International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

# Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET

**Akinlemi Olushola O.[1], K. Suresh Babu[2]**

[1]M.Tech Scholar, School of IT, JNTU Hyderabad, India
[2]Assistant Professor of CSE, School of IT, JNTU Hyderabad, India

**Abstract:** ***With no dwindling in the use of wireless communication and a corresponding speedy proliferation of research in mobile technology, Mobile Adhoc Network (MANET) have been widely used for various applications such as military crisis operations and emergency rescue operations. The infrastructure-less nature and the dynamic topology features of MANET makes these networks highly vulnerable to various security issues like exploiting vulnerabilities of routing protocols and injecting harmful packets in the network etc. These threats deteriorate causes severe damage to the network. The challenge is how to prevent these security threats in MANETs. In this paper, based on DSR protocol, we propose a detection scheme called the Cooperative Bait Detection Scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs. In this scheme, it integrates the proactive and reactive defense architecture and randomly cooperates with a stochastic adjacent node. 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:** MANET, CBDS, Black Hole, Gray Hole, DSR.

## 1. Introduction

Mobile means 'moving' and ad-hoc means 'temporary without any infrastructure'[13]. Therefore, a mobile ad-hoc network is made up of group of mobile nodes, which cooperates to communicate with each other without any fixed central base station [7]. A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network of mobile devices connected by wireless links. MANET is a kind of point to point transmission type and is a group of mobile nodes communicating with each other by wireless [14]. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network [8] [9]. The topology of the network varies rapidly and unpredictable over time because of the mobility of the nodes. Besides, the security of MANET has many defects. These threats make the security of MANET lesser than a cable network and produce many security issues. Because the communication of MANET uses the open medium, attacker can easily overhear message that are transmitted. The design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make MANET vulnerable to diverse types of attacks [11]. One of common attack is Black hole attack that is a malicious node can attract all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination [11]. This is shown in Fig. 1. Black hole attack is a kind of Denial-of-Service attacks and derive Gray hole attack, a variant of black hole that selectively discards and forwards data packets when packets go through it [11]. Cooperative black hole attacks mean several malicious nodes cooperate with each other and work just like a group. This kind of attack results in many detecting methods fail and causes more immense harm to all network [11].

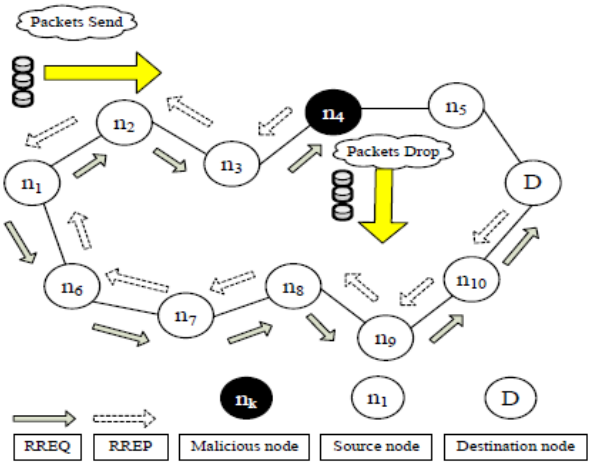


Figure 1. Black hole attack. Node $n_4$ drops all packets

**Malicious Node:** A node under attack due to breaches any of the security principles and is said to be exhibiting a malicious behavior [13].

In this paper we propose CBDS which integrates the Proactive and reactive defense architectures, and randomly establishing a cooperation with adjacent node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program [11]. Finally the detected malicious node is listed in the black hole list and notifies the remaining nodes in the network to halt any communication with them. As a result, my proposed scheme can reduce packets loss that can be cause by malicious nodes and have better throughput [1] [2].

**Paper Structure**

The remaining part of the paper is arranged thus: Section II highlights the security threats in MANETs. Section III describes the detecting and reverse tracing scheme we proposed. Section IV presents the literature work done in the area. Section V contains the conclusion of the work.

## 2. Security threats in MANETs

Since MANETs are widely used due to their capability to form a network without the aid of any centralized infrastructure, security challenges have become a major concern to provide secure communication. Secure communication is guaranteed when the key security principles such as authentication, confidentiality and integrity are present [4]. Absence of centralized administration makes MANETs vulnerable to various types of security attacks [1] [12] and dealing with these is one of the main challenges for the developers [13] [10]. Some of the security attacks that MANETs are susceptible to at different layers in the network are as shown in Table 1

**Table 1:** Attacks in MANETs

| Layer | Attack |
|---|---|
| MAC Layer | Jamming Attack |
| Network Layer | Resource Consumption Attack, Man- in- the- Middle Attack, Neighbor Attack, Routing Attack, Stealth Attack Wormhole Attack, Black Hole Attack, Sinkhole Attack, Gray Hole Attack, Byzantine Attack, Information Disclosure Attack, |
| Transport Layer | Session Hijacking Attack |
| Application Layer | Repudiation Attack |
| Multilayer | DoS Attack, Misrouting Attack, Device Tampering Attack, Jellyfish Attack |

## 3. Cooperative Bait Detection Scheme

This paper proposed a malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes causing black or gray hole attacks and cooperative attacks. It merges the proactive and reactive defense structure, and the source node randomly establishing cooperation with the adjacent node. Using the address of the adjacent node as the destination bait address, it baits malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again, which can achieve the capability of maintenance and immediately reactive response[2][11]. Accordingly, our proposal merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, our mechanism doesn't like the method that just use reactive architecture would suffer black hole attack in initial stage. Although DSR can know the all address of nodes among the route after the source node receives the RREP. Nonetheless, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss. In comparison to DSR, the function of Hello message like AODV was added to help the nodes to identify which nodes are their adjacent nodes within one-hop[11][3]. This function assists in sending the bait address to entice the malicious nodes and utilize the reverse tracing program of CBDS to detect the exact addresses of malicious nodes. In addition, the baiting RREQ packets were created.

**Proposed System Architecture Overview**

This paper attempts to resolve collaborative black-hole attacks issue by designing a AODV routing as DSR-based routing mechanism, which is called **CBDS** (Cooperative Bait Detection Scheme) that integrates the advantages of both proactive and reactive defense architectures [11].

In my approach, the source node stochastically selects an adjacent node with which to establish cooperation, the address of this node is used as bait destination address [11] to deceive malicious nodes to send a RREP reply message.

Malicious nodes are therefore detected and prevented against routing operation, using a reverse tracing technique.

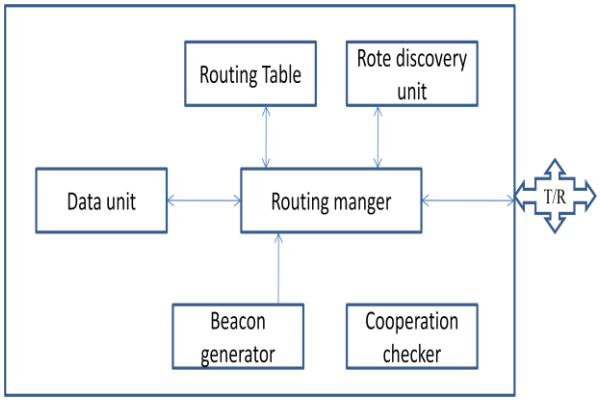


**Figure 2:** Propose System architecture

**Modules**

- Design network
  - Malicious node
  - Legitimated node
- Co-operation checker
  - Beacon generator
  - Neighbor info Manager
- Route discovery

- FREQ generator
- RREQ/RREP processing
- Route maintenance

**Network Design**

In this design, we are mainly dealing with security side, to check my protocol strength; I have to design the attacker and defender nodes. The attacker node able to check the route request and can give the fake reply to the source and attacker can identify the data packet and it will drop. Legitimated nodes can make the cooperation with neighbor and can make the communication, and forwards the data from one to other nodes, and can try to defend from attacker.

**Cooperation Checker**

In this module, we have used the timer to keep the time expire and intimates to generate the periodic packet. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is to store the neighbor information into table when it receives the beacon packet from the neighbor. If the time is got expire the neighbor node info will be deleted from the table

**Route Discovery**

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In this scheme, we are also going to use same method with different style, such as creating the fake route request. The source will generate fake request with destination address as cooperating neighbor. Source already knows the information, for Freq no reply. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism

**Route Maintenance**

In this module, if route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. With secure route discovery model

**Expected Output**

We will show the output in two ways

- Nam (Network animator) window
  - In this window, I can show the animation of packet transfer, packet drops and mobility.

- Analysis
  - Trace file:
    - Stores the information of network events (ex., packet sent, received, dropped at the time, node moved from which place to which place…)
  - Xgraph
    - In this window, I can show the result like as packet delivery radio, packet loss, and delay as graph

## 4. Survey on Overall Development

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:

Kozma, and L.Lazos , "REAct [2][15]: resource-efficient for node misbehavior in ad hoc networks based on random audits," When destination node detects a packet drop; it compels the source node to initiate the audit procedure. Source node chooses an audit node and generates behavioral proof. The same way, the source node prepares it behavioral pattern. Comparison of the results, malicious nodes are determined. The disadvantage was that it is a reactive approach. According to Rashid Hafeez Khokhar, MdAsriNgadi and Satria Mandala [15]," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," Introduced the concept of route confirmation request (CREQ) and route confirmation reply (CREP) to prevent the blackhole attack in AODV. Also it could only detect single black hole. According to W. Wang, B.Bhargava, and M. Linderman [15], "Defending against Collaborative Packet Drop Attacks on MANETs," Introduced the approach of hash based function in REAct system based on the reactive detection. According to Latha Tamilselvan and Dr. V Sankaranarayanan [15]," Prevention of Co-operative Black Hole Attack in MANET" built a scheme for detection of co-operative black hole attack, based on the Fidelity table where presence of 0 indicates a malicious node. But it failed for the case of DSR. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria [15], designed "Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol" suggested a scheme dependent on the details of intrusion detection from local nodes rather than from the source node. This scheme is used only for the case of AODV as it has the advantage of sequence number. According to Sen et al.[13] propose a security mechanism to protect against a cooperative gray hole attack on known AODV routing protocol in MANETs. The proposed system has four modules as: the Neighborhood Data Collection, the Local Anomaly Detection, the Cooperative Anomaly Detection and finally Global Alarm Raiser. According to Lakshmi et al.[13] propose a solution for analyzing and improving the security of Ad hoc On demand Distance Vector routing protocol to prevent black hole attack in MANET. The solution uses Prior Receive Reply method and detect black hole node at route discovery time. According to Das et al.[13] propose a scheme that can detect and remove black hole nodes in MANET at the beginning i.e. during route discovery time. The solution uses extra route to the intermediate node to check whether route from intermediate to the destination node exist or not. According to Chang et al.[11] present a mechanism named Cooperative Bait Detection Scheme (CBDS) based on DSR routing protocol to identify malicious nodes launching black or gray hole attack and cooperative

attacks. According to TSOU et al.[11][13] propose a DSR based secure routing protocol named Baited-Black-hole DSR. It identifies and avoids the black hole attack based on merging proactive and reactive defense approach in MANET with virtual and non-existent destination address to deceive or bait malicious nodes to reply RREP. According to Ramandeep and Jaswinder Singh [13] propose a solution to ensuring security in MANET using cluster head gateway switch protocol. Jian Ming Chang, Po chun Tsuo, Han Chie Chao and Jiann Lieng Chen [11] proposes a cooperative Bait Detection Scheme to Prevent malicious node for MANET using Hybrid Defense architecture.

Others include Mamatha et al.[13] who present a security mechanism capable of identifying and isolating nodes that carry out different types of network layer attacks. Detection is known based on the percentage of number of packets dropped. That particular node dropping packets in excess of the threshold is malicious or misbehaving node. According to Obaidat et al.[13] expanded a recently proposed AODV based on Highly Secured Approach against attacks on MANETs to protect routes in the route selection phase. According to Arya et al.[13] identifies diverse ways for detecting indiscipline or malicious nodes in a MANET. According to Raju et al.[6][13] present an authentication scheme for Mobile Ad Hoc Networks that is designed to combat attacks such as injecting harmful packets, alter packets, drop packets etc. In the scheme, every packet is authenticated at every node. According to Sikarwar et al.[13] propose a framework for protecting communication in ad hoc network using dynamic key cryptography and its comparable study with intrusion detection system. According to Vishnu et al.[7] propose a unique protocol for identifying and removal of network black and gray hole nodes with the help of a backbone network of trusted nodes for restricted IP (RIP) address. According to Sahadevaiah et al.[13] propose a security protocol named cryptographic hybrid key management for secure routing in MANETs, to provide self-organized behavior by distributing the public keys and self-signed certificates among all the nodes to form a network with an initial trust phase. According to Nabet et al. [13] propose an efficient and effective secure routing protocol to ensure routing security in ad hoc networks (ASRP). According to Marti et al. [] presents a method in which contains Watchdog and Pathrater for detecting black hole. The Watchdog employs neighbor nodes to overhear and identify malicious node. Watchdog depends on overhearing the packets whether be discarded deliberately to identify the malicious node.

## 5. Conclusion

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. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for MANETs is still a major concern. My approach is based on using cooperative bait detection scheme to detect and prevent malicious nodes attack in MANETs. My proposal merges the advantage of proactive detection that can avoid just using reactive architecture that would suffer malicious node attack in initial stage and the superiority of reactive response that can reduce the waste of resource.

## References

[1] A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journalof Computer Science and Information Security," Vol. 7, No. 1, 2010.
[2] V. K and A. J PAUL, "Detection and Removal of CooperativeBlack/Gray hole attack in Mobile Ad Hoc Networks," 2010 InternationalJournal of Computer Applications, Vol. 1, No.22, 2010
[3] Scalable Network Technologies (SNT). QualNet.http://www.qualnet.com
[4] Durgesh Kumar Mishra Mahakal Singh Chandel, Rashid Sheikh. "Security Issues in MANET: A Review".
[5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China.Research on MANET Security Architecture design.
[6] G.V.S.Raju and RehanAkbani, "Authentication in Wireless Networks", Proceedings of IEEE 40th Hawaii International Conference on System Sciences, 2007.
[7] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.
[8] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol. 3, ISSN 2151-9617, January 2011.
[9] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO and Jiann-Liang CHEN, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", ICACT, Feb. 2011.
[10] Radhika Saini and ManjuKhari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", International Journal of Computer Applications, Vol. 20, April 2011.
[11] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture", IEEE, 2011.
[12] Ankita Gupta and Sanjay PrakashRanga, "VARIOUS ROUTING ATTACKS IN MOBILE AD-HOC NETWORKS", International
[13] Ramandeep Kaur, Jaswinder Singh,"Towards Security against Malicious Node Attack in Mobile Adhoc Network", International Journal of Advance Research in Computer Science and Software Engineering, volume 3, issue 7, july 2013.
[14] Navdeep Kaur ,Mouli Joshi "Implementing MANET Security using CBDS for combat sleep Deprivation & DOS Attack" International Journal for science and Engineering.
[15] Raja Karpaga, Chandrasekar.P, "Detection and Removal of Cooperative Black Hole/Black Hole Attack in MANET" International journal of Computer Applications, vol. 43, April 2012