ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 2, February 2018

# Review on Malicious Node Detection and Removal in Manets

[1] Niveditha P S, [2] Sreeleja N Unnithan, [3] Prasad R Menon
Dept. of Electronics and Communication engineering
NSS College of engineering, Palakkad

***Abstract:*** **- Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movability and organize themselves arbitrarily. Moreover, other characteristics such as frequent changes of the topology, nodes limitations like energy resource, storage device, CPU and communication channel limitations like bandwidth, reliability add extra challenges. Mobile ad hoc networks aimed to propose solutions to some fundamental problems, such as routing, coping with the new challenges caused by networks and nodes features without taking the security issues into account. Hence, all these solutions are vulnerable to threats. Any node under attack in ad hoc network exhibits an anomalous behavior called the malicious behavior. This paper is a survey on different malicious node detection mechanisms, and the security problems caused due to malicious nodes in mobile ad hoc networks.**

***Keywords:*** **- Malicious node, detection, removal, MANETS.**

## I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a dynamic network composed of mobile nodes that can communicate without relying on an existing infrastructure. Nodes within a communication range communicate directly, while those out of the range make use of other nodes to forward the messages to a given destination. These features make this kind of networks attractive for their application to areas like environmental monitoring, military applications, disaster management, etc. Along with the advances on MANETs and their open media nature, increases the demand for secure routing. MANET possesses many characteristics [3] such as mobility, multi hop communication, dynamic topology, bandwidth constraint and variable link capacity etc. It is vulnerable to various types of attacks due to many security issues such as dynamic nature, limited computation, and lack of clear lines of defense. It is mainly influenced by Denial Of Service (DoS) [4] attacks such as black hole, grey hole, worm hole, impersonation, eavesdropping and replay attacks. A malicious node can easily join the network and starts its malicious behaviour by dropping packets, advertising wrong routing information. A malicious node can silently drops all or some of the packets even when no congestion occurs. This situation becomes more sever when a group of malicious nodes co-operate each other. So, Security in MANET is an essential component for basic network functionalities like packet forwarding, routing and network management performed by all nodes instead of dedicated ones. Network operation can be easily jeopardized if security counter measures are not embedded into basic network functions at the early stages of their design. In order to prevent the adverse effects of routing misbehavior, the malicious nodes must be detected and removed from the network. In this paper we will discuss various techniques for the same but before that we will discuss various security attacks that can occur in MANET and disrupt its normal working operation.

## II. DIFFERENT TYPES OF ATTACKS IN MANETS

Security of communication in MANET is important for secure transmission of information. Attacks on networks come in many varieties and they can be grouped based on different characteristics. There are many ways to diversify attacks:

- Location or source based attacks.
- Behavior based attacks.
- Malicious and selfish node attacks.

Location based attacks are basically of two types:
a) External attacks: External attacks are mainly carried out by node that does not belong or outside the network. They get access to the network by some means and once they get access to the network they start sending bogus packets, wrong routing information and cause denial of service in order to disrupt the performance of the whole network.

b) Internal attacks: In internal attack [6], the attacker has normal access to the network as well as participates in the normal activities of the network. The attacker enters in the network as new node either by compromising a current node in the network or by malicious impersonation and starts its malicious behavior.

Behavior based attacks are also of two types:
a) Active attacks: In active attack the attacker disrupts the performance of the network by stealing important information and destroying the data during the exchange in the network [1]. Active attacks can be an internal or an external attack.
b) Passive attacks: In passive attacks [1], attackers do not disrupt the normal operations of the network but listen to network in order to get important information, what is happening in the network, how the nodes are communicating with each other and how they are located in the network.

**Malicious node attacks:**
a) Denial of Service (DoS) attack:
The first type of attack is denial of service, in which the attacker aims to crab the availability of certain node or even the services of the entire ad-hoc networks. However, as seen so far, they are basically the results of most of the kinds of tampering with network integrity, redundancy and availability. In the traditional wired networks, the DoS attacks are mainly caused by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and the services provided by the target become unavailable.
b) Black hole Attack: Black hole attack is Denial of Service (DoS) attack on routing traffic. Black hole attack has two properties: First, the node advertises itself as having a shortest and fresh route containing larger sequence number and smallest hop count number to a destination node and exploits the mobile ad hoc routing protocol such as AODV, even though the route is not valid, with the intention of intercepting or dropping packets. Second, the attacker drops most of the packets without any forwarding. A black hole can be caused either by a single node or by several nodes in collusion.
c) Worm hole Attack: In a wormhole attack, a malicious node uses a path which is outside the network to route messages to another compromised node at some other location in the network. This attack is hard to detect because the path that is used to pass on information is usually not part of the actual network.
d) Gray hole Attack: A Gray hole attack [8] is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.
e) Eavesdropping attack [9]: This is a passive attack. The malicious node simply listens to the network and observes the confidential information. Later, it uses this information to carry out attacks.
f) Impersonation attack: The attacker assumes the identity of another node in the network and receives messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the attacker is able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion.
g) Sleep deprivation torture: The idea behind this attack as described in [9] is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep.

## III. MALICIOUS NODE DETECTION TECHNIQUES

The notion of malicious node detection in MANETs has been a subject of interest for a number of years. A number of researchers have discussed the problems of malicious node detection in MANETs as follows. Saurabh Gupta et. al. [4] proposed a AOMDV based novel approach for black hole attack named as BAAP. BAAP introduces the concept of legitimacy table, which will be maintained by each node. The good path statistics are based on two different fields: Path count and Sent count i.e. the Legitimacy Ratio of a node is calculated with the help of path count & sent count. Such count calculation gives the picture of correct routing. Rutvij H. Thaveri et. al. [5] proposed an on-demand secure routing protocol for Gray Hole and Black Hole Attacks. It deals with the abnormal routing information provided by the neighbor nodes during path setup and these abnormal nodes will be considered as malicious nodes. The intermediate node uses the routing packets to pass routing and malicious node information to whole network.

Subrat Kar et.al. [6] described a WHOP protocol (Wormhole Attack Detection Protocol using Hound Packet). WHOP suggests the use of hound packet to promote cooperation among the various nodes in the network. Their route selection criteria are purely based on node ID. That is each node must expose its ID during path setup. After the route discovery, source node initiates wormhole detection process in the established path which counts hop difference between the neighbors of the one hop away nodes in the route. The destination node detects the wormhole if the hop difference between neighbors of the nodes exceeds the acceptable level. When malicious nodes form a wormhole they can reveal themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the

latter is a hidden or close one. The merit of the protocol lies in the fact that it can detect hidden worm hole also. Adrian Perrig et. al. [7] proposed an on demand AODV like protocol named as RAP (Rushing Attacks Prevention). The rushing attack, a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. This attack is also particularly damaging because it can be performed by a relatively weak attacker. It uses highly efficient digital signature based cryptography for authentication purpose. A simple delay time based three step authentication neighbor detection protocol is designed to discover a legitimate neighbor. RAP at the cost of higher overhead can find usable routes, thus allowing successful routing and packet delivery. Khalil et. al. [8] proposed a secure routing protocol called LITEWORP. A particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node, which replays it locally. This can have an adverse effect in route establishment by preventing nodes from discovering routes that are more than two hops away. LITEWORP views secure ad hoc routing as a Quality of Service and energy efficiency issue in multi-hop network. The proposed model makes use of time threshold to deliver the packet and simple encryption scheme to authenticate the nodes. This protocol has low storage and processing requirement but it is difficult to find a guard node in a sparse network.

Poovendran and Lazos [9] proposed a model for wormhole attack. Proposed model is based on a graph theoretic model. Small number of network nodes, called guards, is assigned special network operations. It detects and protects against authentication, message integrity and non-repudiation. The proposed model makes use of efficient simple cryptography based on Local broadcast Keys rather than relying on expensive asymmetric cryptography operations. A graph theoretic framework for modeling wormhole links and derive the necessary and sufficient conditions for detecting and defending against wormhole attacks is described in this paper. Based on the framework, it is shown that any candidate solution preventing wormholes should construct a communication graph that is a sub graph of the geometric graph defined by the radio range of the network nodes. Making use of the framework, a cryptographic mechanism based on local broadcast keys in order to prevent wormholes is proposed. This solution does not need time synchronization or time measurement, requires only a small fraction of the nodes to know their location, and is decentralized. Hence, it is suitable for networks with the most stringent constraints such as sensor networks. It is the first to provide an analytical evaluation in terms of probabilities of the extent to which a method prevents wormholes.

Jian-Ming Chang, Po-Chun Tsou et.al. [10] proposed a cooperative bait detection approach defending against collaborative attacks by malicious nodes in MANETs. In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

Pradeep R Dumne, Arati Manjaramkar [11] proposed a Cooperative Bait Detection Scheme to prevent Collaborative Black hole or Gray hole Attacks by Malicious Nodes in MANETs. A method to resolve this problem by using malicious node detection scheme based upon DSR mechanism -cooperative bait detection scheme (CBDS) which uses hybrid defense architectures. CBDS technique helps to find out malicious node by using a reverse tracing technique. Devendra Gupta et. al. [12] proposed a Cooperative approach for Malicious Node Detection in impromptu Wireless Networks. The most important challenge in impromptu wireless networks is energy inefficiency; beneath bound circumstances, it's virtually not possible to interchange or recharge the batteries. Hence it's fascinating to stay dissipation of energy at lower purpose. A number of the issues area unit restricted energy reserve and lack of centralized coordination.

Stefano Tomasin [13] proposed a Consensus-Based Detection of Malicious Nodes in Cooperative Wireless Networks. In a wireless network adopting a cooperative decode and forward protocol, malicious nodes may not forward packets when requested. In this letter they propose to exploit cooperation also to detect malicious nodes. Each

node monitors other nodes' transmissions and apply an adaptive quickest detection (AQD) technique to form an opinion, which is however affected by channel fading. In order to reduce false alarms, opinions are merged with a consensus algorithm at a fusion center, which then blocks malicious nodes. The possibility that malicious nodes report false opinions in order to avoid of being detected is taken into account in the design of the consensus algorithm. Nachammai M [14] proposed a securing data transmission in MANET using an improved cooperative Bait detection approach. To prevent or detect malicious nodes that causes Gray hole or a collaborative black hole attack is a challenge. In this scheme, the malicious nodes and its behaviors are detected using reverse tracing technique by sending RREQ and RREP. However security for transmitting data is not considered by CBDS. In order to have secure transmission after the malicious node detection, the proposed system uses an improved Cooperative Bait Detection approach which incorporates CBDS with message security schemes.

Sougato Adhikari et.al. [15] proposed a Cooperative Network Intrusion Detection System (CNIDS) in Mobile Adhoc Network based on DSR Protocol. This paper conclude that if there is a single intruder node in the MANET and it performs intrusion activities that are sufficient enough to exceed the faulty threshold, then it will get detected as a malicious and intruder node. The same thing is true for multiple malicious and intruder node detection also. But, this system cannot prevent the discovery of future source routes that include intruder nodes (after their detection). This paper, proposes a design of a cooperative network intrusion detection system based on Dynamic source Routing (DSR) protocol with 5 components: a context analyzer, watchdog system (monitor), rating system, alert message verifier and intruder node punishment system. This system is able to identify different types of behaviors of a misbehaving node like suspicious, malicious but not intrusive and both malicious & intrusive. Simulation result shows the effectiveness of our proposal.

T. Prasannavenkatesan [16] proposed PDA-Misbehaving Node Detection & Prevention for MANETs. The open medium, wide distribution of nodes, changing topology and no centralized monitoring makes MANETs vulnerable to malicious attackers. For these types of networks, security is the most essential service to provide protection and prevent malicious attacks occurring in the mobile nodes. Attackers can easily compromise MANETs by inserting malicious or non-co-operative nodes into the network. To compensate MANET from these malicious activities in this paper, it is proposed a new intrusion detection & prevention algorithm named as Packet Dropping detection Algorithm (PDA). MANETs depends on the cooperation of nodes in the network for the forwarding of packets to the destination. The Cooperation requires detecting routes on the neighbor nodes. The cooperative node having malicious activity by the attacker may not forward or drops the packets, partially or fully. By PDA algorithm the neighbor nodes inform about the attacker by raising a global alarm and prevent an intruder from the malicious attacks in the network.

Shubh Lakshmi Agrwal [17] described the analysis of detection algorithm of sinkhole attack & QoS on AODV for MANET. In the Sinkhole attack, malicious node tries to attract data packets of network using its fake routing information in network. Using sink whole attack, data packets can be dropped and routing information can be altered. This research presents an Individual Trust Managing Technique to prevent against sink-hole attack. In this research sinkhole attack is implemented for analyzing different effects on performance of network due to increasing the mobility and probability of attacks. A detection technique is also analyzed for effective detection and removal of attacker node. Neha Sharma [18] proposed a detection as well as removal of Black hole and Gray hole attack in MANET. In this attack the malicious (unwanted node) distract the data packets that it feels is having shortest and the freshest route to the destination node so sender forwards all the data packets to it. After receiving the data packets, it drops them to create a Denial of service attack or processes to extract information from the packet. In this paper a technique is being proposed for detection of the black-hole or malicious node. In this technique, a new procedure a kind of trap method is added in AODV protocol for the detection of malicious nodes. When the Black-hole node is detected after that an alarming method is triggered to make other nodes aware of malicious nodes.

## IV. CONCLUSIONS

This paper discusses various attacks those can occur in MANETs. With the literature review for the malicious node detection techniques, the problem of secure routing in MANETs and various issues involved in the process are discussed. So, the main focus is on the malicious node detection techniques for MANETs proposed in the literature. A brief overview of such proposals has been experienced, which is summarized in tabular form. Thus, it is concluded that MANETs are more prone to malicious node attacks which causes Denial of Service (DoS). This proves to be a setback in MANETs. Thus malicious node detection and its removal are the two main issues that need to be resolved by maintaining the throughput, detection rate.

## REFERENCES

[1] I.-P. Hubaux, T. Gross, I.-y. L. Boudec, and M. Vetterli, "Toward self organized mobile adhoc networks- the terminodes project," Ieee Communications Magazine, vol. 39, no. 1, pp. 118- 124, Jan. 2001.

[2] G. S. Mamatha and Dr. S. C. Sharma "Analyzing the MANET Variaitons, Challenges, Capacity and Protocol Issues" international Journal 0/ Computer Science & Engineering Survey (fJCSES) , voU, no.1 , pp. 14-21 , August 2010.

[3] M. AI-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proc. ACMSE '04, 2004, p. 96-97.

[4] Saurabh Gupta, Subrat Kar, S Dharmaraja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network," in Proc. iCCCT'j j , 2011 , p.468-473 .

[5] Rutvij H. Ihaveri, Sankita J. Patel and Devesh C. linwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad hoc Networks," in Proc. ACCT '12, 2012, p. 556-560.

[6] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet," in Proc. JJT'll, 2011 , p. 226-231.

[7] Yih ChunHu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad hoc Network Routing Protocols," in Proc. WiSe'03 , 2003, p. 30-40.

[8] Issa Khalil, Saurabh 8agchi, Ness B. Shroff, " L1TEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," in Proc. DSN'05, 2005, p. 612-621.

[9] Radha Poovendran and Loukas Lazos, " A graph theoretic fi'amework for preventing the wormhole attack in wireless ad hoc networks," in A CM Journal on Wireless Networks (WINET) , vol. 13, pp. 27 - 59, March2007.