International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 32-38
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

A RESULT PAPER ON DETECTING BLACK HOLE NODES IN MANETS BY ENHANCING CBDS SCHEME

Neeta Sharma
M.Tech (CSE)
BCET, Gurdaspur,
Punjab, India

Dr.Rakesh Gangwar
Associate Professor& Head, Dept. of CSE
BCET, Gurdaspur,
Punjab, India

Abstract: **--A Mobile Ad-hoc network is composed of number of wireless mobile nodesthat are capable of communicating with each other. Network is not secure, due to the mobility and dynamic nature of Manets. In Manets nodes are free to move in anydirection due to which these networks might be more prone to security issues as compared to wireless networks. In this paper, based on DSR protocol, we propose a detection scheme called the Cooperative Bait Detection Scheme (CBDS), which is used for detecting and preventing malicious nodes causing gray hole/collaborative black hole attacks in MANETs. By using the address of an adjacent node as a bait destination address to bait malicious nodes to send a reply message (RREP) and strange nodes are detected using a reverse tracing technique thereby prevents and ensures security.**

Keywords: **Hole, Gray Hole, DSR, CBDS, MANETS, MALICIOUS NODES.**

I. INTRODUCTION

A MANET is considered as self-administrating, infrastructure less network in which nodes are connected to one another using wireless links. Nodes in MANETS itself serves as host as well as router to forward information to neighbor node. There is no any centralized administration. Nodes in Manets are free to move randomly in any direction, so the security becomes the important aspect in MANETS. Each node in Manets has unique identity to communicate with other nodes in a network. From source to destination there is number of nodes to transfer data from one end to another. To transfer data to the destination source needs to find the location as in Manets nodes are free to join and leave the network. Intermediate node is used for transferring data as well as providing routing information. There is no fix topology in these networks, so are highly vulnerable to attacks such as gray hole, black hole. In black hole attacks, malicious node use forged Route Reply (RREP) to claim that it has the shortest route to destination and it drops all the packets. In gray hole attacks, malicious node selectively discards/forwards the data packets.

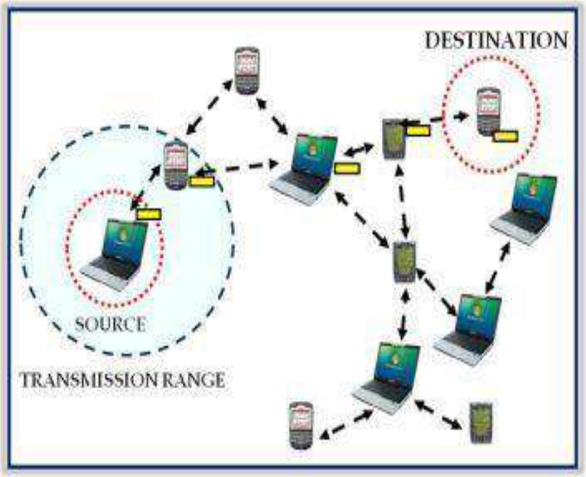

Fig 1. Mobile Ad-hoc Network

A. Characteristics of MANETs

1. **Distributed Operations**: The nodes in a mobile ad hoc network should cooperate with each other and exchange information with each other, and each node performs the function of routing and security as and when needed.
2. **Multi-hop Routing**: When a node has some information that is required to be sent to another node, which is not in its radio range, then the intermediate nodes help them by acting as router to

offer path or link between these nodes.

3. **Dynamic Topology**: As the nodes in MANETs are mobile i.e. can move randomly, so the network's topology can change suddenly. The nodes in the network set their routes dynamically over time.

4. **Energy Constrained Operations**: Each node in the network depends on batteries for their energy, which is limits the capabilities i.e. services and applications provided by a node. This is one of the key concern in the MANETs, as one node act as receiver and router at the same time, so extra amount of energy is required in routing the messages.

B. Overview of DSR Protocol

DSR is a reactive routing protocol. It verifies the best possible route only when packet needs to be forwarded. The process to find a path is just executed when a path is required by a node, which leads to On-Demand Routing.

The DSR protocol is made out of two main mechanisms that cooperate to permit discovery and maintenance of source routes in MANET.

- **Route Discovery**: When a source node S has some data to send to the destination node D, it obtains a route to D. This is called Route Discovery. This phase is used only when Source needs to send a packet to Destination and has no information of a route to it.
- **Route Maintenance**: The existing routes are no longer usable when there is a change in the network topology. In such a scenario, the source S can use an alternative route to the destination D, or invoke former phase. This is called Route Maintenance.

In DSR the sender (source, initiator) determines the entire path from the source to the destination node (Source-Routing) and stores the locations of the intermediate nodes of the route in the packets. In contrast to the reactive protocols ABR or SSA, Dynamic Source Routing is beacon-less which meaning that there are no hello-messages used between the nodes to notify their neighboring nodes about their existence. Dynamic Source Routing was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only travel around at a reasonable speed. DSR is based on the Link-State Algorithms; each node is proficient to save the best way to a destination. Any change noticed in the network topology is broadcasted to the whole network by flooding.

II. LITERATURE SURVEY

In an attempt to find a lasting solution to the security challenges in MANETs, various researchers have proposed different solutions for various security issues in MANETs. However, most of these methods can just detect a single malicious node or need to cost much time and resource to detect cooperative black hole. A number of researches are being carried out for enhancing the security in MANETs. Security in MANETs is still a major concern. Some survey of the researches for the detection of black hole attack and gray hole attack are given:

Jaspinder kaur et.al.in 2014 describes Detect and Isolate Black hole attack in MANET using AODV Protocol **.**The black hole attack is the most common type of attack which is triggered by malicious node which is present in the network. In this work, new technique has been proposed which detect the malicious node and isolate it from the network which is responsible for triggering the black hole attack. The basic idea to detect and isolate malicious node from the network using fake route request packets. In our proposed methodology source node which wants route to destination will flood fake route request packet in the network. The fake route request packets contain the IP address of the node which doesn't exist in the network. The malicious node will reply back to source with the route reply packet. The node which reply with the route reply packet is detected as the malicious node and it is secluded from the network. To isolate malicious node from the network, source again flood the guenon route request packets in the network. The source get various route reply and from the route reply various available paths are there, source never select that path in which the malicious node exist which is been detected in fake route request packets.

Antony devassy et.al.in 2012 describes Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID. Black hole is a malicious node that always gives the false reply for any route request without having specified route to the destination and drops all the received packets. This can be easily employed by exploiting susceptibility of on demand routing protocol AODV. In mobile Ad hoc networks black hole attack is a strict threat which can be prevented by broadcasting the MN-ID (malicious node id) to the whole nodes in the network. The existing method identified the attacked node, retransmit the packets and again find a new route from source to destination.

M.Mohanpriya et.al.in 2013 describes Modified DSR protocol for detection and removal of discerning black hole attack in MANET. They have proposed a modified DSR routing protocol which defines a threshold value and compares the ratio of number of packets received at the destination to the number of packets sent by the destination. If the number of packets received at the destination is less than 80 percent of the packets sent by the source then it initiates the process to detect the malicious node.

H. dehghanet.al.in 2012describes Evaluation of DSR protocol under a new Black hole attack. In this paper, apart, the creators have presented and assessed a novel more damaging attack named Deep Black Hole. This attack promotes fake route reply messages more explicitly than past ones. Assessment of system parameters was performed identified with DSR convention in NS-2. The simulation results demonstrated that this kind of attack, contrasted with common Black hole and selfish nodes, is all the more harming and prompts system dissent of administration. This stabbing brought about a reduction in the quantity of system directing bundles and end-to-end adjourn particularly contrasted with selfish nodes.

Bo yang et.al.in 2012 describes Historical Evidence Based trust management strategy against Black Holes in MANETs. In this study, a approach to avoid gray hole attack, one sort of black hole attack, which is all the more tricky and undercover attack is proposed by the authors. The neighbor watching model taking into account guard dog idea is centered around the direct trust value (DTV) to identify single black hole attack. Authentic confirmation is likewise contemplated against gray hole attacks. Also, the neighbor proposal model that companied with indirect trust value (ITV) is utilized to make out the cooperative black hole attacks. Then again, the authors have tried to adjust the trust values from distinctive neighbor nodes to relieve the harm by their misdirecting.

Bo yang et.al.in 2014 describes Dempster- Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. In this paper, the authors have proposed a Dempster-Shafer (D-S) proof based trust administration system to surmount cooperative black hole attack as well as gray hole attack. In the proposed system, a neighbor watching model in light of watchdog method is utilized to identify single black hole attack by concentrating on the direct trust value (DTV).Demonstrable confirmation is additionally looked into to clash with black hole attacks. At that point, a neighbor suggestion model companied with indirect trust value (ITV) is utilized to make sense of the helpful cooperative black hole attack. D-S proof hypothesis is actualized to join ITVs from assorted neighbors. A percentage of the neighbor nodes may pronounce a false ITV, which impact can likewise be pointed through the proposed strategy.

Harmandeep Singh et.al.in 2013 describes Securing MANETs Routing Protocol under Black Hole Attack. In this paper they were proposing a technique to identify attack i.e. Black hole attack and solution to avoid the black hole attack by ascertain a safe route for secure transmission. Mainly they focused on improving the security of the one of the popular MANET Routing Protocol namely as AODV. In this method they had used very simple and effective way of providing security in AODV against black hole attack that causes the interception and secrecy of the ad hoc wireless networks. The solution detects the malicious nodes and isolates it from the active data forwarding. As from the graphs illustrated in results they could easily conclude that the performance of the normal AODV drops under the presence of black hole attack.
Jian-Ming Chang et al, In Mobile Ad Hoc network, a critical need is creating the communication among the nodes and node must to cooperate with one another. We have proposed a new mechanism (called the CBDS) for detecting malicious nodes in Mobile Ad Hoc Network under gray/collaborative black hole attacks. It achieves its goal with Reverse tracing technique.

AkinlemiOlushola et.al, in this paper presents to beat this issue a new method is taking into account dynamic source routing (DSR) which could be said as helpful prod discovery plan (CBDS). It combines the favors of both proactive and responsive assertion phenomena. This system performs an opposite following procedure which helps in achieving the desire. As an outcome CBDS perform better than the current strategy which incorporates the DSR and 2ACK conventions with respect to parcel conveyance proportion and steering overhead.

A.Agalya et.al, in this scheme, it incorporates the proactive and receptive resistance architecture and arbitrarily collaborates with a stochastic contiguous node. By utilizing the address of an adjoining node as a bait destination location to bait spiteful node to send an answer message (RREP) and unusual nodes are recognized utilizing an opposite following system in this manner counteracts and guarantees security.

Ramandeep Kaur at el. In this paper presents a technique to prevent and detect malicious node attack in MANETs using Cluster head Gateway Switch Routing (CGSR) protocol. The proposed technique detects the malicious node attack on the basis of miss ratio.

Navdeep Kaur at el, this paper presents to beat this issue a new method is taking into account which could be said as helpful sting discovery plan (CBDS). It combines the favors of both proactive and responsive assurance phenomena.

Chin-Feng Lai et al, IEEE, in this paper the author tries to solve the issues of black hole and gray hole attacks caused by malicious nodes by conniving a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS).

C. Deepika Shin at el, Mobile Ad-hoc Network is a wireless temporary network setup by mobile nodes. The work is to detect the black hole attack which acts in groups which is called as co-operative black hole attack. The (CBDS) scheme is based on the DSR routing mechanism is designed to achieve the goal.

RishikeshTeke at el,—mobile specially appointed system is generally utilized as a part of today's reality at this very moment having attributes, for example, remote integration, progressively evolving topology. In MANET portable hubs additionally goes about at this very moment trade the information bundle. Dr.V.Egaiarasu at el, mobile Ad-hoc systems (MANET) are social affairs of self-sorting out portable hubs with aspect topologies and have no static organization.

Navdeep Kaur at el (2014), with the expansion of mobile technology, the wireless communication is turning out to be more widespread than any time in recent memory.

Ramandeep Kaur at el (2013), In this paper, With the fast development in remote innovation, for example, portable workstations, remote telephones, remote sensors, the significance of remote innovation turns out to be more unmistakable.

R. Mehala at el ,The presence of malicious nodes, this requirement may lead to severe security anxieties; for instance, such hubs may disturb the routing procedure .this proposal to research the attainability of modifying our CBDS way to deal with location different sorts of shared assaults on MANETs and to examine the coordination of the CBDS with other surely understood message security plots keeping in mind the end goal to develop an exhaustive secure directing structure to ensure MANETs against villains.

A.Agalya at el, in this paper MANET, a significant need to convey the communication between nodes is that every node ought to work alongside one another. This communication could deal with numerous obstacles made by foe bringing in disconnection. To conquer this issue new system in light of element source directing (DSR) which could be said presently location plan (CBDS).

AkshitaRana et al, in this paper they presents a new technique for defending of wormhole attack in wireless mesh network. Our proposed method based on epigraph relay method and cooperative threading technique. Our evaluation result shows that better prediction of wormhole attack in wireless chaos network. But due to thread generation it takes more time in comparison of another technique. In future we will minimize the calculation time of thread token generation and improve the efficiency of our proposed method.

III. EXISTING WORK

A malicious node is the one which have intention of getting access to the useful information in the network and not letting the packets reaching the desired user. The malicious node causes packet drop in the network. For packet dropping attack to occur malicious node comes in the route from source to destination. Whenever the useful data comes to it, the malicious node simply drops the packets without forwarding them to the destination; sometimes it selectively drops some of the packets. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These malicious nodes may work as a group.

A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it.

In CBDS the initial bait step is used to detect the malicious nodes in the network. In this the neighbor of the source node is randomly chosen as the bait destination address to forward the Route Request messages in the network. After that reverse tracing step is executed, in which packets is sent over the path in which the suspected nodes are present.

This detects the nodes but it results in the larger packet drops in the network occurred in the reverse tracing step to detect the malicious nodes. Our proposed work aims at detecting the malicious black hole nodes at the first step.

IV. PROPOSED SCHEME

In MANET, nodes are self-configuring so it can move freely in any direction. There is no central controller in MANET. Security of the MANET is a big issue. Different types of attacks are possible in MANET. Among various attacks black attack is the severe attack as it drops the packets forwarded to it resulting in the loss of the useful information.

We aim at reducing packet loss caused in the network using CBDS scheme. We will consider single malicious node in the network. Our proposed scheme works in the following way:

1. Source node randomly selects it neighbour as the bait destination address and forwards the Route Request messages in the network.
2. Two cases arise: if the neighbour node selected is malicious or it is genuine node.
3. If the neighbour node selected is genuine, then two Route Replies will be received by the source in the network. One from the malicious node and second from the node itself present in the network.
4. In this scenario, the source node would reject the Route Reply messages received other than the RREP from the neighbour node and store its ID.
5. In other case, if neighbour node is the malicious node itself, the source node would receive only one reply. This would mean that no other malicious node is present in the network. Then source node sends test packets to the neighbour bait node if it forwards packets correctly then ok, if not forwards packets correctly then reject reply.
6. So, in both the cases after storing the suspected nodes ID, the source node would send Route Request message intended to find path to original destination node. In RREQ message, the suspected node ID would also be forwarded so that the nodes do not communicate or send RREQ to the malicious node in order to prevent it from harming the network.
7. Since the RREQ will not be sent to the malicious node, this time only destination node would send RREP to the source node.
8. The source node would choose the shortest path then to forward data to the destination node.

V. RESULT AND SIMULATION

A.**THROUGHPUT-**This is defined as the total amount of data received at the destination from the source divided by the time it takes for the destination to get final packet. The throughput is the number of bits transmitted per second. As the packet dropped is prevented in this work. So throughput of the proposed system is more than existing system.

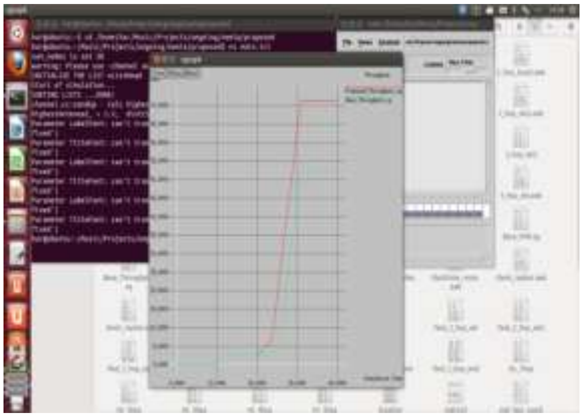

Fig 2. Throughput Graph

B**. PACKET DROP-**It indicates exactly the number of packets dropped in the network. In packet drop graph red line shows the proposed packet drop and green line shows the base packet drop**.**

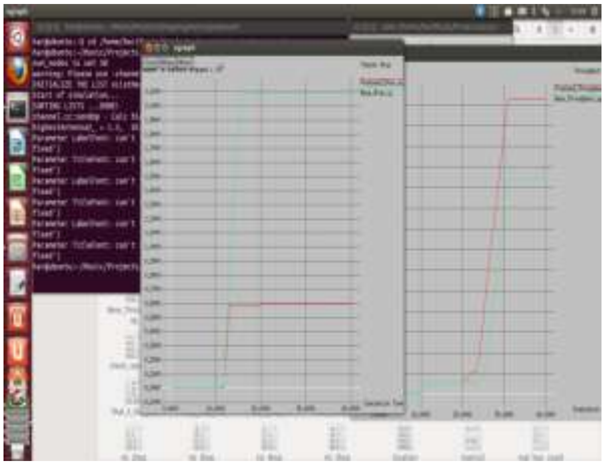

Fig 3. Packet Drop Graph

C**. PACKET DELIVERY RATIO-** This is defined as the ratio of total number of packets delivered to the total number of packets sent to the destination. This indicates the percentage of packets dropped in the network. In packet delivery ratio drop graph red line shows the proposed packet delivery ratio and green line shows the base packet delivery ratio.

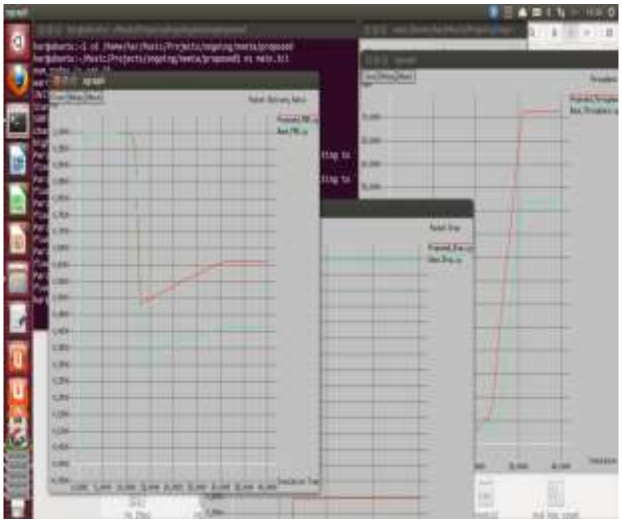

Fig 4. Packet Delivery Ratio Graph

VI. CONCLUSION AND FUTURE WORK

In this paper, we conclude that due to the self configuring nature of the mobile ad hoc network much type of inside and outside attacks are possible which degrades the network performance. In this paper, we proposed a new mechanism (by enhancing CBDS) which is based on the fake route request packets to detect and isolate grey/collaborative black hole attacks in MANET. The proposed technique is implemented in network simulator version 2 and results are analyzed graphically by taking various network parameters like throughput, packet delivery ratio and packet drop. The simulation results show that this technique is more efficient than the previous techniques. As future work, the proposed technique can also be applied to address other types of collaborative attacks on MANETs to increase the performance of the system.

VII. REFERENCE

[1]A.Agalya,C.Nandini, S. Sridevi, ―DETECTING AND PREVENTING BLACK HOLE ATTACKS IN MANETS USING CBDS (Cooperative Bait Detection Scheme) , International Journal of Modern Trends in Engineering and Research (IJMTER), Volume 02, Issue 04, [2015].

[2]AkshitaRana, Deepakshrivastava, ―A defending of wormhole attack in wireless mesh network based on epigraph relay method and cooperative threading technique, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 9, November 2012.

[3] Manjeet Singh, Apurva Sharma, ―Security in MANET Using ECBDS on Resource Consumption Attack and Byzantine Attack , IJITKM Volume 8 • 2015 pp. 4-7.

[4]C.Krishna Priya1, Prof.B.Satyanarayana, ― A REVIEW ON EFFICIENT KEY MANAGEMENT SCHEMES FOR SECURE ROUTING IN MOBILE AD HOC NETWORKS, International Journal of Computer Engineering and Applications, Volume V, Issue I, Jan 14.

[5] AnshikaGarg, Shweta Sharma, ―A Study on Wormhole Attack in MANET, International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 3 Issue 2, May 2014.

[6] Muskan Sharma, ChanderPrabha , Combating Resource Consumption and Byzantine Attacks in MANET through Enhanced CBDS Technique, American International Journal of Research in Science, Technology, Engineering & Mathematics AIJRSTEM 14-543; © 2014.

[7] C. Deepika Shiny *, I. Muthumani, ― Detection and Recovery of Packet Drop under Network Layer

Attack in MANET, International Conference on Electrical, Information and Communication Technology, 28 February 2015.

[8] AdityaBakshi, A.K.Sharma, Atul Mishra, ―Significance of Mobile AD-HOC Networks (MANETS), International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013.

[9] Dr.V.Egaiarasu, D.Kailashchandra, ―Detection of Black Hole and Worm Whole Attacks in MANETS, SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) – volume 2 Issue 3 May to June 2015.

[10] AkinlemiOlushola O., K. Suresh Babu, ―Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET, Volume 3 Issue 4, April 2014.

[11] M. Ahmed Usmani1, ManjushaDeshmukh, ―Defending Against Attacks in MANETs using Cooperative Bait Detection Approach, Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET , International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2014.

[12] NavdeepKaur and Mouli Joshi , ―Implementing MANET Security using CBDS for Combating Sleep Deprivation & DOS Attack, International Journal for Science and Emerging, 2014.

[13] RamandeepKaur , Jaswinder Singh, ― Towards Security against Malicious Node Attack in Mobile Ad Hoc Network, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[14] RishikeshTeke, Prof. ManoharChaudhari,- A Survey on Security Vulnerabilities And Its Counter measures At Network Layer In MANET, RishikeshTeke et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014,

[15] R. Mehala, S.Sathya, M.Sc., M.Phil. , DETECTING MALICIOUS ATTACKS USING DYNAMIC THRESHOLD OPTIMIZATION ALGORITHM, IJCSMC, Vol. 3, Issue. 11, November 2014, pg.212 – 222.

[16] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai ―Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach in Natural Sciences and Engineering Research Council of Canada (NSERC), Taiwan, Dec 2013–Mar 2015, pp. 65–75.