Available online at www.worldscientificnews.com

World Scientific News

WSN 49(2) (2016) 78-89 EISSN 2392-2192

Detection of wormhole attack using cooperative bait detection scheme

M. Newlin Rajkumar[a], M. U. Shiny[b], R. Amsa Rani[c]

Department of Computer Science & Engineering, Anna University Regional Centre, Tamil Nadu, India

[a-c]E-mail address: newlin_rajkumar@yahoo.co.in , shinysusma05@gmail.com , rk.amsa@gmail.com

ABSTRACT

Mobile Ad-Hoc Network is an wireless systems it supports mobile communication in a network. MANETs are affected by several security attacks but it affects the features that are like open medium, dynamical changes in topology, lack of central monitoring and management and it not obtain the clear defence mechanism to MANETs. To prevent or detect malicious nodes launching collaborative wormhole attacks is a challenge. The existing system designs a dynamic source routing (DSR)-based routing mechanism, but it is also referred to as the cooperative bait detection scheme (CBDS) to detect the wormhole attacks effectively. Here we describes the various wormhole attacks and prevention methods for wormhole attack.

***Keywords*:** Index Terms-Cooperative Bait Detection Scheme (CBDS); Dynamic Source Routing (DSR); Mobile Adhoc Network (MANET); Wormhole attacks

1. INTRODUCTION

MANET –Mobile Ad-Hoc Network is a centralized infrastructure. Nodes not works at a host but it act as a router. However receiving data nodes need cooperation with forward packets, and hence forming a wireless local area network. It is mainly used in application such as medical assistance, disaster relief services, and military network in battlefields. MANET is random topology because the routers move randomly free in the network. MANET is more vulnerable than wired network.

A adaptable ad hoc arrangement (MANET) is an basement beneath arrangement of adaptable devices. In MANET adaptable accessories acquaint on arrangement aisle for acquisition letters from one arrangement to another. In MANET all accessories are acceptable to move in any direction, and accordingly change its links to added accessories frequently. Every accessory should forward cartage altered to its own use, and wish to be a router. The capital claiming in architecture a MANET is the every accessory to always advance the abstracts bare to appropriately avenue traffic.

These MANETs may accomplish by themselves or could as well be affiliated to the beyond Internet. MANETs are an anatomy of Wireless ad hoc arrangement that about includes a routable networking ambiance on top of a Link Band ad hoc network. Lots of assay has been activated in comparing MANET protocols appliance absolutely altered parameters. These are focused on accretion achievement of MANET networks to absorb activity with ability and acquisition added efficient. In ad hoc networks, nodes aren't accustomed with the cartography of their networks. Instead, they charge to acquisition it: a cast new bulge announces its attendance listens for announcements advertisement by its neighbours. Every bulge learns apropos altered abutting nodes and about to ability them, and accomplishes an advertisement that it can as well ability them. In MANETs, the nodes are adaptable and array operated. As the nodes accept bound array assets and multi hop routes are acclimated over a alteration arrangement ambiance due to bulge mobility, it requires activity able acquisition protocols to absolute the ability consumption, prolong the array activity and to advance the robustness of the system. Node misbehaviour is such a class of aegis blackmail for Adaptable Ad hoc Networks (MANETs). In general, misbehaviour can be conducted at every band in MANETs, such as awful calamity of the Request-To-Send (RTS) frames in the MAC layer, dropping, modification, and misroute to the packets in the arrangement layer, and advised advancement of affected observations apropos the behaviours of added nodes in the appliance layer.

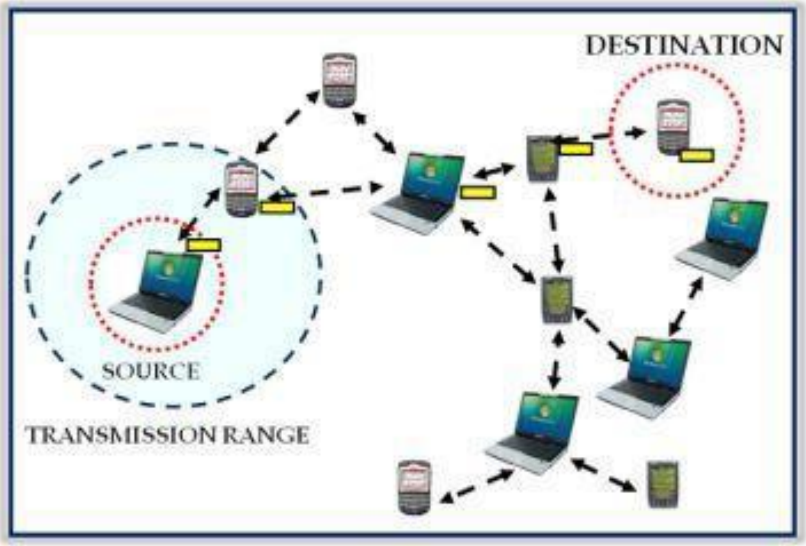

Figure 1. Shows how data is send from transmitter to receiver.

Some of the vulnerabilities are as follows:-

- Lack of centralized management
- Resource availability
- Scalability
- Cooperativeness
- Dynamic configuration
- Limited Power Supply

2. ROUTING AND VARIOUS PROTOCOL SUPPORTS FOR ROUTER ROUTING

Routing is select path from source node to destination node. The source node sends the packet to the destination node which used the router. The router collects the path during source sends the packet to destination. It having various protocols supports for router.

Proactive protocol

In proactive protocol need to constantly detect or monitor the neighbour node.in this protocol existence of malicious nodes, the directly detection is constantly created and resource used for detection is constantly wasted.

Advantage:

- It ensures preventing and avoiding an attack in its initial stage.

Reactive protocol

Reactive or Trigger protocol only when the destination node detects a significant drop in the packet delivery ratio.it is sustenance for the ad hoc distance vector routing algorithm. Reactive protocol builds up routes only when required by source node. Some examples of reactive protocol is Ad-hoc On Demand Routing, Dynamic Source Routing, Location Aided Routing.

Advantage:

- It requires minor routing information

Hybrid protocol

Hybrid protocol is a hierarchical protocol based on position in the global system. It also used in the distance vector for router. The router connects the possible link to the corresponding packets. In this protocol is a more accurate to find the best path from source to destination path in network and routers also report and update the any changes in network topology.

3. CLASSIFIED INTO TWO MAIN CATEGORIES OF ATTACKS:

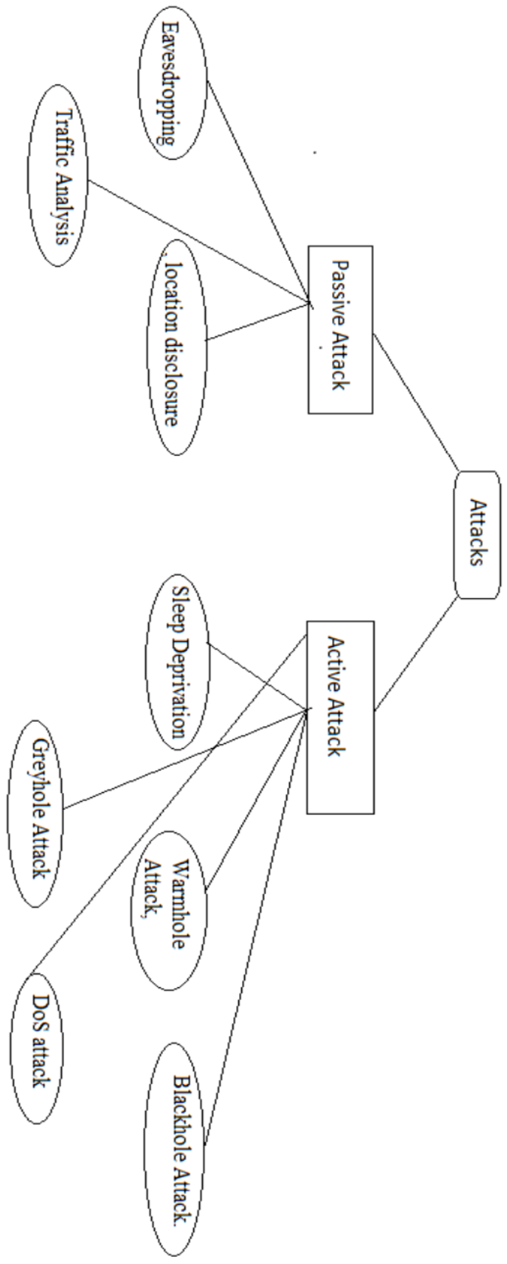

Fig. 2. Classification of Attacks in MANET

Passive attacks

A acquiescent advance is a arrangement advance in which a arrangement is monitored and sometimes it scanned for accessible ports and susceptibilities. The purpose is only to gain information about the target and no data is changed on the target. Passive attacks include active investigation and passive investigation. It can be include eavesdropping attack, Traffic analysis.

Eavesdropping attack

It is serious security threat to a wireless sensor network since the eavesdropping attack is a prerequisite for other attack. It is unauthorized real-time interception of a private communication, such a phone call, instant message, video conference or fax transmission It is known as disclosure attacks, are passive attacks by external or internal nodes. The attacker can analyse broadcast messages to reveal some useful information about the network.

Traffic Analysis:

Traffic analysis is that the method of intercepting and examining messages so as to deduce data from patterns in communication. It is dead attainable to interact in protocols, or obtain to impress communication between nodes. Traffic analysis in unintended networks might reveal the existence and placement of nodes, the communications configuration, the roles contend by nodes, the present sources and destination of communications.

ACTIVE ATTACKS

This attacks as a result of unauthorised state changes within the network like denial of service, modification of packets, and therefore the like. These attacks are network exploit during which a hacker makes an attempt to create changes to knowledge on the target or knowledge route to the target. Classify active attacks into four groups: dropping, modification, fabrication, and temporal order attacks. It ought to be noted that AN attack are often classified into over one cluster.

Dropping Attacks

Malicious or narcissistic nodes deliberately drop all packets that aren't destined for them. whereas malicious nodes aim to disrupt the network association, stingy nodes aim to preserve their resources. Dropping attacks will stop end-to-end communications between nodes, if the dropping node is at a crossroads.

Denial of Service (DOS) attack

A DoS attack [9] could also be outlined as occurrences that diminishes or eliminates a networks capability to perform its expected perform. These attacks are launched against server resources or network information measure by preventing approved users from accessing resources. DoS attack might quickly block service availableness or for good distort data within the network. DoS attacks will exhaust restricted wireless resources like information measure, cupboard space, battery power, CPU, or system memory. Networks are attacked by modifying routing data or dynamical system configuration, thereby directly offensive knowledge integrity.

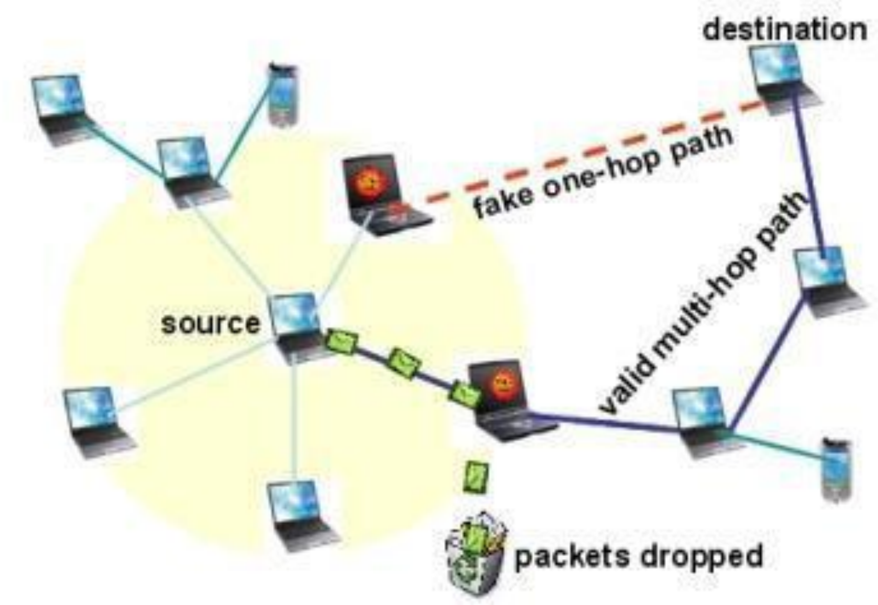

Fig. 3. DOS Attack

Modification Attacks

In a message modification attack an entrant alters packet header addresses to direct a message to completely different networks. In sider attackers modify packets to disrupt the network. for instance, within the sinkhole attack the offender tries to draw in nearly all traffic from a selected space through a compromised node by creating the compromised node enticing to alternative nodes.

4. SECURITY GOALS

- Confidentiality
- Availability
- Authentication
- Integrity
- Non-repudiation

Confidentiality

Confidentiality protects that laptop associated advantages are non-heritable by approved parties solely.it means that solely those that have right to access ought to very acquire that access. Privacy and secrecy area unit synonyms of confidentiality.

Availability

Availability means that advantages area unit gettable to approved parties at appropriate time. Handiness relates to each services and information.

Authentication

Authentication node to safeguard the originality of peer node it is communication with nodes. Authentication is important affirmation that participants in communication are valid and not imitate.

Integrity

Integrity means that the assets is tailored solely by approved parties in a certified method. Adaption includes deleting, creating, writing and dynamical standing.

Non-repudiation

It protects that the sender and therefore the receiver of the message doesn't disclaim that they need ever sent or received such a message.

5. WORMHOLE ATTACK

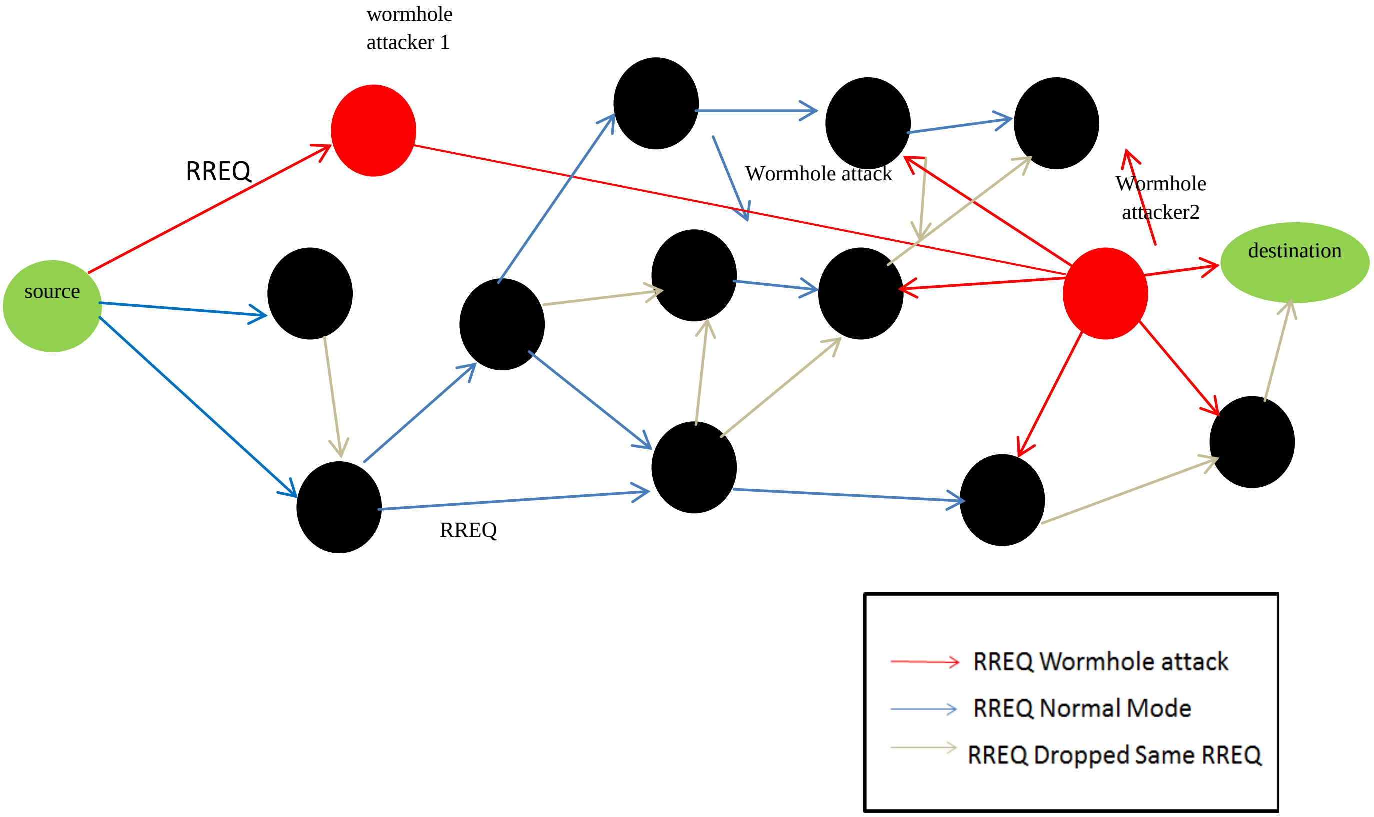

Fig. 4. Wormholehole attack

Dynamic topology feature of painter build these networks extremely liable to routing attacks like wormhole attack. The planning of the routing protocol trusts fully that each one nodes would transmit route request or information packets properly. Wormhole attack consists in recording traffic from one region of the network and replaying the various regions.

Wormhole attack consists of 2 nodes the offender nodes that area unit connected to every alternative with a link primarily this link is thought as tunnel. Node is transmitted packets in one region to a different. Wormhole nodes transmitted pretend shortest route to the destination and discard information packets. So that they believe that the route is shorter than the first one.

Wormhole nodes pretend a route that is shorter than the first one at intervals the network means that it produces illusion for the legitimate node so that they believe that the route is shorter than the first one. However it's not necessary that the route through wormhole nodes is also shorter

6. TYPES OF WORMHOLE MODES

- Packet In-band Channel
- Out-of Band Channel
- High Power Transmission

Packet In-band Channel

This variety of mode the malicious node captures the packet from legitimate node or supply node and encapsulate the packet header of the initial packet and destination it to the other malicious node. When receiving the encapsulated packet alternative the opposite malicious nodes either drop the packet or forward the packet to other nodes that are present within the network. The attacker nodes are at intervals the network.

Out-of Band Channel

During this variety of mode the malicious nodes are connected to every different via associate degree outer link. A channel with high information measure is placed between the nodes at the 2 ends therefore as they will produce hollow link.

High Power Transmission

During this variety of mode once the supply node forward the packet the wrongdoer node captures, it enforces the nodes to follow the trail and then that everyone traffic passes to the present link.

7. MODULE DESCRIPTION

- Initial Bait Step
- Initial Reverse Tracing Step
- Shifted to Reactive Defense Phase
- Hop Latency based worm hole attack detection algorithm

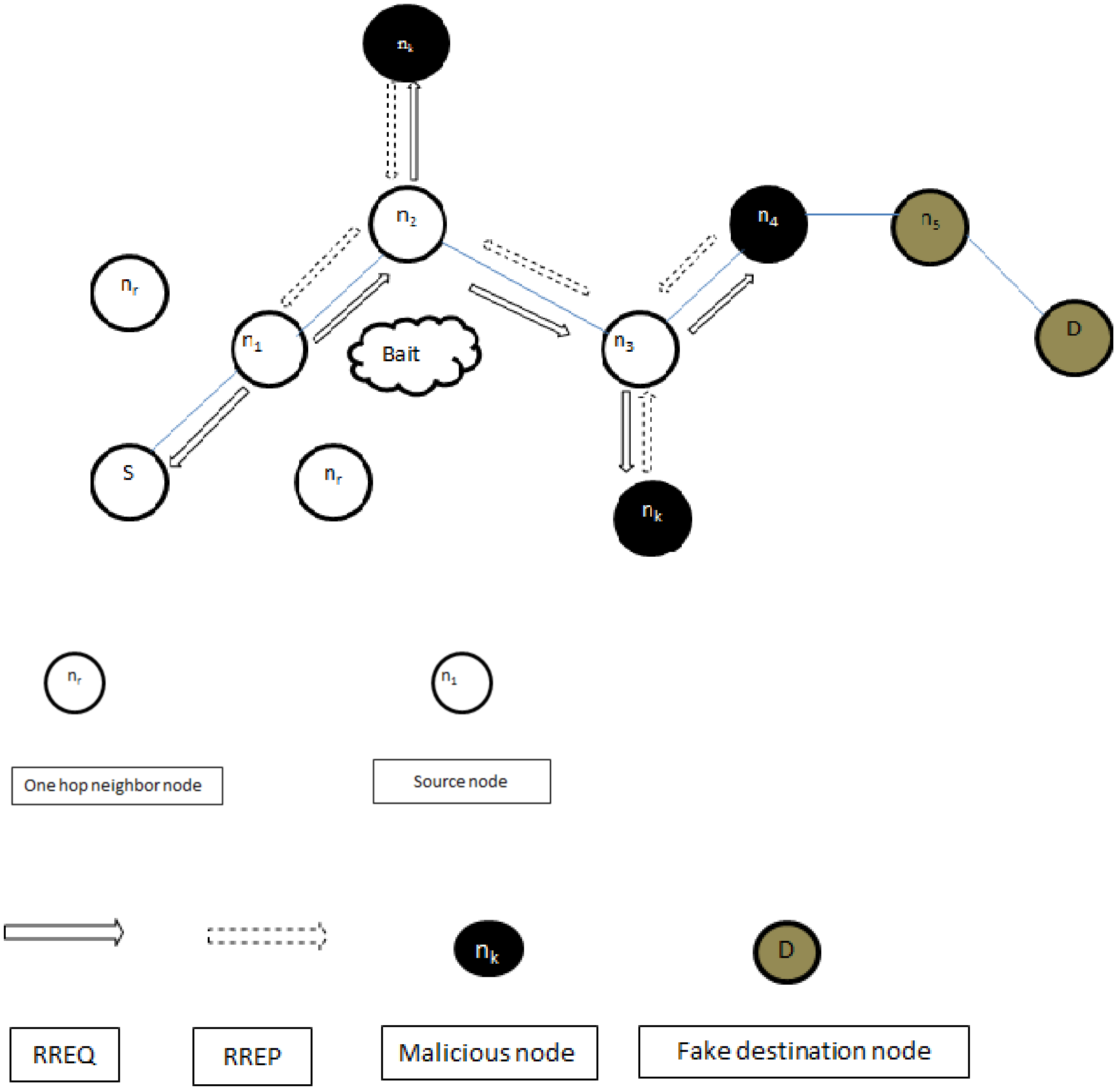

Fig. 5. Random selection of a cooperative bait address

Initial Bait Step

The initial bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ'. It is finding the shortest path node then sends the data packets. The method is designed to generate the destination address of the bait RREQ'. The source node stochastically selects an neighbouring node,i.e., nr, within its one-hop neighbourhood nodes and collaborates with this node by taking its address as the destination address of the bait RREQ' each baiting node is stochastically and the neighbouring node would be changed ,if the node moved the bait would not remain unchanged node had not launched a wormhole attack, then after the source node had sent out the RREQ', there would be other nodes reply RREP in the addition to the n node .malicious node existed in the reply routing.

Reverse tracing program initiated in order to detect this route. Next step nr was the malicious node of the wormhole attack then after the source node had sent the RREQ'. nr purposely gave no reply RREP, it would be directly listed on the wormhole list by the source sent a reply RREP it would mean no other malicious node in the network except the route that n rhad provided. The route discovery phase of DSP will be started. The route nr provides will not list in the route discovery phase.

Initial Reverse Tracing Step

The reverse tracing method detect the behaviours of the malicious nodes through the route reply to the RREQ' message. If the malicious node has received the RREQ', it will reply the false RREP. The reverse tracing operation will be conducted for nodes receiving the RREP, the goal is doubtful path information and the temporarily trusted region in the route.It must be highlighted the CBDS is able to detect more than one malevolent node simultaneously when these nodes send reply RREPs.

Shifted to Reactive Defence Phase

Initial proactive defence, the DSR route discovery process is activated. When the route is recognized and the destination create that the packet delivery ratio significantly falls to the threshold, the detection scheme would be activated. It is again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a change value in the range that can be adjusted to the current network efficiency.

The initial threshold value is to 90%. The designed used in dynamic threshold algorithm that can be controls the time efficiency. The packet delivery ratio falls under the same threshold. If the downtime is shortened, it means that the malevolent nodes are still present in the network. The threshold must be adjusted upward. Otherwise, the threshold will be lowered. The operations of the CBDS are captured.

It should be detected that the CBDS offers the possibility to obtain the doubtful path information of malicious nodes as well as that of neighbour nodes; thereby, it can identify the trusted zone by simply looking at the malevolent nodes reply to every RREP. In addition, the CBDS is accomplished observing whether a malicious node would drop the packets or not. The proportion of dropped packets is disregarded, and malevolent nodes launching a black hole attack would be detected by the CBDS the same way as those launching wormhole attacks are detected.

Hop Latency based worm hole attack detection algorithm

The main characteristic of wormhole attack is that the wormhole peers create the impression of one hop neighbour node but in reality node can be distant separately. Hence the transmission time taken (per hop latency) for a wormhole link is higher than between any two legitimate neighbour nodes. Per Hop latency computation based on round trip time (RTT) is accepted for all links between source and destination nodes during the DSR route discovery phase. The link with maximum RTT “per hop latency” “exceeding threshold value” would be marked as candidate wormhole link and the corresponding nodes as doubtful wormhole peers. RTT is defined as the time difference between DSR RREQ and DSR RREP packet propagation at a node.

$$RTT = RREP - RREQ - RTT\ previous$$

8. CONCLUSION

In this paper, wormhole attack is used to detect the malicious nodes in MANET. Also black- hole attack is used to identify the malicious node. For future work inclusion of a better reactive detection scheme can improve efficiency at real time by monitoring continuously. But wormhole attack is efficiently performed comparing black hole attack.

References

[1] Baadache A and A. Belmehdi (2010), 'Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks,' *Intl. J. Compute. Sci. Inf. Security*, Vol. 7, No. 1.

[2] Chang C, Y.Wang, and H. Chao (2007), 'An efficient Mesh-based core multicast routing protocol on MANETs,' *J. Internet Technol.*, Vol. 8, No. 2, pp. 229-239.

[3] Orson's and J. Macker (1999), RFC 2501, 'Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations'.

[4] Deng H, W. Li, and D. Agrawal (2002), 'Routing security in wireless ad hoc network,' *IEEE Commun. Mag.*, Vol. 40, No. 10.

[5] Gupta S, Subrat Kar and S Dharmaraja., 'WHOP: Wormhole Attack Detection Protocol using Hound Packet'.

[6] IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer.

[7] Johnson D and D. Maltz (1996), 'Dynamic source routing in ad hoc wireless networks,' *Mobile Comput.*, pp. 153-181.

[8] Kozma W and L. Lazos (2009), 'REAct: resource-efficient accountability for node misbehaviour in ad hoc networks based on random audits,' in Proc. *WiSec*, pp. 103-110.

[9] Liu K, D. Pramod, K. Varshney, and K. Balakrishnan (2007), 'An Acknowledgement based approach for the detection of routing misbehavior in MANETs,' *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536-550.

[10] Marti S, T. J. Giuli, K. Lai, and M. Baker, 'Mitigating routing misbehaviour in mobile ad hoc networks (2000),' in Proc. *6th Annu. Intl. Conf. MobiCom*, pp. 255-265.

[11] Piro C, Clay Shields, Brian Neil Levine (2011), 'Detecting the Sybil Attack in Mobile Ad hoc Networks'.

[12] QualNet Simulaton Tool, Scalable Network Technologies (2013).

[13] Ramaswamy Fu S, M.Sreekantaradhya (2003), J. Dixon, and K. Nygard, 'Prevention of cooperative blackhole attacks in wirelessadhoc networks," in Proc. *Int. Conf. Wireless Network,'* pp. 570-575.

[14] Rubin I, A. Behzad, R. Zhang, H. Luo, and E. Caballero (2003), 'TBONE: A mobile backbone protocol for ad hoc wireless networks,' in Proc. *IEEE Aerosp. Conf.,* Vol. 6, pp. 2727-2740

[15] Tsou P C, J.-M. Chang, H.-C. Chao (2003), and J.-L. Chen, 'CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,' in Proc. *2nd Intl. Conf. Wireless Commun*, VITAE, Chennai, India pp. 1-5.

[16] Vasudeva A, Rahul Saha, Mritunjay Kumar Rai, 'Sybil Attack on Lowest Id Clustering Algorithm in the Mobile Ad Hoc Network'(2012), *International Journal of Network Security & Its Applications* (IJNSA), Vol. 4, No.5.

[17] Vishnu K and A. J Paul (2010), 'Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,' *Int. J. Comput. Appl.,* Vol. 1, No. 22, pp. 28-32.

[18] Wang W, B. Bhargava, and M. Linderman (2009), 'Defending against collaborative packet drop attacks on MANETs,' in Proc. *28th IEEE Int Symp. Reliable Distrib. Syst.,* New Delhi, India.

[19] Weerasinghe H and H. Fu (2007), 'Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation,' in Proc. *IEEE IC*, pp. 362-367.

[20] Xue X and K. Nahrstedt (2004), 'Providing fault-tolerant ad hoc routing service in adversarial environments,' *Wireless Pers. Commun.,* Vol. 29, pp. 367-388, 2004.

(Received 02 May 2016; accepted 28 May 2016)