2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)
November 5-6, 2015
(Iran University of Science and Technology) – Tehran, Iran

Modified CBDS for defending against collaborative attacks by malicious nodes in MANETs

Ahmad Haghighi, Kiarash Mizanian and Ghasem Mirjalily
Faculty of Electrical and Computer Engineering
Yazd University
Yazd, IRAN
haghighi.ahmad@stu.yazd.ac.ir, k.mizanian@yazd.ac.ir, mirjalily@yazd.ac.ir

***Abstract*— Mobile Ad-hoc Networks (MANETs) are widely used nowadays. Because of its characteristics like open medium, 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 proposed two improvements to Cooperative Bait Detection Scheme (CBDS), we reduced both the false-positive rate in detection and the routing overhead. The proposed method (called Modified CBDS) employs Network Simulator-2 (NS-2) to validate the effectiveness under different scenarios. Simulation results show modified CBDS has a better performance in terms of throughput, end-to-end delay and energy consumption.**

Keywords—Mobile ad-hoc network (MANET); Cooprative bait detection scheme; Modified CBDS; Blackhole; Grayhole attack

I. Introduction

Mobile ad-hoc networks have become increasingly popular in recent years because of their characteristic 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, the 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, that 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, broadcast a route request (RREQ) packet, when this packet 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, choose best path and send packets through it.

There are several different mechanisms for detection and combat against blackhole/grayhole attacks, which each one has 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 based on MANET specifications, IDS with dynamic hierarchical structure is a good choice [5]. Some other mechanisms are Trust Based [6]–[9], which based on nodes' history and observation each node earns a trust level that used for routing and detection. Usually these methods are more vulnerable to grayhole attacks. Some mechanism improves existing routing protocols and decreases vulnerabilities.

In this paper, we modified CBDS [10] protocol; the CBDS suffers from false-positive in detection, so we modified detection phase to increase accuracy and decrease the false-

978-1-4673-6506-2/15/$31.00©2015 IEEE

positive rate, also we reduced processing load and size of routing packets by removing and summarizing some transferred data and some operations so performance increased and accuracy preserved. Rest of the paper is organized as follows. Section II presents the related works. Section III describes our proposed method. Simulation results and analysis are presented in Section IV. Finally, conclusions are drawn in Section V.

II. Related Works

Many studies have been proposed for detection and combat against malicious nodes in MANETs. Existing studies can be categorized based on their specifications and applications, for example: which kind of attack can be detected (blackhole, grayhole or both), number of malicious nodes can be detected simultaneously (in each operation), the detection mechanism (Proactive [11], [12] /Reactive [13], [14] detection) and usability in all environments or exclusive to specific environments (requires specific assumption and conditions).

In [15] 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 respective node. Therefore, when RREP 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 [16] Singh Bindra et al. improved DRI and name it EDRI table and afterwards in [17] authors improved EDRI table and name it Modified EDRI.

In [18] R. Jhaveri improved their previous work (R-AODV [19], [20]) 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 be less than sequence number, node detects the sender of RREP as a malicious node, so inform 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 [21] Mohanapriya and Krishnamurthi proposed an approach to combat grayhole attacks by improving DSR routing protocol. They send data in some blocks, and receiver is aware of size of blocks; therefore, if the receiver observed a considerable decrease in size of received blocks, would initiate 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 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 procedure for 4-hop distance from it and so on.

In [10] authors improved their previous work (CBDS [22]). 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, 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).

III. Proposed Method

A. 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.

1) 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.

a) 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

b) 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.

c) 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.

d) If n_r deliberately gave no reply RREP, it would be directly listed on the blackhole list by the source node

e) 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.

2) 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_1 of the RREP in the IP field and get the address list $K_i = \{n_1 . . . n_i\}$, 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).

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

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

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

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), (5).

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

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

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).

3) 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.

B. The Modified CBDS

The CBDS [10] 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.

1) 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 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 authors' claim is not true for all scenarios, for example in Fig. 1, network is secure and there is not any malicious node but the source node receives more than one RREP.

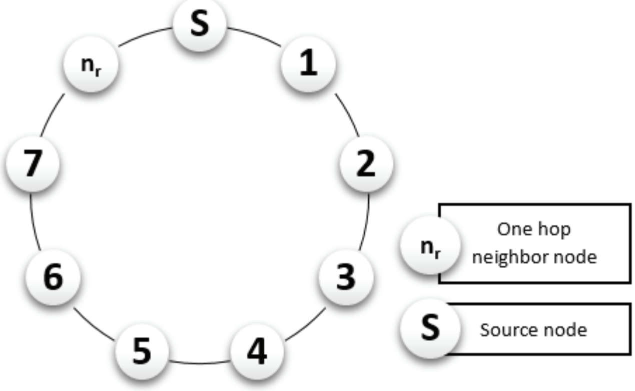

Fig. 1. A network scenario with no malicious node

In Fig. 1 Source Node *S* cooperates with node n_r and sends a RREQ' packet. Assume every node is in transmission range of it's before and after 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).

$$K'_6=\{7\text{-}n_r\},\ K'_5=\{6\text{-}7\text{-}n_r\},\ K'_4=\{5\text{-}6\text{-}7\text{-}n_r\},\ K'_3=\{4\text{-}5\text{-}6\text{-}7\text{-}n_r\},\ K'_2=\{3\text{-}4\text{-}5\text{-}6\text{-}7\text{-}n_r\},\ K'1=\{2\text{-}3\text{-}4\text{-}5\text{-}6\text{-}7\text{-}n_r\},\ K'_S=\{1\text{-}2\text{-}3\text{-}4\text{-}5\text{-}6\text{-}7\text{-}n_r\} \quad (6)$$

$$S = K'_S \cap K'_1 \cap K'_2 \cap K'_3 \cap K'_4 \cap K'_5 \cap K'_6 = \{7\text{-}n_r\} \quad (7)$$

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

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 avoid such mistakes and to reduce the false-positive rate, 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 n_r's response for a specific time (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, it marks node 7 as a malicious node and informs other nodes; otherwise, node 7 is secure.

2) 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 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 (9).

$$n(P)^2/4 \quad (9)$$

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 (10) and after receiving RREP, in worth case source node only need to sort received addresses to calculate *T* list.

$$n(P)/2 \quad (10)$$

Consequently, in modified CBDS we decreased size of RREPs by reducing the number of inserted addresses from (9) to (10), -note that (9) is square of (10) - also on average; operations from *n(P)/2 +1* difference and intersect between *n(p)/2* sets, reduced to only sorting one set.

IV. Simulation

A. Simulation parameters

For study performance of our work, simulations carried out on Network Simulator 2 (NS-2) simulator [23], version 2.35 installed in Ubuntu 14.04 LTS 32bit. Simulation done during 100 second in a 500 m x 500 m area with 20 mobile wireless node, which position and mobility of each one is random. Two types of traffic used in simulations, Continuous Bit Rate (CBR) and FTP. We considered 6 scenarios for simulation, common parameters between all scenarios presented in Table I and specific parameters of each scenario presented in Table II. In scenario 5 and 6 two nodes randomly selected as a malicious node to launch a blackhole attack.

TABLE I. COMMON SIMULATION PARAMETERS

Parameter	Value
Coverage area	500 x 500 m
Number of nodes	20
Simulation time	100 s
Mobility	Random
Pause time	0.5
Initial Energy (per Node)	100 Joule

TABLE II. SIMULATION PARAMETERS PER SCENARIO

Parameter	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6
Min Speed	1	1	30	30	1	1
Max Speed	30	30	60	60	30	30
Connections	2 Pair	4 Pair	2 Pair	4 Pair	2 Pair	4 Pair
Traffic Type	1 FTP + 1 CBR	2 FTP + 2 CBR	1 FTP + 1 CBR	2 FTP + 2 CBR	1 FTP + 1 CBR	2 FTP + 2 CBR
Number of Malicious Nodes	0	0	0	0	2	2

B. Performance metrics

We use following metrics to compare 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 *di*, and the number of packets received by the destination node is *pktdi*. The average end-to-end delay of the application traffic *n*, which is denoted by *E*, is obtained as

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{di}{pktdi} \quad (11)$$

[1] Function n(X) returns number of X's elements

- **Total Remaining Energy:** This is defined as the sum of all remained energy in every node at a specific time (e.g. End of simulation) or after transmitting specific amount of data, that we calculate it for transferring 200,000 Application Layer packet. The remained energy of node i at the time of measurement (when 200,000 packet transferred in the network) is e_i. The total remained energy of n node, which is denoted by *RE,* is obtained as

$$RE = \sum_{i=1}^{n} e_i \qquad (12)$$

- **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 of the application traffic *n*, which is denoted by *T*, is obtained as

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

C. *Simulation results*

As shown in Fig. 2 and Fig. 3, throughput and End-to-end delay improved in modified CBDS, because we decreased the routing overhead (the size of RREP and CPU load) in modified CBDS so routing done faster. 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 (9) number of inserted addresses in RREP is the square of hop counts, but in modified CBDS, (10) is linear. In modified CBDS, although the source node waits for receiving the response to test packets from n_r (for decrease false-positive rate) and this operation inserts some delay in routing; but this added delay in comparison to removed delay is very low and as shown in Fig. 2 end-to-end delay totally decreased.

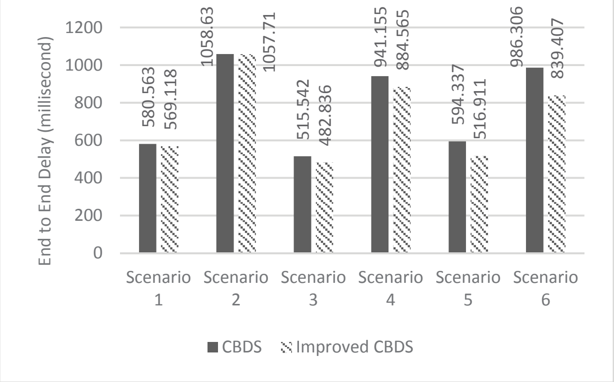

Fig. 2. End to end delay under different scenarios

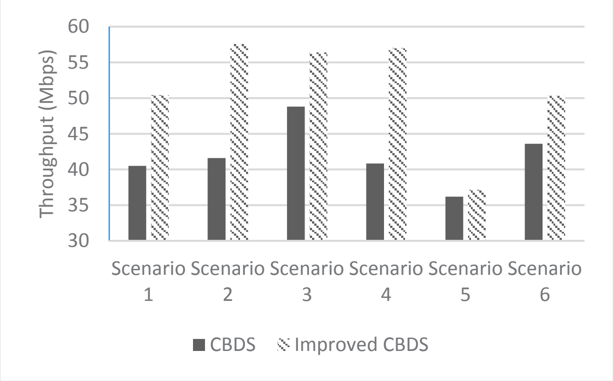

Fig. 3. Throughput under different scenarios

In Fig. 4 can be observed that energy consumption improved in modified CBDS and after sending the specific number of data packets (200,000 packets in our simulation), total left energy in the network is more than CBDS. Also like throughput and end-to-end delay, in long distance improvement on energy consumption is more obvious.

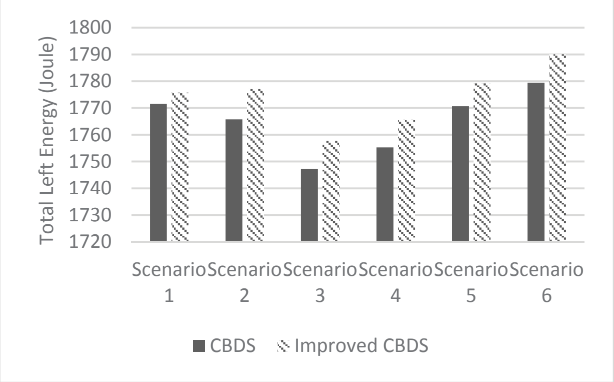

Fig. 4. Total left energy in all nodes under different scenarios

V. 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 one of the available methods called CBDS (a DSR based routing protocol, able to tackle blackhole and grayhole attacks) and propose modified CBDS with decreased false-positive rate and lower routing overhead. Simulation results prove that modified CBDS has better performance in terms of throughput, end-to-end delay and energy consumption.

REFERENCES

[1] Aarti, Dr 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] A. Haghighi, S. Hajiramezan, and K. Mizanian, "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. "Light-weight 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] 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.

[11] Baadache, Abderrahmane, and Ali Belmehdi. "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." arXiv preprint arXiv:1002.1681 (2010).

[12] 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.

[13] 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.

[14] 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. Vol. 27. 2009.

[15] Ramaswamy, Sanjay, et al. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks." international conference on wireless networks. Vol. 2003. 2003.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[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] 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.

[22] 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 VITAE), 2011 2nd International Conference on. IEEE, 2011.

[23] "The Network Simulator - ns-2." [Online]. Available:http://www.isi.edu/nsnam/ns/. [Accessed: 31-Dec-2014].