of DSR will be started.

#### Initial reverse tracing step

In this step the malicious nodes are detected through its route reply (RREP) to the RREQ'. Whenever a malicious node has received the RREQ', it will reply with a false RREP. If the intermediate node  $n_i$  receives the RREP, it will separate the P list (1) by the destination address  $n_i$  of the RREP in the IP field and get the address list  $K_i = \{n_1 \dots n_i\}$ , where P is the recorded path in the RREP, and  $K_i$  represents the route information from source node S to destination node  $n_k$ . After that, node  $n_k$  determines the differences between the address P list and  $K_i$  list to calculate  $K'_i$  as in (2).  $K'_i$  represents route information to the destination node (3).

$$P = \{n_1 \dots n_k \dots n_m \dots n_r\} \quad (1)$$

$$K'_i = P - K_i \quad (2)$$

$$K'_i = \{n_{k+1} \dots n_m \dots n_r\} \quad (3)$$

The  $K'_i$  is stored in the RREP's "Reserve field" and they reverted to the source node, then the source node calculates the dubious path S and trusted path T as in (4) and (5).

$$S = K'_1 \cap K'_2 \cap \dots \cap K'_i \quad (4)$$

$$T = P - S \quad (5)$$

After calculating T set, the source node sends the test packets to this route and sends the recheck message to the second node toward the last node in T and ask from it to entered a promiscuous mode in order to listen to which node the last node in T sent the packets to and fed the result back to the source node. By these received results source node can detect the malicious node(s).

### Shifted to Reactive Defense Phase

In this phase if destination found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again.

### The Modified CBDS

The CBDS [11] suffers from false-positive in detection. In modified CBDS, we modified second step (Initial reverse tracing step) of CBDS and added some operations to reduce the false-positive rate, also we improved performance in terms of throughput, end-to-end delay and energy consumption by decreasing routing overhead.

### Decrease false-positive rate

In the first step of CBDS methodology authors claim after selecting Bait and sending RREQ', if node  $n_r$  is not malicious, we must receive only one RREP, moreover, the received RREP must be from node  $n_r$ , otherwise exist malicious node(s) in the network.

In DSR (also CBDS) intermediate nodes can response to RREQs and send RREP based on their route cache (if we limit sending RREP only to destination node(s), we ignored a grand feature moreover CBDS is useless). So the authors' claim is not true for all scenarios, for example in Figure 1, network is secure and there is not any malicious node but the source node receives more than one RREP.

In Figure 1 Source Node S cooperates with node  $n_r$  and sends a RREQ' packet. Assume ev-

ery node is in its transmission range before and after its neighbors. RREQ' packet received by node number 7 through path S-1-2-3-4-5-6 and received by node  $n_r$  through path S- $n_r$ . As node 7 and node  $n_r$  are neighbors (or in general node 7 have a route to  $n_r$ ), node 7 sends a RREP, thus source node S receives 2 RREP and for CBDS it means there is malicious node(s) in the network so initiate second phase to detect the hypothetical malicious node. Therefore, the source node sends a RREQ' and in response receives  $P = \{S-1-2-3-4-5-6-7-n_r\}$  and  $K'_i$  sets (6) and calculate S list (7) and T lists (8).

$$K'_6 = \{7-n_r\}, K'_5 = \{6-7-n_r\}, K'_4 = \{5-6-7-n_r\}, K'_3 = \{4-5-6-7-n_r\}, K'_2 = \{3-4-5-6-7-n_r\}, \quad (6)$$

$$K'_1 = \{2-3-4-5-6-7-n_r\},$$

$$K'_s = \{1-2-3-4-5-6-7-n_r\}$$

$$S = K'_s \cap K'_1 \cap K'_2 \cap K'_3 \cap K'_4 \cap K'_5 \cap K'_6 \quad (7)$$

$$K'_6 = \{7-n_r\}$$

$$T = P - S = \{S-1-2-3-4-5-6\} \quad (8)$$

After calculating T set, the source node sends the test packets to this route and sends the recheck message to Node number 5 and asks from it to enter a promiscuous mode in order to listen to which node the node number 6 sent the packets to and fed the result back to the source node. There is not any malicious node in our scenario, so node 6 forward packets to node 7 and node 5 observe it and inform source node; therefore, the source node makes a mistake and detects node 7 as a malicious node. To overcome such mistakes and for reducing false-positive rate, in proposed scheme, we added another step to second phase of CBDS (i.e. reverse tracing), in which node  $n_r$  must respond to test packets received from path P, and the source node after receiving response of recheck message (from node 5) waits for response of node  $n_r$  to the test packets for a specific

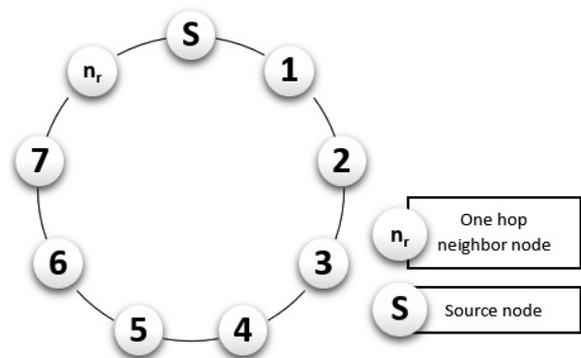


Fig. 1. A network scenario with no malicious node

time  $tt_r$  (9), which dynamically calculated based on time of receiving the response of recheck message and length of T and S. If the source node does not receive any response during its waiting time  $tt_r$ , it marks node 7 as a malicious node and informs other nodes; otherwise, node 7 is secure ( $t_{rck}$  is the time which takes packet from 5 reach to the source node and  $\alpha$  is a constant number).

$$tt_r = 2 * t_{rck} * \left( \frac{n(S)}{n(T)} + 1 \right) + \alpha \quad (9)$$

### Reduce routing overhead

As mentioned before, every node in CBDS while receive a RREP, calculates relevant  $K'_i$ , append it to the RREP and forward it. Therefore, when RREP is received by source node, this information used to calculate T list. The number of  $K'_i$  is between 0 to  $n(P)^1$ , and each one has between 1 to  $n(p)-1$  element. Every element is a node address, so in average every RREP carries  $n(P)^2/4$  address (10).

$$\frac{n(P)^2}{4} \approx \sum_{i=n(P)-x}^{n(P)-1} i = \frac{3n(P)^2 - 4n(P)}{8} \quad (10)$$

In modified CBDS, instead of calculation  $K'_i$  lists and appending them to RREP, every node just inserts its own address in the RREP and forward it. Thus in average each RREP carry  $n(P)/2$  address (11) and after receiving RREP, in worth case source node only need to sort received addresses to calculate T list.

$$\frac{n(P)}{2} \approx \frac{(n(P)-1)+0}{2} \quad (11)$$

Consequently, in modified CBDS we decreased size of RREPs by reducing the number of inserted addresses from (10) to (11), -note that (10) is square of (11) – also on average; operations from  $n(P)/2 + 1$  difference and intersect between  $n(p)/2$  sets, reduced to only sorting one set.

**Table 2.** Simulation parameters per sub-Scenario

Parameter	Sub-scenario name	n15_s10	n15_s30	n30_s10	n30_s30
Number of nodes		15	15	30	30
Min speed		1	1	1	1
Max speed		10	30	10	30

## SIMULATION

### Simulation parameters

Simulations carried out on Network Simulator 2 (NS-2) simulator [24], version 2.35 installed in Ubuntu 14.04 LTS 32bit. We considered 16 scenarios for simulations. A simulation has 4 categories and each category has 4 sub-scenarios. In category 1 we did not have any malicious node in the network, in category 2 one node randomly selected as malicious, in category 3 exist 3 random malicious node and in category number 4, 40 percent of total nodes are malicious. Simulation done during 100 second in a 500 m x 500 m area, whose position and mobility of each one is random. Common parameters between all categories presented in Table 1 and specific parameters of each sub-scenario are presented in Table 2.

**Table 1.** Common simulation parameters

Parameter	Value
Coverage area	500 x 500 m
Simulation time	100 s
Mobility	random
Pause time	0.0
Connections	3 CBR
Packet Size	512 byte
Rate	2 Mb
Radio range	250 m
Threshold	fixed (90%)
$\alpha$	2 sec

### Performance metrics

We use following metrics to compare the performance between CBDS and modified CBDS:

- **Average End-to-End Delay.** This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is  $d_i$ , and the number of packets received by the destination node is  $pktd_i$ . The

average end-to-end delay for n application traffics, which is denoted by E, is obtained as:

$$E = \frac{1}{n} \sum_{i=1}^n \frac{d_i}{pkt d_i} \quad (12)$$

- **Throughput.** This is defined as the total amount of data (bi) that the destination receives them from the source divided by the time (ti) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput for n application traffics, which is denoted by T, is obtained as:

$$T = \frac{1}{n} \sum_{i=1}^n \frac{b_i}{t_i} \quad (13)$$

- **False Positive Rate.** This is defined as the total number of secure nodes which is detected as malicious divided by the number of secure nodes:

$$FPR = \frac{n(\text{Malicious list})}{\text{Number of Secure Nodes}} \quad (14)$$

## SIMULATION RESULTS

### Throughput and End-to-End Delay

In modified CBDS, although the source node waits for receiving the response to the test packets from nr (for decrease false-positive rate) and this operation inserts some delay in routing; but in comparison to CBDS some routing operations summarized (K' sets) and some operations removed (e.g. intersect and difference), so as shown in Figure 2 and Figure 3 throughput is similar for both CBDS and MCBDS. In category 1 which there isn't any malicious node in the network, CBDS works a little better than MCBDS, but as much as rate of malicious node increased, MCBDS overcomes CBDS and MCBDS has a better performance in term of End-to-End Delay. For Throughput as shown in Figure 4 and Figure 5 performance is like End-to-End Delay and MCBDS performs better than CBDS for networks with malicious nodes.

In scenarios with long distance between source and destination (e.g. large networks) this improvement is more obvious, because the

number of hops between source and destination increased and in CBDS as in (10) number of inserted addresses in RREP is the square of hop counts, but in modified CBDS, (11) is linear so in big scenarios with long duration time and large network (area and number of nodes), simulations under CBDS fails but for MCBDS simulations finished successfully.

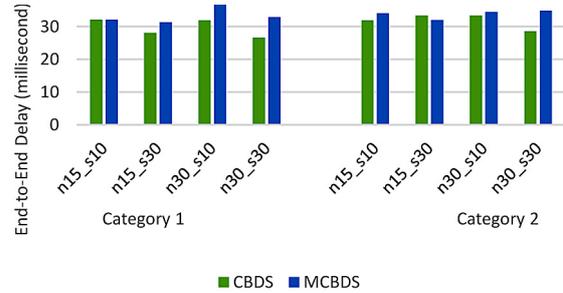


Fig. 2. End-to-End Delay under category 1 and 2

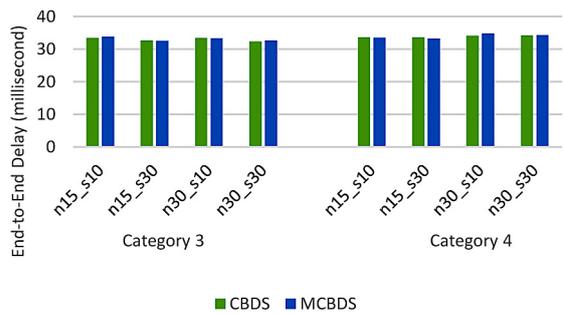


Fig. 3. End-to-End Delay under category 3 and 4

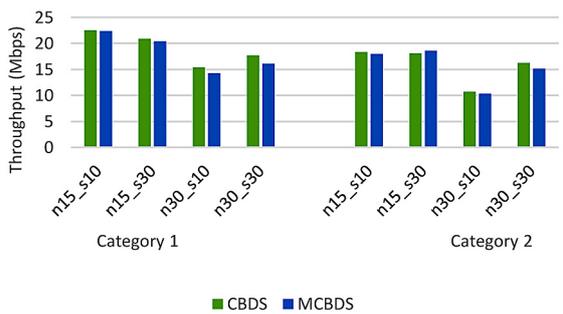


Fig. 4. Throughput under category 1 and 2

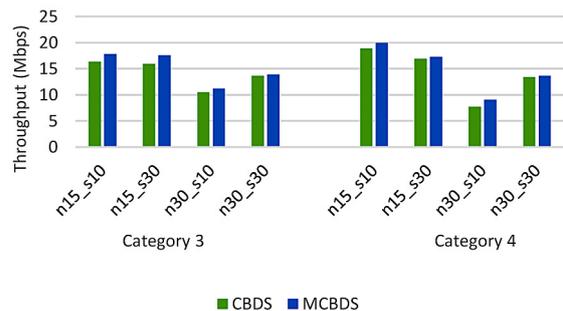


Fig. 5. Throughput under category 3 and 4

## False Positive Rate

Any node has a Malicious List which contains address of nodes that detected as malicious, at the end of simulations after removing address of real malicious node(s); number of safe nodes which wrongly detected as malicious calculated and used in FPR calculation (14). Figure 6 shows False-positive rate for CBDS.

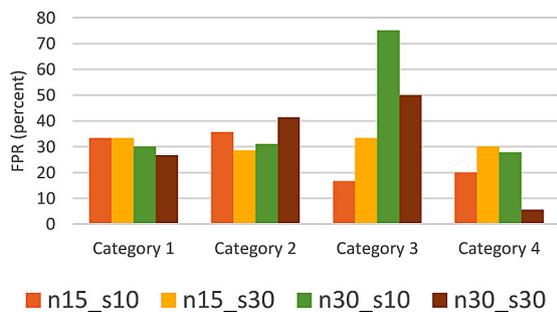


Fig. 6. False Positive Rate under different scenarios

## CONCLUSION

Security of mobile ad-hoc network is a big challenge, default routing protocols are vulnerable to blackhole and grayhole attacks. In this paper, we focus on CBDS scheme (a DSR based routing protocol, able to tackle blackhole and grayhole attacks) and propose Modified CBDS. Simulation results prove that in MCBDS false-positive rate dropped close to zero and almost performance (in terms of throughput and end-to-end delay) preserved.

## REFERENCES

1. Aarti, SS. Tyagi, Study of Manet: Characteristics, Challenges, Application And Security Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3 (5), 2013, 252–257.
2. Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. DoS attacks in mobile ad hoc networks: A survey. *Advanced Computing & Communication Technologies (ACCT)*, 2012 Second International Conference on. IEEE, 2012.
3. Johnson, David, Y. Hu, and D. Maltz. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. No. RFC 4728. 2007.
4. Anantvalee, Tiranuch, and Jie Wu. A survey on intrusion detection in mobile ad hoc networks. *Wireless Network Security*. Springer US, 2007, 159–180.
5. Haghghi A., Hajiramezan S., and Mizanian K. Providing a new method to deal with th Byzantine attack in intrusion detection system with dynamic hierarchy in MANETs (in Persian), *Second National Conference on Applied Research in Computer & Information Technology*. CIVILICA, 2014.
6. Thachil, Fidel, and K.C. Shet. A trust based approach for AODV protocol to mitigate black hole attack in MANET. *Computing Sciences (ICCS)*, 2012 International Conference on. IEEE, 2012.
7. Bhalaji, N., et al. Trust based strategy to resist collaborative blackhole attack in MANET. *Information Processing and Management*. Springer Berlin Heidelberg, 2010, 468–474.
8. Marchang, Ningrinla, and Rohit Datta. Lightweight trust-based routing protocol for mobile ad hoc networks. *Information Security, IET*, 6 (2), 2012, 77–83.
9. Aggarwal, Akshai, et al. Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs. *Advanced Computing & Communication Technologies (ACCT)*, 2014 Fourth International Conference on. IEEE, 2014.
10. Haghghi A., Mizanian K., and Mirjalily G., Modified CBDS for defending against collaborative attacks by malicious nodes in MANETs. *IEEE 2015, 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*. IEEE, 2015.
11. Chang, Jian-Ming, et al. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *Systems Journal, IEEE*, 9 (1), 2015, 65–75.
12. Baadache, Abderrahmane, and Ali Belmehdi. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. *arXiv preprint arXiv, 1002 (1681)*, 2010.
13. Liu, Kejun, et al. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *Mobile Computing, IEEE Transactions on* 6 (5), 2007, 536–550.
14. Kozma, William, and Loukas Lazos. REAct: resource-efficient accountability for nodemisbehavior in ad hoc networks based on random audits. *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009.
15. Wang, Weichao, Bharat Bhargava, and Mark Linderman. Defending against collaborative packet drop attacks on manets. *2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)(in Conjunction with IEEE SRDS 2009)*, New York, USA, 27, 2009.
16. Ramaswamy, Sanjay, et al. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. *International Conference on Wireless Networks*, 2003.

17. Bindra, Gundeep Singh, et al. Detection and removal of co-operative blackhole and grayhole attacks in MANETs. *System Engineering and Technology (ICSET), 2012 International Conference on*. IEEE, 2012.
18. Hiremani, Vani, and Manisha Madhukar Jadhao. Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. *Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on*. IEEE, 2013.
19. Jhaveri, Rutvij H. MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. *Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on*. IEEE, 2013.
20. Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. A novel solution for grayhole attack in aodv based manets. *Advances in Communication, Network, and Computing*. Springer Berlin Heidelberg, 2012, 60–67.
21. Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. A novel solution for grayhole attack in aodv based manets. *Advances in Communication, Network, and Computing*. Springer Berlin Heidelberg, 2012, 60–67.
22. Mohanapriya, M., and Ilango Krishnamurthi. Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers & Electrical Engineering*, 40 (2), 2014, 530–538.
23. Chang, Jian-Ming, et al. CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture. *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VI-TAE), 2011 2nd International Conference on*. IEEE, 2011.
24. The Network Simulator - ns-2. [Online]. Available: <http://www.isi.edu/nsnam/ns/>. [Accessed: 31-Dec-2014].