xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.3083-3089
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.346

Counter and Timer Based Baited Method for Separating Blackhole Attacks in MANET

S G Rameshkumar, Assistant Professor, Department of Electrical Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India, rameshkumarsg17@gmail.com
G Mohan, Professor, Department of Electrical Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India.

ABSTRACT- Mobile Ad Hoc Network (MANET) is extra achievement recognition owing to two main features such as dynamic topography and no necessity of centralized management. However owing to two attributes, MANET is extremely prone to several security attacks. This paper depicts the Counter and Timer Based Baited Method for Separating Black hole Attacks in MANET. In this approach, Baiting message, Non-neighbor Reply as well as counter functions are detected the black hole nodes in MANET. This approach checks the forward and received count. This function also isolates the black hole nodes and separates from the routing table. The simulation results illustrates that diminishes node Delay, increases the network throughput and minimizes the energy utilization in the network.

Keywords: **Mobile Ad Hoc Network, Black hole attack detection, Baiting message, Non-neighbor Reply, and Forward also received count.**

I. INTRODUCTION

MANET is a short-term network which contains single mobile nodes that can transmit with all lacking any assist from communications. Nodes in the MANET can transmit through applying multi-hop communication. If a source node is inside communication range of destination, straight data communication can take place else, in-between nodes have to route the data [1].

In MANET, the nodes can connect also depart quickly; therefore the topography of this network is dynamic. This dynamic topography create network is further susceptible to many types of attacks. This outcomes to create this network very hard in developing route reliability. MANET forever conducting several types of malicious attacks though, we concentrate on black hole attacks [2]. Healthcare organization necessitates nonstop supervising with both occasional updates also emergency information flowing via the network. However, the significant issue detected in these kinds of positions is the attacker nodes happening inducing needless delays also dangerous results. It induces for the happening of traffic congestion also creates network delay.
In a black hole attack, the attacker node acts itself as having a suitable shortest route to attain to the destination node. In this method false route will be produced through the attacker's node also the entire the traffic is redirected to that attacker node [3]. As a result, in neglecting of packets to the determined destination, in the meantime entire packets will be engaged otherwise slipped through the attacker node [4].

Using Timer Based Baited Technique (TBBT) contains both timers as well as baiting method to discovering also separating Black hole nodes in a MANET. This approach improves black-hole revealing ability by Baited message. This approach applies false id baiting method for discovering black-hole nodes in the network. However, this approach increases the network delay and minimizes the Throughput [5]. To solve these problems, Counter and Timer based Baited Method (CTBM) for Separating Black hole Attacks in MANET is introduced. This approach contains three functions namely Baiting message, Non-neighbor Reply as well as counter. These three functions separate the Black hole nodes in the network.

II. RELATED WORKS

Blackhole attack is one of the bellying attacks; also it is known as a full packet drop attack owing to the open intermediate as well as dynamic topology. The facade of black hole nodes happens throughout the route detection stage. Primarily, the sender node does not present any applicable path to the receiver node [6].

Blackhole attacks can be classified into three types of attacks such as single hole attacks, multiple attacks, as well as collaborative attacks. As their identity entail, a single node otherwise moreover node can participate in attacker actions [7].

The nodes in the network can be easily attacked by collaborative attacks such as black hole attack, gray hole attack and jellyfish attacks. These are the most serious attacks which drops the packet without transmitting. Modified Cooperative Bait Detection approach is used for maintaining versus collaborative attacks. It is discerning cancerous nodes in MANETs under interactive black hole also jellyfish assaults [8].

Blackhole attacks can be classified into three types of attacks such as single hole attacks, multiple attacks, as well as collaborative attacks. As their identity entail, a single node otherwise moreover node can participate in attacker actions [9].

The nodes in the network can be easily attacked by collaborative attacks such as black hole attack, gray hole attack and jellyfish attacks. These are the most serious attacks which drops the packet without transmitting. Modified Cooperative Bait Detection approach is used for maintaining versus collaborative attacks. It is discerning cancerous nodes in MANETs under interactive black hole also jellyfish assaults [10]. Anti black hole approach that identifies the Blackhole nodes. Here, evaluates untrusting value through R_{REQ} and R_{REP}. If the node untrusted value is greater than the threshold that node represents the black hole in the network [11]. Modified Extended Data Routing Information is applied to identify as well as reduce co-operative black hole as well as gray hole attacks. This table is applied to notice an attacker node also continue a history of its preceding malevolent exemplifies to contain the gray hole behaviour [12]. Detection and removal of Cooperative Black or Gray hole attack to notice as well as remove the attack on sender and in-between node [13]. In Blackhole and Grayhole attackers intentionally interrupt data communication through transmitting mistaken routing data. Ad-hoc On-demand Distance Vector (AODV) approach that an in-between node discovers the attacker node transmitting fake routing data; routing packets are utilized to exceed routing data, but also to pass information concerning cruel nodes [14].

Behavioural as well as Node functioning of AODV approach to notice gray hole attack. Here, behavioural abnormality recognition for gray hole attack also node observe the abnormality of data rendered through gray hole node also transmit the gray hole node obstruct message to every entered nodes for avoidance of this kind of attack [15].

III. PROPOSED METHOD

In MANET, several approaches have been applied to detect the black hole attacks however, it stay disputing to prevent the data from black hole attacks. Therefore necessitate introducing method to resolve the security trouble. In this approach, Counter and Timer Based Baited method for Separating Blackhole Attacks in MANET. This approach contains three parts namely Baiting message, Non-neighbor Reply as well as counter.

Bait Message Part

In this part, every node has a bait-timer, the rate of the timer is preset arbitrarily to B sec, and also every time the timer attains B it makes as well as disseminates a bait request (B_{REQ}) with an arbitrarily yielded false id. Calculating the behavior of a black-hole while it attains any route request it answer with a Reply taking which it has the better route yet if it does not be present. While the black-hole attains the B_{REQ} it transmits a reply to the source taking which it has a route; as the source attains the Bait Reply (B_{REP}) it instantly conceives the node that answered as a black-hole as well as upends it to the black-hole record since it maintain to have a route to a false node. In the B_{REQ}, the rate of Time to Live (TTL) is preset to one so as to evade congesting with false requests.

Non-neighbor Reply

In this part, every node recognizes its neigh boring nodes since of the hello message communications procedure. Whenever the source obtains a reply it verifies the id of the Node through the Shortest route if it is in the black-hole record; next it rejects the reply; or else it verifies if the id present in the neighbor

table through equating the ID with ones in the neighbor table; if it is not a neighbor node next the source rejects that reply to evade all transmission with unidentified nodes.

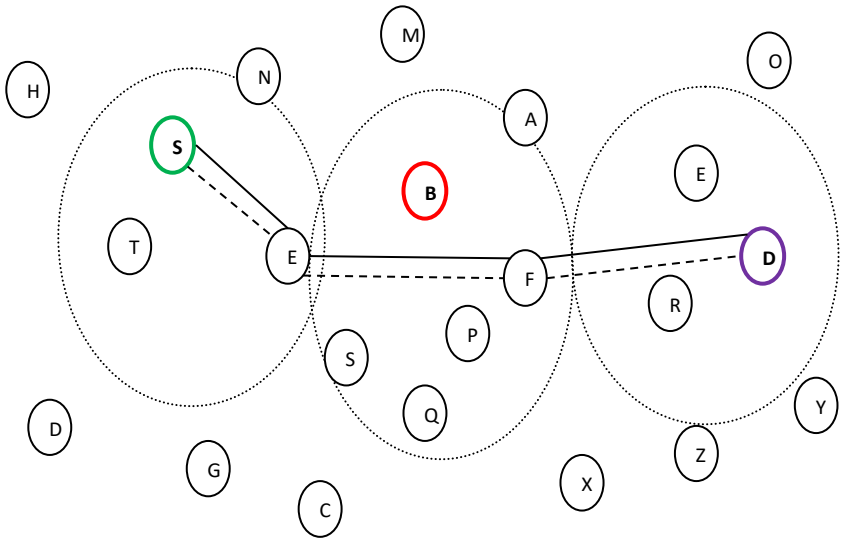

Figure 1. Illustration of proposed scheme

As shown in Figure 1, every node disseminates hello message to recognize its neigh boring nodes. In baiting message part every node makes a B_{REQ} with an arbitrary false id as well as a TTL identical to 1 also next disseminates the B_{REQ} to the entire its neigh boring nodes; both black-hole nodes B1 will reply message to the B_{REQ}. Nodes E, F, as well as L will append node B to their black-hole record since node B answered for every bait got from E, F, as well as L established on the usual behavior of the black hole node which it reacts to every request even if it does not have an present route for the required node. Every node rearrange bait-timer with an arbitrarily B sec, whenever Source S desires to transmit with destination D it disseminates Route Request. Node E transmits Route Reply taking which it has the better route; node S verifies if node E presents in its neighbor record or not; because node E in node S transmission range next node E is in the neighbor record as well as node S initiates to communicate the data via E to D.

Counter Verification

In this part, neighbor node keeps two counters $forward_{count}$ as well as $received_{count}$ utilized for considering amount of forwarded packets as well as amount of received packets correspondingly. $Forward_{count}$ is added through Neighbor node while it communicates a packet to in-between node. If in-between node transmits the packet, it will be listen through Neighbor node also it increases $received_{count}$. At last, Neighbor node will transmit packets to in-between node till $forward_{count}$ attains a threshold; after that if $received_{count}$ is 0, source node recognized as black hole node. Since, actually Blackhole node do not transmit any packets however basically losses them hence, Neighbor node will have $forward_{count}$ larger than threshold as well as $received_{count}$ as 0. This threshold value is computed along with the network. Threshold rate calculates entirely on how many packets can exhaust for testing black hole node.

Performance Analysis

In this approach, the performance analysis is carried out using the network simulator (ns2.35). Here, we randomly positioned 50 mobile nodes within an area of 800m×800m. The arbitrary way-point movement model is utilized for node motion process. Constant Bit Rate is used for handling the traffic model. User Datagram Protocol is used for communication between the nodes. The propagation model two ray ground is used for propagating the radio waves. The Omni-directional antenna is utilized for receiving the signals from all directions. The performance of CTBM is analyzed by using parameters like packet obtained rate, packet drop rate, Average Delay (AD), outstanding energy as well as throughput.

Packet Obtained Rate (POR)

POR is denoting as the number of packets received at receiver per particular time. POR is assessed by Equation 1.

$$POR = \frac{\sum_{0}^{n} \text{Packets Obtained}}{\text{Time}} \quad (1)$$

Where,
n = Node count
The POR of TBBT as well as CTBM is diagrammed in Figure 2. It illustrates that the proposed scheme CTBM has 28.09% better POR when compared to the existing TBBT mechanism.

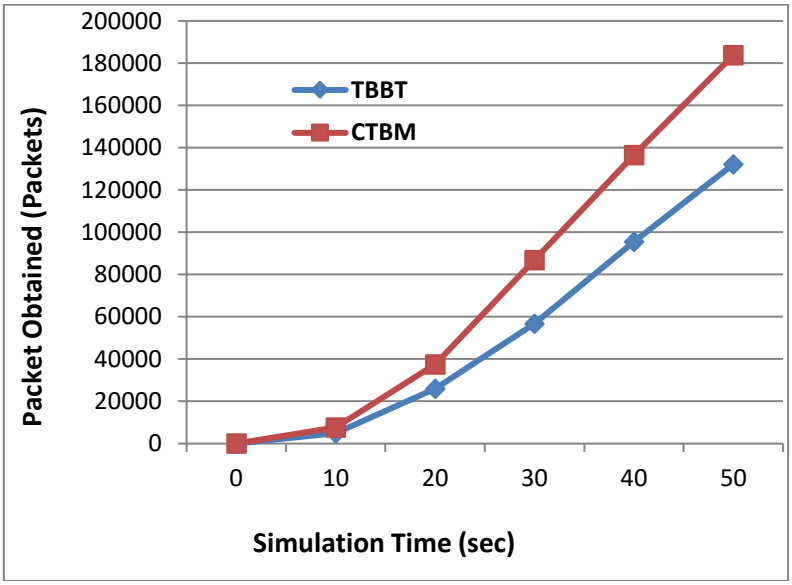

Figure 2. POR of TBBT as well as CTBM

Packet Drop Rate (PDR)

PDR is denoted as the distinction among the transmitted packets and obtained packets in the communication MANET per particular time. PDR is measured by Equation 2.

$$PDR = \frac{\sum_{0}^{n} \text{Sent Packets - Received Packets}}{\text{Time}} \quad (2)$$

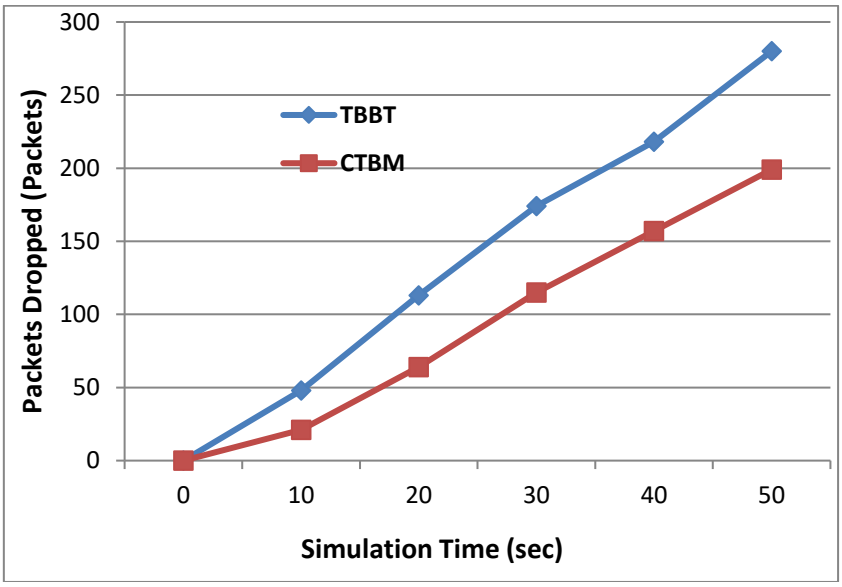

Figure 3. Packet drop rate of TBBT as well as CTBM

Figure 3 shows the PLR values obtained from the simulation analysis of TBBT as well as CTBM. It indicates that PLR of TBBT is higher by 28.92% when compared with CTBM.

Outstanding Energy (OE)

Amount of energy outstanding in a node at the present occurrence of period is called as RE. A determine of outstanding energy commits at which energy is enthusiastic by the MANET functions.

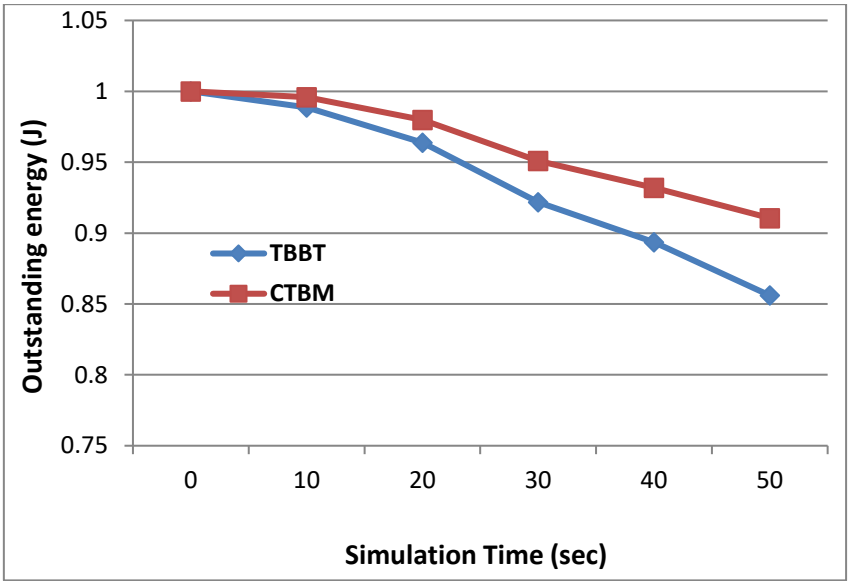

Figure 4. Residual energy of TBBT as well as CTBM

Figure 4 indicates RE of the MANET is enhanced for proposed scheme CTBM when compared with TBBT. Around 0.054 joule of energy is saved per node by using the CTBM protocol for routing.

Average Delay (AD)

The AD is represented as the time period difference among data sent and packets obtained. It is measured by Equation 3. Figure 5 shows the AD analysis of CTBM as well as TBBT mechanisms. It reveals CTBM has 29.27% lower delay for a node when compared to the TBBT mechanism.

$$\text{Average Delay} = \frac{\sum_{0}^{n} (\text{Packet Received Time} - \text{Packet Sent Time})}{n} \quad (3)$$

Where
n = number of nodes

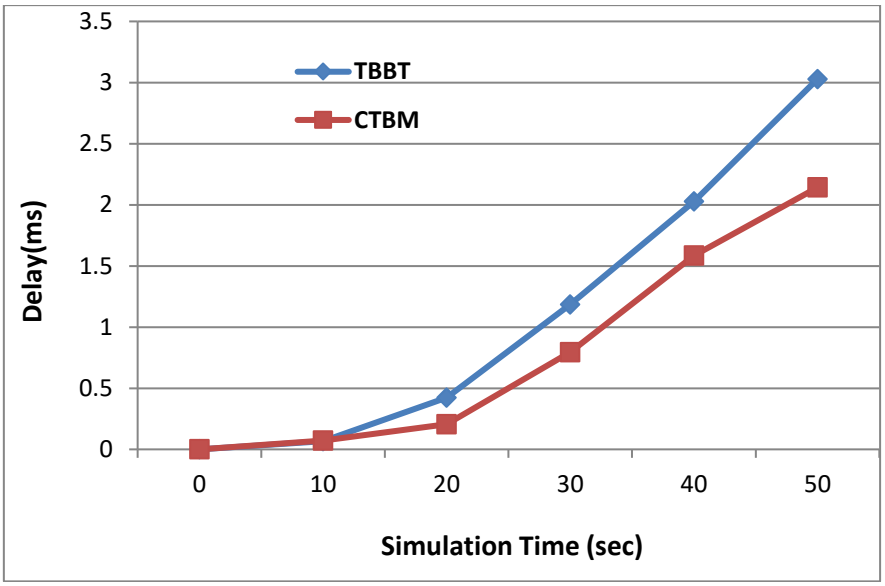

Figure 5. AD of TBBT as well as CTBM

Throughput

Throughput denotes to an entire number of packets successfully delivered across network per unit time. Throughput is obtained using Equation 4.

$$\text{Throughput} = \frac{\sum_{0}^{n} \text{Packets Received}(n) * \text{Packet size}}{\text{Time}} \quad (4)$$

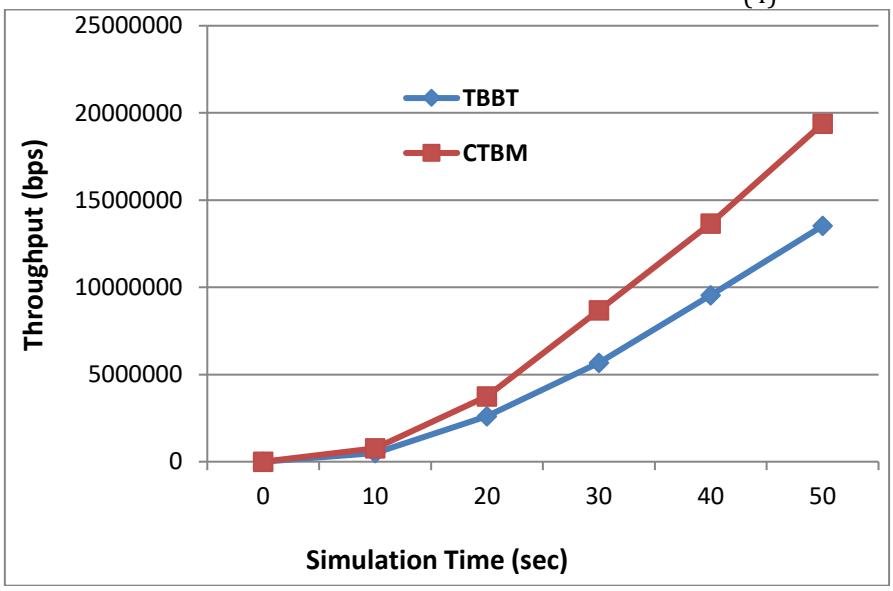

Figure 6: Throughput of TBBT as well as CTBM

Figure 6 indicates the throughput analysis for TBBT as well as CTBM mechanisms. It can be observed from Figure 6 number of packets received successfully for every 1000 packets for CTBM is greater than 30.25% compared to that of the CTBM mechanism.

IV. CONCLUSION

MANET security is the today's major dispute. We mainly concentrate on detecting black hole attack and introduced a possible solution for discovering also removing them. In this strategy we proposed Counter and Timer Based Baited Method for Separating Black hole Attacks in MANET. In this

approach, Baiting message, Non-neighbor Reply as well as counter functions are detected the black hole nodes in MANET. In addition, this approach isolates the blackhole nodes and removes from the routing table. The simulation results illustrates that diminishes node Delay, increases the network throughput and minimizes the energy utilization in the network.

REFERENCES

[1] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*(2011), 32-37.

[2] Gerhards-Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007, October). Detecting black hole attacks in tactical MANETs using topology graphs. In *32nd IEEE Conference on Local Computer Networks (LCN 2007)* (pp. 1043-1052). IEEE.

[3] Puttini, R., Percher, J. M., Mé, L., & de Sousa, R. (2004, June). A fully distributed IDS for MANET. In *Proceedings. ISCC 2004. Ninth International Symposium on Computers And Communications (IEEE Cat. No. 04TH8769)* (Vol. 1, pp. 331-338). IEEE.

[4] Santhakumar, R. (2017). Resource allocation in wireless networks by channel estimation and relay assignment using data-aided techniques. *Int. Journal of MC Square Scientific Research*, *9*, 40-47.

[5] Yasin, A., & Abu Zant, M. (2018). Detecting and isolating black-hole attacks in MANET using timer based baited technique. *Wireless Communications and Mobile Computing*, *2018*.

[6] Sarma, K. J., Sharma, R., & Das, R. (2014, February). A survey of black hole attack detection in manet. In *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)* (pp. 202-205). IEEE.

[7] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security*, *5*(3), 338-346.

[8] Bala, A., Bansal, M., & Singh, J. (2009, December). Performance analysis of MANET under blackhole attack. In *2009 First International Conference on Networks & Communications* (pp. 141-145). IEEE.

[9] Woungang, I., Dhurandher, S. K., Peddi, R. D., & Obaidat, M. S. (2012, May). Detecting blackhole attacks on DSR-based mobile ad hoc networks. In *2012 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1-5). IEEE.

[10] Sherif, A., Elsabrouty, M., & Shoukry, A. (2013, December). A novel taxonomy of black-hole attack detection techniques in mobile Ad-hoc network (MANET). In *2013 IEEE 16th International Conference on Computational Science and Engineering* (pp. 346-352). IEEE.

[11] Hiremani, V. A., & Jadhao, M. M. (2013, December). Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. In *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)* (pp. 944-948). IEEE.

[12] Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K. H., Pathan, M. S., Hussain, M. I., & Memon, M. Q. (2019). A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. *Future Internet*, *11*(3), 61.

[13] Kshirsagar, D., & Patil, A. (2013, July). Blackhole attack detection and prevention by real time monitoring. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

[14] Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science*, *48*, 472-479.

[15] Singh, H. P., Singh, V. P., & Singh, R. (2013). Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review. *International Journal of Computer Applications*, *64*(3).