Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.562 – 569

RESEARCH ARTICLE

Secure Method for AODV Routing By Detection and Prevention of Collaborative Blackhole Attack in MANET

Priya Jeejo Payyappilly[1], Pinaki A. Ghosh[2]

[1]Atmiya Institute of Technology and Science, Rajkot, Gujarat, India

[2]Atmiya Institute of Technology and Science, Rajkot, Gujarat, India

[1] anniejollyjeejo1@gmail.com, [2] paghosh@aits.edu.in

Abstract— Mobile Ad Hoc networks (MANETS) are self configuring, decentralized networks in which the nodes communicate without the need of infrastructure. The nodes work in an environment in which mutual trust between the nodes form an important part of the communication. This property of the network is exploited to launch a blackhole attack. Blackhole attack is a network layer denial of service attack in which an adversary node attracts the data traffic towards itself by advertising a short route to the destination and instead of forwarding, it simply drops the packets. When multiple malicious nodes launch a simultaneous attack, it degrades the performance of the network considerably. This research aims at purging the network of collaborative blackhole nodes by use of trust values to distinguish malicious node from a genuine node. Simulation results show a better performance of the network under the collaborative blackhole attack.

Keywords— MANETs, Blackhole attack, Collaborative blackhole attack, selfish node, trust value, denial of service, AODV.

I. INTRODUCTION

The rapid proliferation of wireless networks and devices has brought us to a new age of information storage, sharing and retrieval. Easy availability of wireless devices renders a promising environment of flawless communication without the need of wires in the near future. One such development in the field is the Ad Hoc Network. It is a budding field of research and deployment which focuses on minimizing the use of base stations [2] or access points used in conventional wireless networks for communication. 'Ad Hoc' is a Latin word meaning 'for a specific purpose'. Ad hoc networks are formed by autonomous systems communicating to each other mostly through wireless links. Each device in the network is known as a node. The nodes are peers; having similar privileges and functioning as a client and server interchangeably during the course of communication period. The concept of Ad Hoc Networks has been further extended to incorporate the nodes when they are moving. This concept is known as Mobile Ad Hoc Network [1] [2] also known by the acronym MANET. MANETs do not rely on any base stations or access points for its functioning. Nodes co-operate to forward data to each other in the network [1] [2] assuming the nodes to be trustworthy. This property of MANETs is abused by adversaries to launch blackhole attack [3] [4]. It is a network layer denial of service attack which attracts traffic from the network towards itself and drops the data packets. This deteriorates the

performance of the network to a great extent. Further harm is done when a number of nodes carry out this attack simultaneously. This is known as collaborative blackhole attack [4]. The purview of this research is to study the harmful effects of collaborative blackhole attack on MANET performance using the AODV protocol and propose a solution to mitigate this attack.

The rest of this paper is organized as follow: Section II explains the protocols used for MANETs emphasizing on the AODV protocol. Then attacks on MANETs are explained highlighting blackhole and collaborative blackhole attacks. Section III explains the literature survey carried out for mitigation of blackhole and collaborative blackhole attacks. Section IV explains the proposed approach and its followed by conclusion and references.

II. Routing Protocols and Security Vulnerabilities of MANETs

A. *Protocols in MANETs:*

Routing Protocols help in assigning an optimal and efficient path for the data packet to reach from the sender to the receiver. They help in discovery of route from sender to receiver, forwarding data from sender to receiver and maintenance of the found route. Routing protocols in MANETs are categorized as proactive, reactive and hybrid routing protocols. Proactive Routing protocols are also known as table driven routing protocols [6] [2]. That is because, the method is to periodically store the data about the neighbouring nodes in their respective routing tables and then propagate this information to other nodes in the network. The main constraint of this method is that limited bandwidth is wasted during this propagation phase. The protocols using this approach include Destination Sequenced Distance Vector (DSDV) protocol and Wireless Routing Protocol (WRP). Reactive protocols are also known as On-Demand routing protocols. These protocols discover routes by sending control messages to neighbouring nodes requesting route information and the nodes which have the information about the route reply by generating control messages. This approach is better than proactive approach as it saves overhead upto some extent. Protocols using this method are Dynamic Source Routing (DSR) protocol, Signal Stability-based Adaptive routing (SSA), Ad hoc On demand Distance Vector Routing (AODV) protocol and Temporally Ordered Routing Algorithm (TORA). To combine the advantages of proactive and reactive approaches, a hybrid approach is proposed [4]. This mechanism is useful for larger networks and frequent topology changes. It functions by dividing the network into zones. Routing inside the zone is done by proactive approach and outside the zone is done by reactive approach [4]. The hybrid routing protocol is the Zone Routing Protocol (ZRP).

B. *Ad hoc On demand Distance Vector (AODV) Routing Protocol:*

Any reactive protocol does three functions in the network viz. a) Route Discovery, b) Data Forwarding and c) Route Maintenance. AODV performs these functions by using three control packets i.e. Route_Request (RREQ) packet, Route_Reply (RREP) packet and Route_Error (RERR) packet [1] [2] [3]. A node disseminates route requests (RREQ) [2] when it is determined that it needs a route to the destination but doesn't have one available or the previous route to a destination is marked invalid o it no longer exists. When any intermediate node receives the RREQ it checks whether the RREQ has been repeated, if yes then the RREQ is discarded, otherwise, it is processed and rebroadcasted. A route generates an RREP if it itself is a destination node or it has a route existing towards the destination node. When the RREP is generated, the node copies the Destination IP address and the originating sequence number from the RREQ message into the corresponding field of the RREP message. For maintaining the network information, a hello packet is periodically forwarded to the nodes in the network. Each node sends this hello packet to its one hop neighbours. The neighbours in turn reply to this hello message. If a particular node doesn't receive the hello message in a

specified amount of time, it broadcasts the RERR packet to the nodes in its precursor list. The RERR packet is sent when the link break causes one or more of the destinations to become unreachable from some of the node's neighbours. Thus the network information is maintained in this way by AODV protocol.

C. *Security Vulnerabilities of MANET:*

The environment of mutual trust between the nodes gives rise to many security vulnerabilities. An attack can be described as a breach of security mechanism in order to fulfill some malevolent purposes. The nodes so not foresee the latent presence of an attacker and therefore any node; either from among the nodes of the network or a node joining the network remotely can launch attacks on the network. The nodes which launch any attack are termed as selfish or misbehaving node. This corrupts the performance of the network. The messages cannot be relayed and sensitive information can be modified or lost. Many attacks affect the networks [3]. These attacks can be categorized on the basis of the layers of the OSI model which they attack as: Physical Layer attacks: Jamming, Interception, Eavesdropping, Active interference, Data Link Layer attacks: Monitoring, Traffic Analysis, Disruption of MAC, Network Layer Attack: Black hole Attack, Grayhole Attack, Wormhole Attack, Flooding, Transport Layer Attack: Session Hijacking, SYN Flooding, Application Layer Attack: Repudiation, Data Corruption, Malicious code.

D. *Blackhole Attack :*

A blackhole [5] node in the network attracts all the data packets towards itself by advertising a fresh enough route to the destination to the other nodes in the network. This attack can be launched by the fabrication of the control messages i.e. RREP or RREQ. RREQ falsification is the process in which the RREQ is modified where the malicious node increases the destination sequence number of the RREQ received from the source but doesn't increment the hop count. When the destination or the intermediate node receives the RREQ with smaller hop count but higher sequence number, it chooses the route via the malicious node and then, the malicious node launches the blackhole attack. The blackhole attack by RREP falsification is much simpler. The malicious node replies to the RREQ message immediately when it receives the RREQ. The source node thinks it as the fresh enough route and replies to it immediately and disregards the legitimate RREP received from the genuine node.

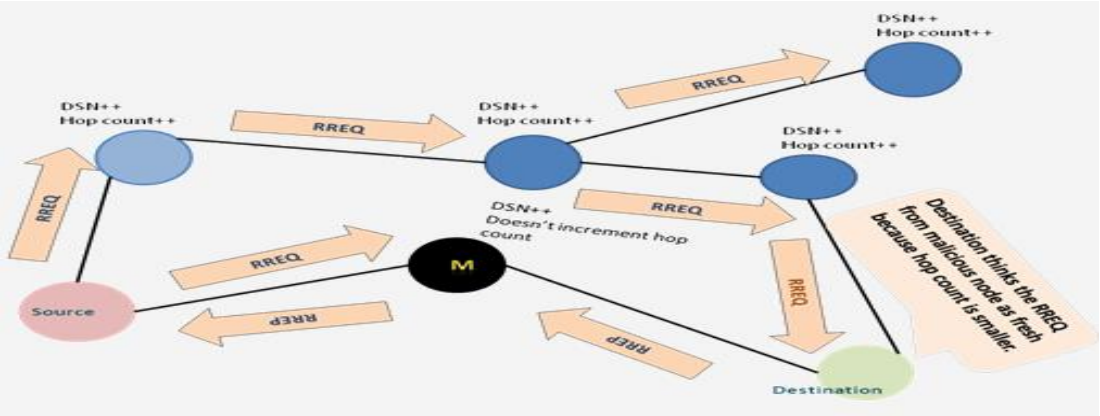

Figure 1. Blackhole Attack by RREQ fabrication

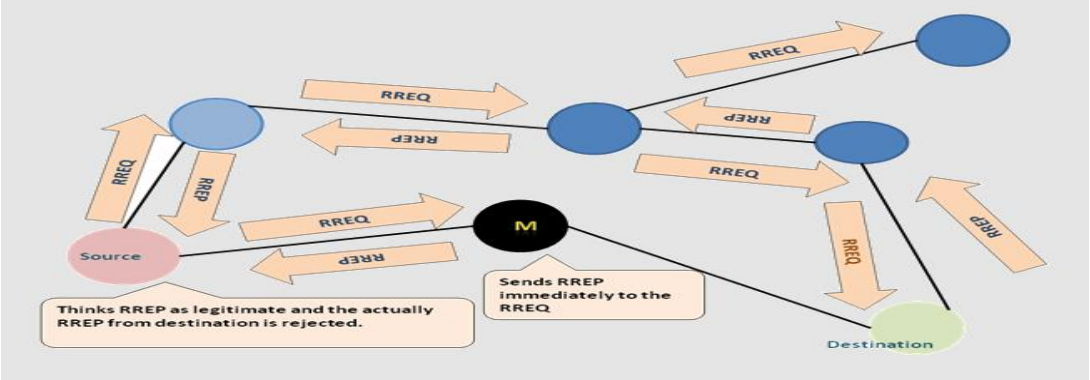

Figure 2. Blackhole Attack by RREP fabrication

E. *Collaborative Blackhole Attack:*

Collaborative blackhole attack [5] is the phenomena in which a number of nodes launch a blackhole attack together. The timing of the launch of attack may vary, if the nodes launch attack at the same time, the performance of the network is reduced to nothing.

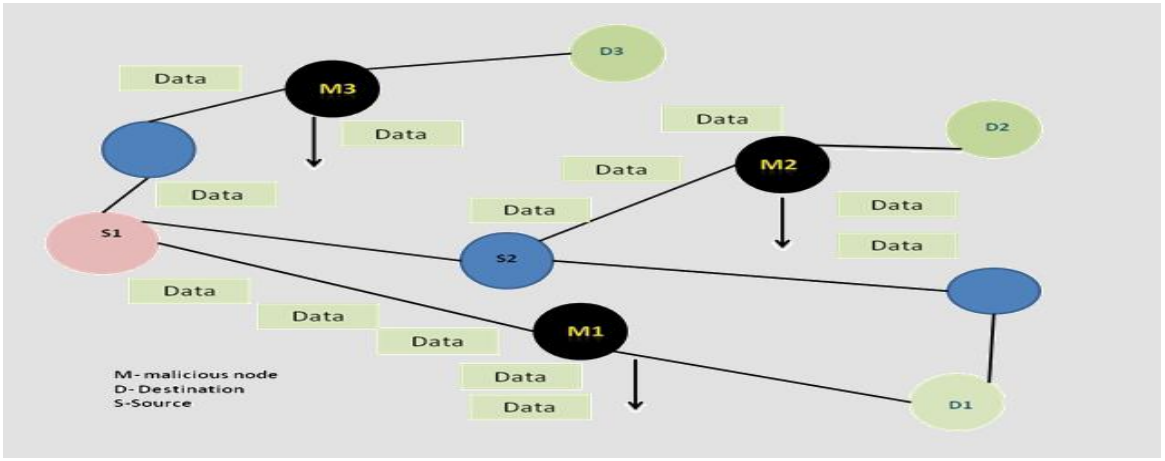

Figure 3. Collaborative Blackhole Attack

III. Literature Survey

This section explains the existing works done to mitigate the blackhole and collaborative blackhole attack.

Jin-Ming Chang et al. [8] proposed a bait detection approach in DSR based MANETs. In this approach, a node is first initialized as bait for the blackhole node by mutual co-operation among nodes. The selection of node is done stochastically. The node will send a false RREQ named as 'Bait RREQ'. The 'Bait RREQ' is sent to the nodes in the networks and after analysis and reverse tracing, the blackhole node is discovered. The protocol used is DSR.

Tarun et al. [9] proposed the implementation of watchdog mechanism in AODV by enhancing the protocol as W-AODV to detect malicious nodes. This mechanism functions by using special nodes called watchdogs which promiscuously hear the other nodes in the network to ensure that the nodes forward the packets to the next node. If these watchdog nodes find out that those nodes have not forwarded the packets yet, they entitle the node as malicious and forward this information to other nodes in the network. The other nodes also blacklist these nodes. These watchdog nodes provide an alternate route to the other nodes if a malicious node is detected. The authors have listed the advantage that a watchdog is node reliant only on the information of the local node therefore it is difficult to be badly influenced by another node in the network . But it has the drawback of adding an additional

header and consumption of energy. Also, they have listed in their conclusion that the watchdog method is challenging to deploy in an environment where collaborative black hole attack is launched because it can only monitor its neighbour node.

S.Sankara et al. [10] proposed a mechanism known as Secure AODV in which AODV protocol is enhanced by using a secure routing mechanism. The destination is identified by the use of a unique identification termed as MRREP the MRREP is a hashed identification number to enhance the security. When the destination node receives the RREQ, it responds by generating MRREP and sends it through different nodes. Now the malevolent node doesn't know about the MRREP. It sends an RREP with highest sequence number. Now, the sender gets RREP through different nodes and stores it in a Reply Collect Table (RCT) [10] and matches the Unique Identification Number by comparing with the other entries in the table. The blackhole node is the one which doesn't contain unique identification number. The source discards such nodes and arranges the value of other nodes in descending order.

IV. Proposed Approach

A. Explanation of proposed approach:

The basis of the proposed approach is formed by the fact that the attacker node may either change hop count of RREQ or reply first to an RREP. The proposed approach performs two functions namely: 1) Detection of collaborative blackhole attack and prevention of collaborative blackhole attack. A value called trust value is computed for each node. Initially, each node is treated equally and trusted completely. The node in due course increases or decreases the trust of the neighbour. Trust is based on RREQ and RREP sent and received as well as the data packets received. Trust is increased when RREQ is sent, data packets received and decreased when RREP is received before a predefined time. Trust value is like a counter which is increased and decreased. Here, DSN (DESTINATION SEQUENCE NUMBER) is used for identification of blackhole nodes. Intermediate nodes verify whether sent RREQ- DSN >>> received RREP-DSN then node is identified as blackhole. This is the detection part. This process of verification is done when trust value becomes 0 because comparing DSN every time consumes power. For the prevention part, each node just removes the node from its routing table. The schematic representation of the proposed work is shown below:

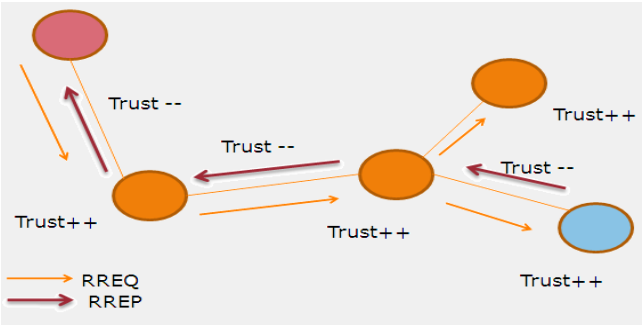

Figure 4. Proposed approach phase one

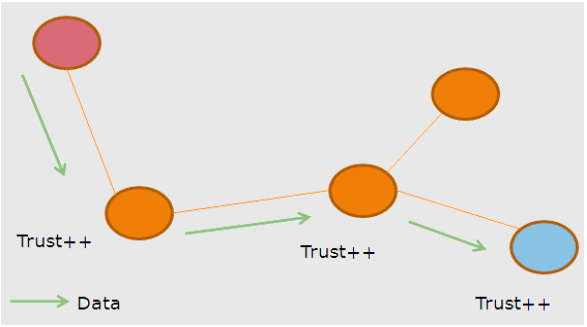

Figure 5. Proposed approach phase 2

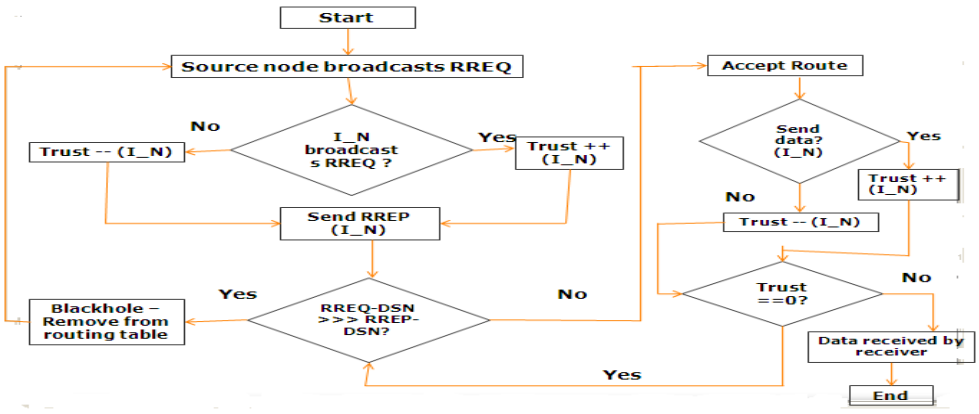

Figure 6. Proposed approach flowchart

B. Simulation Results:

Simulation results show better performance in terms of packet delivery ratio and throughput by the proposed approach. The simulation was done in ns-2 discrete event simulator. The details and results are given below:

- **Performance metrics:**
  - Throughput: The difference between the sent and received packets in a given unit of time is called throughput. Here the throughput is measured in kilobits per second (kbps).
  - Packet delivery ratio or packet delivery fraction (pdr / pdf): The number of data packets delivered to the destination.
  - End to end delay: Average time taken by data packet to arrive to the destination.

Parameters	Values
Terrain Area	500 X 500
Protocol	AODV
Traffic	cbr (UDP)
Antenna	Omni directional
Packet size	512 bytes
Performance Parameters	Throughput, packet delivery ratio and end to end delay
No. of nodes	50, 100, 150, 250, 350,450, 500
Simulation time	100 sec
No. of malicious nodes	0, 3,4, 5,10, 15

Table 1. Implementation Details

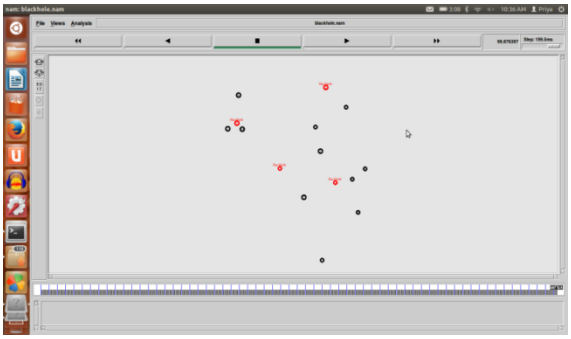

Figure 7. Simulation

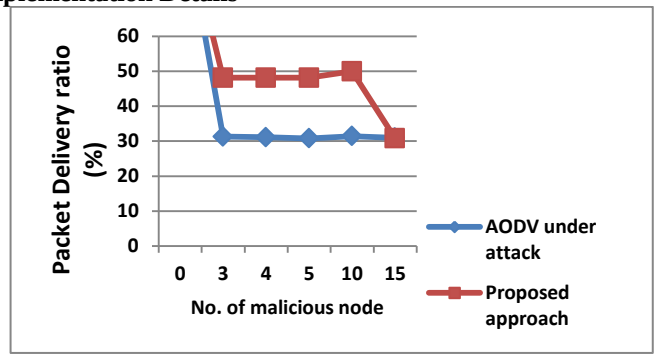

Figure 8. a. Packet Delivery Ratio (%)

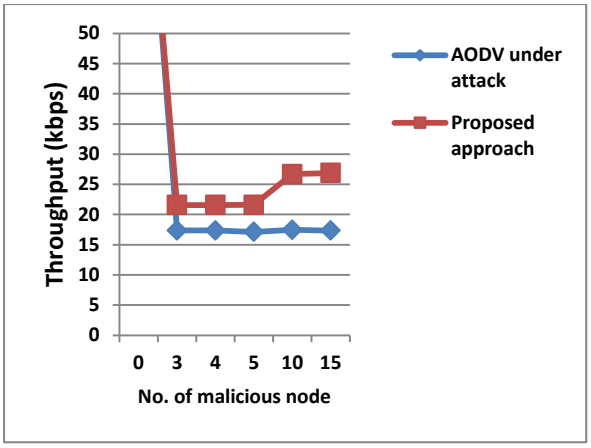

Figure 8. b. Throughput (kbps)

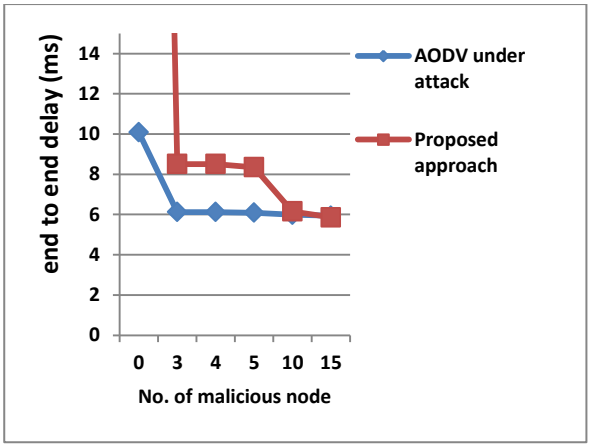

Figure 8. c. End to end delay (ms)

Figure 8.Results of the simulation

V. Conclusion

Mobile Ad hoc networks are formed by moving independent nodes communicating with each other with the help of wireless links. The nodes communicate by mutual co-operation among themselves assuming a trustworthy environment. This feature is exploited to launch blackhole and collaborative blackhole attacks in MANETs. The purpose of this attack is to capture data packets by advertising itself to have the shortest route to the destination and then drop the packets. This affects the performance of the network considerably. A method is proposed to mitigate this attack by use of trust values and comparison of sent RREQ-DSN and received RREP-DSN numbers. The blackhole attack with multiple malicious nodes has been deployed and the simulation results show the improvement in throughput, end to end delay and packet delivery ratio through this approach. The simulation results show the effective prevention of the attacks. The future course of study in this direction can be to further increase its working by taking into account the removal of blackhole nodes from the network dynamically.

References

1. Ivan Stojmenovic, Handbook of Wireless Networks and Mobile Computing; 5th Edition; Wiley India Edition, New Delhi, 2001, pp 536.
2. Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks and Applications", International Journal of Computational Engineering and Management, vol. 11, January 2011, pp. 32-37.
3. Hoang Lan Nguyen and Uyen Tang Nguyen, "Study of different types of attacks on Multicast Mobile Ad Hoc Networks", Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, IEEE, 2006.
4. Praveen Joshi, "Security Issues in routing protocols in MANET at network layer", Procedia Computer Science , vol 3, 2011, pp. 954-960.

5. Fan-Hsun Tseng, Li-Der Chou and Han- Cheih Chao, "A Survey of Blackhole Attacks in Wireless Mobile Ad Hoc Networks ", Human- centric Computing and Information Sciences, a Springer Open Journal, 2011, pp. 1-16.
6. Dr. S.S. Dhenakaran, A. Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013, pp. 251-259.
7. Mandala, S.; Abdullah, A.H.; Ismail, A.S.; Haron, H.; Ngadi, M.A.; Coulibaly, Y., "A review of blackhole attack in mobile adhoc network," Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2013, vol., no., pp.339-344.
8. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chen-Feng Lai, "Defending Against Collaborative Blackhole Attacks by Malicious Nodes in MANETs: A Co-operative Bait Detection Approach" IEEE systems journal, 2014, pp 1-11.
9. Tarun Varshney, Tushar Sharmaa, Pankaj Sharma,"Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network", 2014 Fourth International Conference on Communication Systems and Network Technologies, pp 217-221.
10. S. Sankara Narayanan and Dr. S. Radhakrishnan, "Secure AODV to Combat Black Hole Attack in MANET", 2013 International Conference on Recent Trends in Information Technology. IEEE 2013.

