NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 4, Apr.-2017

TECHNIQUES FOR PREVENTING AND DETECTING MISBEHAVING NODES IN MANET: A SURVEY

POOJA L.CHELANI
Lecturer, Govt Polytechnic,Mumbai

USHA C.KHAKE
Lecturer, Govt Polytechnic,Mumbai

VANDANA S.LOKHANDE
Lecturer, Govt Polytechnic,Mumbai

ABSTRACT:

A Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other throughradio waves without the aid of any stand-alone infrastructure or centralized administration. These nodes are self-organizing and self-configuring and they act as both hostas well as routers.In MANET each node is free to move independently.MANET is simple and flexible hence widely used in military communication, emergency communication and mobile conferencing. Due to dynamic nature and no certification authority, MANETs are more prone to different types of attacks. The essential requirement for the establishment of communication among different nodes in MANET is that, nodes should cooperate with each other. If misbehaving nodes are present, it may lead to serious security concerns. This paper reviews various techniques available for detecting and preventing malicious node behaviour. Each paper is reviewed with the metrics like type of misbehaviour, detection mechanism, advantages and limitations. Based on our review we are proposing the improved bait detection mechanism.(IBDS), for the detection of misbehaving node that combines the advantages of both proactive and reactive defense schemes.

KEY TERMS: MANET, Attacks in MANET, Misbehaving Nodes, Malicious Nodes, Selfish Nodes, Intrusion Detection system.

1. INTRODUCTION:

Mobile Ad hoc network (MANET)is a collection of autonomous mobile nodes. Mobile nodes can be laptops, cell phones, PDAs etc. Each node in MANET is equipped with a wireless transmitter and receiver, which allows it to communicate with other nodes in its radio communication range without any fixed infrastructure. If a node wants to forward a packet to a node that is beyond its radio range, the cooperation of other nodes in the network is needed. MANET is simple and flexible hence widely used in military communication, emergency communication and mobile conferencing. As MANETs are widely used, the security issue has become one of the important concerns. Only one compromised node can cause the failure of the entire network. There are two types of attacks, passive and active attacks in MANETs [1]. In passive attacks, packets containing secret information might be eavesdropped, which may violate confidentiality. Active attacks include deleting or dropping packets, modifying the contents of packets, and simulating other nodes that violate availability, integrity, authentication, and non-repudiation.

1.1 CHARACTERISTICS OF MANET [2]:

MANET has various characteristics like:

- Wireless Communication Medium
- Dynamic Network Topology
- Can be set up anywhere easily
- No need of centralized administration
- Nodes can acts as both transmitter and receiver
- No fixed infrastructure needed and Multihop Routing

1.2 MANET VULNERABILITIES [2]:

Vulnerability is a flaw or weakness in security system. Due to infrastructure less property and dynamic topology MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows

- No Centralized Authority
- Limited Power Supply
- No predefined Boundary
- Nodes can join and leave network at any time

1.3 ATTACKS IN MANET[2]:

Attacks in MANET can be classified into Passive and Active attacks.

1) Passive attacks: A passive attack does not modify the data transmitted within the network. Packets containing secret information might be eavesdropped, which may violate confidentiality. Passive attack does not disturb the operation of routing protocol.
2) Active attacks: Active attacks are severe attacks that disrupt the operation of routing protocol. Active attacks includes deleting or dropping packets,

modifying the contents of packets, and simulating other nodes.

Various attacks studied in the literature [3], [4] are described below.

DENIAL OF SERVICE ATTACK: This attack restricts access to a certain resource.

IMPERSONATION: Malicious node act as genuine node and then analyse network traffic.

EAVESDROPPING: Node listens confidential information like location, public key, private key, password etc.

BLACK-HOLE ATTACK: A malicious node sends fake routing information and claims that it has a most favourable route. It then causes other genuine nodes to route data packets through the malicious one. A malicious node drops all received packets instead of forwarding those packets to intended recipients.

MAN-IN-THE-MIDDLE ATTACK: An attacker sits between the sender and receiver and listens information being sent between two nodes.

WORMHOLE ATTACK: Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network.

SPOOFING: Spoofing attack takes place when a malicious node gives false information about its own identity, and then forces sender to change the topology.

1.4 MISBEHAVIOUR OF NODES:[5]

"Misbehaviour" refers to node that has an unusual behaviour.If behavior of node deviates from its specification then the node is said to be misbehaving. Misbehaviour can be in following ways:

- Drop Packets
- Delay Packets
- Drop Acknowledgements
- Delay Acknowledgements
- Modify routing information
- Don't forward packet to save its own resources
- Forward control packets while dropping data packets

Due to this misbehaviour of nodes MANET is vulnerable to various types of attacks. In this paper we discuss various techniques for detection of misbehaving nodes. Each technique has its own advantages and disadvantages.

In section 2 we covered literature survey of different techniques for detection of misbehaving nodes. Section 3 includes comparison of surveyed techniques. In section 4 we Proposed an Improved Bait detection Scheme (IBDS) to detect misbehaving nodes. In section 5 we covered conclusion and direction for further research.

2. LITERATURE SURVEY:

Many research works have studied the problem of Misbehaving node detection in MANETs. In general, detection mechanisms can be grouped into two broad categories.

1) **Proactive detection schemes** are schemes that need to constantly detect or monitor nearby nodes. In these schemes even if malicious nodes doesn't exists, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However advantage of these schemes is that it can help in preventing or avoiding an attack in its initial stage.

2) **Reactive detection schemes** are those that trigger only when the destination node detects a significant drop in the packet delivery ratio.

Based on above classification we will review various detection techniques.

In [6]S. Marti, et al proposed mechanism for detection of misbehaving nodes. It describes two modules, Watchdog and Pathrater [6]. Watchdog identifies misbehaving nodes and Pathrater computes a route to avoid these nodes. Misbehaviour discussed here is about dropping data packets.The Watchdog listen promiscuously to the next node's transmission, checking that the node correctly forwards the packet it has received.. Watchdog maintains a buffer of recently sent packets.It compares each over-heard packet with the packet present in buffer. If match found, the packet in the buffer is removed. It then assumes that the packet has been already forwarded. While if a packet is present in the buffer for long time and watchdog overhears that the node failed to forward packet within predefined time then watchdog increases failure counter of a node.

Each node will have its failure counter having a predefined threshold value.If the failure counter of any node exceeds threshold value then watchdog reports that the node is misbehaving. It then sends a message to the source about misbehaviour of a node. Pathrater uses the information given by Watchdog and avoid those malicious nodes in further transmissions. Watchdog fails in situations like ambiguous collision, receiver collision, limited power transmission, false misbehaviour reporting, collusion and partial dropping.

In [7] N. Nasser and Y. Chen describes mechanism for detection of misbehaving nodes, known as ExWatchdog.ExWatchdog is extension to Watchdog

technique. Using this mechanism, limitation of Watchdog mechanism(False misbehaving) has been overcome. Ex watch dog aims to detect nodes that falsely report other nodes as misbehaving. It maintains a table that stores entry <source, destination, sum, path>.The current node may be the source, the destination or the intermediate node, it inserts such an entry into the table when sending, forwarding or receiving packets for the first time. Here Sum is the total number of packets that the current node sends, forwards, or receives. Path is the route that is used for the communication between<source, destination>. When an intermediate node on a route path reports to the source that its next hop is malicious, the source will not immediately treat this as malicious node. Instead, it will send a message to the destination using an alternative path in the routing table. The message contains <Source, destination, path, malicious_node_address>,malicious_node_address is the address of the node being reported malicious. The source node then searches a path that has no malicious node in it from the routing table. If there is no such path available, the source then initiate a Route Discovery to find a new one. After finding a path, the source sends the message using the new path. Upon receiving the message, destination node will search its own table to see if there is a match. If there is no matching entry in the table, it means the node is malicious and the destination node returns a message to the source confirming that the malicious node is really malicious. Ex Watch dog could solve only the problem of false misbehaviour reporting but other problems of Watchdog are still there.

In [8] Liu et al. proposed a 2ACK scheme for the detection of routing misbehaviour in MANETs. It is a network layer detection scheme to detect malicious nodes. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received or not. A parameter acknowledgment ratio is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme is proactive scheme and hence produces additional routing overhead regardless of the existence of malicious nodes.

In [9] Buchegger, et al discusses reputation based scheme for detection of misbehaving node. The technique is known as CONFIDANT (Cooperation of Nodes: Fairness in Dynamic Ad Hoc Networks), which is actually a routing protocol. CONFIDANT mechanism has four working components, namely, Monitor, Reputation System, Path Manager and Trust Manager. Using Monitor component node can detect deviations of next node on source route. It can be done her by listening to next node's transmission. Alarm message is sent to the Trust Manager for giving warning information. It notifies about the misbehaviour of node. Each node maintains Local Rating Lists. Such lists can be used in route request to avoid bad nodes along the route to destination. It also helps to ignore the requests from malicious nodes about forwarding packet. Rating is updated only if there is sufficient evidence of malicious behaviour that is significant for a node and that has occurred a number of times, exceeding threshold.Evidences can be taken either from Monitor Component or Trust Manager Component.

In [10]S. Subramaniyan and W. Johnson proposed a reputation based scheme to detect selfish nodes. Technique is known as Record and Trust Based Detection Technique. This technique analyzes detection of selfish node during routing and packet dropping.In this technique trustworthiness of a node is evaluated based on their behaviour. By building trust model for a node we can evaluate trust of its neighbouring nodes. Trust scheme helps to detect abnormal behaviours of node. When nodes with selfish behaviour are detected, neighbouring nodes do not cooperate with such selfish nodes. Each node has a global trust state for all selfish nodes in network. The trust state is maintained in the form of Trust Table. Trust Table has two fields, node id and trust value. Trust state of node is updated after receiving new trust certificates. Evaluation of a certificate can be done by verifying response from every neighbouring node Trust for a node can be calculated as follows. Collect the information such as Energy, Packet Count, and Queue Size from neighbours. It then generates report and need to validate report rules. Review the current trust value. Compare current trust value with threshold value. If current trust value is greater than threshold value then the node is detected as selfish node and this selfish node is added to Black List.This method of selfish node detection is very efficient. It also enhances packet delivery ratio, reduces average packet drop ratio hence reduces overall overhead.

In[11] Xue and Nahrstedt proposed a prevention mechanism called best effort fault tolerant routing (BFTR). BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path in use and this is compared with predefined behavior of good routes. If the behaviour of the path deviates from a predefined behaviour set, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes.

In [12] P.N.Raj and Swadas proposed Detection, Prevention and Reactive AODV (DPRAODV) Scheme to

detect misbehaving nodes. In DPRAODV as compared to normal operation of AODV, an additional check is done to find whether the RREP_seq_no value is higher than the threshold value which is predetermined. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list.ALARM packet is sent to its neighbours. Later, if any other node receives the RREP packet it checks the black list. If that node is found in the black list, it simply ignores it and does not receive reply from that node again.

In [13] Mistry N. Jinwala Proposed a solution for analyzing and improving the security of AODV routing protocol against malicious node attack. This scheme modifies the working of source node using additional function pre_receive_reply. A table cmg_rrep_tab, a variable mali_node and a new timer mos_wait_time are also added to the default AODV. After receiving the first RREP, the source node waits for mos_wait_time and mean while it stores all the RREPs in the cmg_rrep_tab table until mos_wait_time. In this technique the value of mos_wait_time is considered to be half the value of rrep_wait_time. The source node will analyze the stored RREPs and will discard the RREP which have high destination sequence number. The node which has sent these RREP with high destination sequence number is considered to be malicious node. This technique also records the identity of suspected malicious nodes as mail_node, so that in future it can discard messages coming from that node.

In [14] Jian-Ming Chang proposed a detection scheme called the cooperative bait detection scheme(CBDS),for detecting malicious nodes in MANETs causing black hole attack.In this technique, the source node randomly selects a neighbour node and the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP . Whenever the malicious nodes reply they are detected and prevented from participating in the routing operation, using a reverse tracing technique. At some later time packet delivery ratio is checked at the destination and if it drops to a certain threshold, an alarm is sent by the destination node to the source node to trigger the detection mechanism again. This scheme is hybrid scheme i.e it combines characteristics of proactive and reactive defense schemes.

3. COMPARISION OF EXISTINGTECHNIQUES:

In this section different techniques of Misbehaving node detection are compared against various parameters like Misbehaviour type, Mechanism used for Detection, effectiveness and summarized in Table-1.

Table-1

Technique	Misbehaviour Type	Mechanism used for Detection	Advantages	Limitations
Watchdog 2000	Drop Data Packets	Listens to its next hop's transmission	Network throughput increased by 17%-27%	Receiver collision,limited transmission power,False Misbehaviour report
EX-Watchdog 2007	Drop Data Packets	Detects a node that sends false report	Solves problem of false misbehaviour. ,Throughput increased by 11% more than Watchdog.	Receiver collision,limited transmission power,Partial dropping
BFTR 2004	Drop Data Packets	end-to-end acknowledgements to monitor the quality of the routing path	BFTR can work in environments where malicious nodes collude.	routing overhead increases as the number of misbehaving nodes increases
DPRAODV 2009	Drop and delay packets	Check whether the RREP _seq_no value is higher than the threshold value	The PDR is improved by 80- 85% than AODV when under black hole attack	A little bit higher routing overhead and end-to-end delay than AODV
Nital Mistry et al.'s Method 2010	Drop Data Packets	Additional table cmg_rre_tab and variables mali_node, mos_ wait time are used	The PDR is improved by 81% when network size varying, and rise 70% when mobility varying	Rise in end-to-end delay is 13.28% when network size varying, and rise 6.28% when mobility varying
2ACK scheme 2011	Forwards control packet and drops data packets	2ACK packet is sent back only for fraction of received packets	Packet delivery ratio is improved to 90%	Suffers from false misbehaviour
CONFIDANT2014	Drop Data Packets	Listens to its next hop's transmission	Throughput increased by 10%	Receiver collision,limited transmission power,False Misbehaviour report
RTBD 2014	Drop Data Packets	Trustworthiness of a node is evaluated	Packet delivery ratio is increased by 18%	No security for neighbouring nodes
CBDS 2015	Attracts nodes to send packets and Drop data packets	Bait packet is sent to attract misbehaving node to send reply	The PDR isimproved by95% whennetwork sizevarying, and rise 90% whenmobility varying.	every time the address of next neighborhood is taken as bait destination address, less randomness

4. PROPOSED SOLUTION:

This paper proposes a detection scheme called Improved bait detection scheme(IBDS) which detects malicious node in MANET causing black hole attack. The technique discussed in [14] has limitation that every time the address of next neighbourhood is taken as bait destination address, but if at some time the malicious node become intelligent and doesn't reply to this bait address then this technique would fail. Our technique overcomes this limitation by improving Initial Bait step. The proposed scheme has following three steps.

1. Bait step
2. Reverse Trace
3. Reactive defense.

1. Bait Step: In the first step the source node sends Bait packet i.e RREQ' packets with random and non existent destination address to attract malicious nodes to send reply. As soon as the mailicious node will send reply , the node is stored in black list and alarm packets are send to all the nodes.
2. Reverse Trace: In second step Reverse tracing is performed to confirm the malicious nodes and to check the behaviour of malicious node by sending test packets.
3. Reactive Defense: In third step Packet Delivery Ratio at the destination is checked and if it falls to certain threshold, again the Bait step is triggered. Working of IBDS is shown in fig 3.

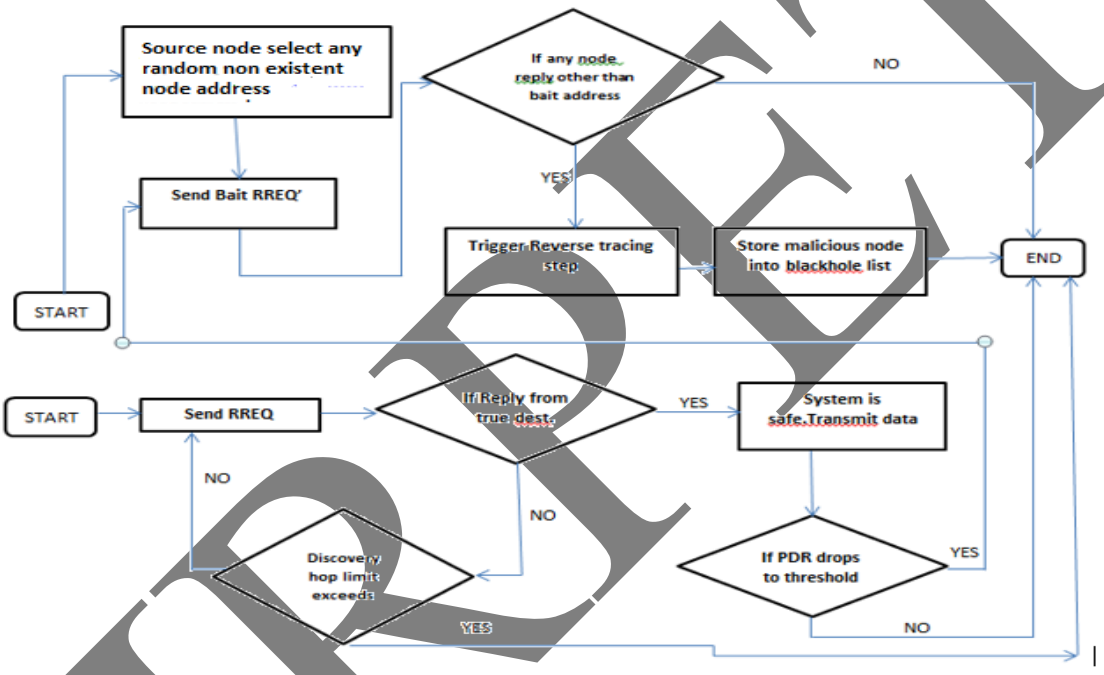

Fig 3. Flowchart of IBDS

Since there is randomness in initial bait step, the malicious node will be detected efficiently and system performance will be improved.

5. CONCLUSION:

This paper Reviews and compares various existing techniques for detecting and preventing Misbehaving nodes in MANET. Some schemes are proactive defence schemes which provides prevention at early stage but prone to repeated routing over head. while some schemes are reactive defence schemes that are on demand defence schemes ,these schemes get triggered only when the packet delivery ratio drops at the receiver. Existing techniques are reviewed and compared with the metrics like type of misbehaviour, detection mechanism, advantages and limitations. The paper proposes an hybrid defense scheme called Improved Bait detection scheme(IBDS) to detect malicious nodes causing black hole attack which is an improvement over the existing CBDS[14] technique.

REFERENCES:

1) Y.Xiao, X.Shen "*A Survey on Intrusion Detection in Mobile Ad Hoc Networks*," in Wireless / Mobile Security: Springer- Verlag, 2006.
2) S.S.tyagi, Aarti *"Study of MANET:Charecteristics,challenges and security attacks*" International journal of Advanced research in computer science,2013
3) Zaiba Ishrat *"Security Issues, Challenges and Solution in MANET,"* International Journal of Current Science and Technology, vol. 2, Issue 4, Oct. - Dec. 2011.
4) J. Godwin Ponsam, Dr. R.Srinivasan "*A Survey on MANET Security Challenges, Attacks and its Counter-*

measures," International Journal of Emerging Trends and Technology in Computer Science, vol. 3, Issue 1, Jan.– Feb. 2014.

5) I. Hatware, A. Kathole, M. Bompilwar "*Detection of Misbehaving Nodes in Ad Hoc Routing*," International Journal of Emerging Technology and Advanced Engineering, vol. 2, Feb. 2012.
6) S. Marti, T. J. Giuli, K. Lai, and M. Baker "*Mitigating Routing Misbe-haviour in Mobile Ad Hoc Networks*," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, 2000, pp. 255-265.
7) N. Nasser and Y. Chen "*Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network*," in Proceedings of the IEEE International Conference on Communications, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
8) K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "*An Acknowledgement based approach for the detection of routing misbehavior in MANETs,*" IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007
9) S. Buchegger, J. Y. Le Boudec "*Performance Analysis of the Confidant Protocol (cooperation of nodes: fairness in dynamic ad hoc networks),"* in MobiHoc'02, IEEE/ACM Symposium on Mobile Ad Hoc Networking and Com-puting, 2002.
10) S. Subramaniyan, W. Johnson and K. Subramaniyan "*A Distributed Framework for Detecting Selfish Nodes in MANET using Record- and Trust-Based Detection (RTBD) Technique*," EURASIP Journal on Wireless Communications and Networking, Springer, 2014.
11) Y. Xue and K. Nahrstedt, "*Providing fault-tolerant ad hoc routing service in adversarial environments,"* Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004.
12) P.N. Raj and P.B. Swadas. Dpraodv*: A dyanamic learning system against blackhole attack in aodv based manet*. Arxiv preprint arXiv:0909.2371, 2009.
13) Mistry N, Jinwala DC, IAENG, Zaveri M (2010) *Improving AODV Protocol Against Blackhole Attacks*. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010
14) Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao "*Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach"* IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015.