IJCSE International Journal of Computer Science and Engineering Open Access
Review Paper Volume-2, Issue-2 E-ISSN: 2347-2693

A Review of Malicious Node Detection in Mobile Ad-hoc Networks

Dipali D. Punwatkar[1*] and Kapil N. Hande[2]

[1]Department of CSE, PBCE Nagpur, India, dipalipunwatkar05@gmail.com
[2] Department of CSE, PBCE Nagpur, India, kapilhande@gmail.com

www.ijcaonline.org

Received: 12 Feb 2014 Revised: 18 Feb 2014 Accepted: 22 Feb 2014 Published: 28 Feb 2014

***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.

***Index Term*—**Mobile Ad Hoc Networks, Malicious Behavior, Malicious Node Detection Mechanisms, Security

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. Routing in MANET is challenging due to the constraints existing on the transmission bandwidth, battery power and CPU time and the requirement to cope with the frequent topological changes resulting from the mobility of the nodes. Therefore there is a strong motivation for a node to deny packet forwarding to others and being malicious. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Any routing protocol must encapsulate an essential set of security mechanism.

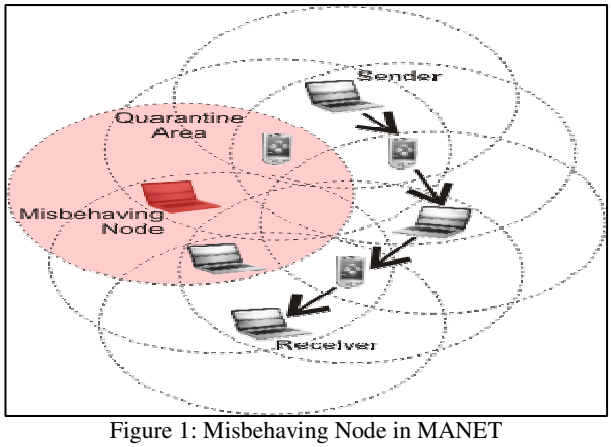

Figure 1: Misbehaving Node in MANET

These mechanisms are used to prevent, detect and respond to security attacks.

In MANET, uncooperative node is malicious node. These nodes are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Malicious node causes packet dropping, false routing and etc.

Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANET.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- No intention for energy-saving.
- Launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

Mobile Ad hoc Network features are given below:

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the
- MANETs are capable of multi-hop routing.

Corresponding Author: Dipali D. Punwatkar

- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- 5 .All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.

The rest of this paper is organized as follows. Section II describes related work. Section III describes malicious node behavior and security attacks. Section IV introduces the problem definition and proposed work. Finally section V concludes the paper.

II. RELATED WORK

The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community.

Watchdog and path rater [16] approach is proposed to detect and isolate the misbehaving nodes. In this approach, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes. However, it has the demerit of not penalizing the malicious nodes.

Buchegger and Boudec[14] suggest that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially.

Trust Evaluation method[19] provides an effective security mechanism based on data protection and secure routing. But it relies on global information and hence the reaction time is more. It would be preferable to reduce the reaction time.

Li Zhao [18] have proposed Multipath Routing Single path transmission (MARS) scheme to mitigate adverse effects of misbehavior. This scheme combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

In the Reputation scheme[17], the reputation of the nodes is assessed based on their past history of relaying packets, and are used by their neighbors to ensure that the packet will be relayed by the node. Instead of choosing the shortest path to the destination, the source node chooses a path whose next hop node has the highest reputation. As a result, the good nodes (nodes with higher reputations) become overloaded. Once the load on the good nodes is more than what the resources can manage, they start dropping packets and start losing reputation. As a result, their incoming traffic is reduced to a level at which they can forward all the packets they receive for relaying. Also the number of route discoveries is more with increase in the average hop length.

Tarag Fahad and Robert [21] Askwith have proposed the new mechanism called Packet Conservation Monitoring Algorithm (PCMA) to detect selfish nodes in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other in MANET. Much of research on security policies focuses on policy representation and evaluation or building security mechanisms based on specific policies without addressing policy enforcement.

K. Sanzgiri et al[20] proposed the Authenticated Routing for Ad-hoc Networks (ARAN) secure routing protocol is an on-demand routing protocol which relies on the use of digital certificates to identifies and defends against malicious actions in the ad-hoc network.

III. MALICIOUS NODE BEHAVIOR AND SECURITY ATTACKS.

There are malicious routing attacks that target the routing discovery phase by not following the routing protocol. The different types of attacks are given below.

1) Modification
Modification is the most common attack; in which malicious node modifies the content fields of routing packets that transit through it. A malicious node could modify packets before rebroadcasting them, so that they include less attractive metrics, false addresses, and fake hop count in order to redirect network traffic. This attack can cause severe routing disruptions such as; conflicted and suboptimal routes, erroneous routing.

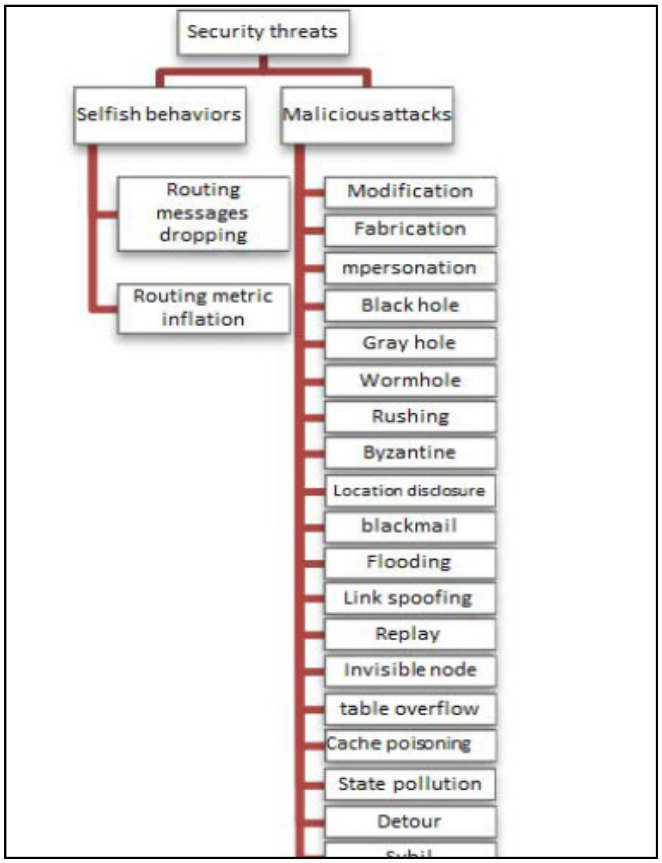

Figure 2. Classification of security threats and malicious attacks caused due to malicious nodes

2) Fabrication
This attack refers to the generation of faked routing messages, in order to disrupt network operation or to deplete other nodes' resources. Such attack is difficult to detect.

3) Impersonation
Also called spoofing attack, it usually constitutes the first step in the majority of attacks. The malicious node hides its real identity and takes legitimate node's identity, thus it can receive all the messages destined to this node and gain access to the network. This attack can also be used for creating loops in order to isolate a target node from the rest of the network.

4) Black hole
This attack exploits the vulnerabilities of routing protocols and it is carried out in two steps. First, the malicious node attracts traffic through itself by advertising better routes to the requested destinations. Afterward, the malicious node drops all the data or control packets passing through it without any forwarding.

5) Gray hole
This attack is a refined form of black hole attack, in which a malicious node drops only selected packets and forwards the others, depends on the source or the destination of packets. Another kind of gray hole may behave maliciously for a given period by dropping all packets then switch to normal behavior later. This attack defeats trust-based mechanisms and makes the detection of malicious node more difficult to achieve.

6) Wormhole
Also called tunneling attack, it is one of the most sophisticated attacks in MANETs. In this attack, a malicious node captures packets from one location in a network and tunnels them through an out-of-band channel to another malicious node located several hops away, which replays them to its neighboring nodes The tunnel between the malicious nodes is actually faster than links between legitimate nodes, so the tunneled packets arrive sooner than packets through other routes. Therefore, the malicious nodes are more likely to be included in the route and take an advantage for future attack. Detection of wormhole attack is generally difficult, and requires the use of an unalterable and independent physical metric, such as time delay or geographical location.

7) Rushing
This attack can be carried out against on-demand routing protocols that use duplicate suppression in their operations. In order to reduce the route discovery overhead, each intermediate node processes only the first received route request packets and rejects any duplicate packets that arrive later. Rushing node exploits this mechanism by quickly disseminating route request packets in order to be included in the discovered routes. Rushing attack can be performed in many ways: by transmitting at a higher wireless transmission power level, by ignoring delays at MAC or routing layers, by keeping other nodes' transmission queues full or by using a wormhole tunnel.

IV PROBLEM DEFINITION AND PROPOSED WORK

Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior of any participating node(s). The main problem is that, there is no guarantee that a communication path is free from malicious

or compromised nodes which deliberately wish to disrupt the network communication**.** Thus protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs).

Another problem in mobile ad hoc networks is that the nodes are resource constraint. Nodes are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality, and non-reputation should be guaranteed during the communication between source and destination. Nodes in MANETs are totally independent from any centralized device and they are free to move anywhere. This causes suddenly appearance and disappearance of the nodes and moving of nodes from one place to another place also increases the probability to compromise. Thus it is necessary to keep the track of nodes in the network that participate in data packet transmission.

Ad hoc network might consist of several home-computing devices, including laptops, cellular phones, and so on. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop. Hence Intermediate node play a key role for honest and secure communication.

Any node under attack in ad hoc network exhibits an anomalous behavior called the malicious behavior. In this situation, the entire operation of a network gets disturbed and to preclude such malicious behavior several security solutions have been discovered. The proposed work is to identify malicious behavior of a node and to defend such behavior; security solutions are presented which are used in furnishing a secure and reliable communication in ad hoc.
In this paper we mainly focus on two attacks and proposed routing protocol.

1) Bandwidth Consumption DoS Attack
Network bandwidth denial of service (DoS) attacks seek to consume the available bandwidth or router resources at or near a target host or network, such that legitimate traffic cannot reach its destination. The primary means for achieving this goal by sending large traffic volumes (packet floods) that do not respect congestion control signals, such as that in the Transmission Control Protocol (TCP) or Explicit Congestion Notification (ECN). In wireless networks, such attacks can also be carried out through radio jamming.

Defending against bandwidth DoS attacks is often difficult for the target site, because the congestion usually occurs upstream (farther in the network) from any equipment that the site controls (e.g. a router or firewall). For an effective response, a target site typically needs to coordinate a response with its parent ISP. If the attack traffic is easy to characterize or otherwise “stands out”, such as a UDP packet flood against a web site, blocking at an appropriate upstream location by the ISP is relatively straightforward. When the attack traffic is not easy to characterize, or the necessary router resources or features are not available for filtering, ISPs resort to black holing.

In that case, a routing entry for the target’s network prefix (which may include other, otherwise un-targeted sites) is injected into the ISP’s routing protocol. That entry points effectively causes all traffic to the target, both legitimate and attack, to be dropped by the ISP routers. In this way, the attack traffic is dropped as soon as it enters the ISP’s network, thereby avoiding link congestion. Since legitimate traffic to the target site is also dropped, black holing does not help restore access to said site.

2) Buffer Overflow Attack
Buffer overflow attacks: stack based and heap based. Heap-based attacks flood the memory space reserved for a program, but the difficulty involved with performing such an attack makes them rare. Stack-based buffer overflows are by far the most common.

In a stack-based buffer overrun, the program being exploited uses a memory object known as a stack to store user input. Normally, the stack is empty until the program requires user input. At that point, the program writes a return memory address to the stack and then the user's input is placed on top of it. When the stack is processed, the user's input gets sent to the return address specified by the program.

However, a stack does not have an infinite potential size. The programmer who develops the code must reserve a specific amount of space for the stack. If the user's input is longer than the amount of space reserved for it within the stack, then the stack will overflow. This in itself isn't a huge problem, but it becomes a huge security hole when combined with malicious input.

3) Dynamic Source Routing Protocol (DSR)
DSR is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. In DSR (Dynamic Source Routing) routing protocol for MANET (Mobile Ad hoc Networks), malicious nodes can easily disrupt the communication. There may be nodes in network some of which may actively want to attack the network. As nodes are part of the network such attacks can be easily carried out and cause a lot of damage. In the proposed scheme, a mechanism of defense against Buffer Overflow and Bandwidth consumption would be implemented, this will be done by identifying the malicious nodes which are not behaving properly and

excluding such nodes from the source routing table maintained at the source node. The implementation of mechanism to identify the malicious node would make the protocol secure from such attacks.

V. CONCLUSION

In this paper, malicious behavior of node is discussed and security solution to defend such behavior is defined. The objective of this paper is to prevent denial of service attack which could be caused by malicious node by creating buffer overflow and malicious bandwidth consumption and make DSR more secure. This paper concludes that with the introduction of any attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increase in checksum errors and packet loss ratio. So it is very important for any network to detect these malicious nodes and isolate them from the network for the proper and smooth functioning of MANET.

REFERENCES

[1]. R. Gopal, V. Parthasarathy, A.Mani,“ Techniques to Identify and Eliminate Malicious Nodes in Cooperative Wireless Networks”, IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), Jan **2013**.

[2]. Dipali Koshti and Supriya Kamoji, “ Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks” International Journal of Soft Computing and Engineering (IJSCE) , Volume-**1**, Issue-**4**, September **2011**.

[3]. Radhika Saini and Manju Khari, “ Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network” International Journal of Computer Applications, Volume **20**– No.**4,** April **2011**.

[4]. G.S. Mamatha and Dr. S.C. Sharma, “ Network Layer Attacks and Defense Mechanisms in MANETS- A Survey” International Journal of Computer Applications (0975 – 8887),Volume **9**– No.**9**, November **2010**.

[5]. Jaswinder Singh and Ramandeep Kaur , “Towards Security against Malicious Node Attack in Mobile Ad Hoc Network”, IJARCSSE Volume 3, Issue 7, July **2013**.

[6]. S.B.Aneith Kumar S.Allwin Devaraj J. Arun kumar, “ Efficient Detection of Denial of Service Attacks in MANET” IJARCSSE, Volume **2**, Issue **5**, May **2012**.

[7]. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, “A Survey Of Routing Tacks In Mobile Ad Hoc Networks” IEEE Wireless Communications, October **2007**.

[8]. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, “Security In Mobile Ad Hoc Networks: Challenges And Solutions” IEEE Wireless Communications, February **2004**.

[9]. C.Siva Ram Murthy and B S Manoj, ―Mobile Ad Hoc Networks-Architecture and Protocols, Pearson Education,ISBN 81-317-0688-5 **,2004**.

[10]. Theodore S. Rappaport, “Wireless Communication” Prentice Publisher, ISBN 0133755363, January **1994**.

[11]. “Intrusion Detection System” http://www.intrusiondetection system-group.co.uk/, Link visited on December **2010.**

[12]. William Stallings “Cryptography and Network Security”, Fourth Edition, Pearson Education. ISBN **978-81- 7758-774-6, 2006**

[13]. Jangra1,A. Goel,N. Priyanka and Bhati,K. - Security Aspects in Mobile Ad Hoc Networks(MANETs):ABigPicture,International Journal of Electronics Engineering, pp. **189-196**, **2010.**

[14]. S. Buchegger and J. Boudec, “Performance Analysis of the Confidant Protocol,” Proc. Int’l Symp, Mobile Ad Hoc Networking and Computing, **2002**.

[15]. Y.Huang and W.Lee, “A cooperative IDS for adhoc network Security of adhoc and sensor networks”, ACM, **2003**,pp.**135-145.**

[16]. D. Djenouri and N. Badache, “Struggling against selfishness and black hole attacks in MANETs,” Wireless Commun. and Mobile Computing, no. 8, pp. **689–704, 2008.**

[17]. V. Srinivasan, P. Nuggehalli, C.F. Chiasserini and R.R Rao,”Cooperation in wireless Ad Hoc Network”, in IEEE INFOCOM, California, USA, **2003**.

[18]. Li Zhao and José G. Delgado-Frias 'MARS: Misbehavior Detection in Ad Hoc Networks“ IEEE GLOBECOM **2007** proceedings.

[19]. Idris M. Atakli, Hongbing Hu, Yu Chen*,Wei-Shinn Ku ,Zhou Su “Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation” **2008** SpringSim

[20]. Dahai DU, Hong FAN, Guan WANG” A Secure Routing Protocol for Mobile Ad hoc Networks “Journal of Computational Information Systems **9**: **22 (2013) 9023–9030**

[21]. Tarag Fahad & Robert Askwith”A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks “ ISBN: **I-9025-6013-9c 2006** PGNet.

AUTHORS PROFILE

Author is a student of M.Tech. Computer Science and Engineering of Nagpur University. she had completed graduation in bachelor of engineering in Computer Engineering from Nagpur University, Nagpur, Maharashtra, India in 2010