SELF-ROUTING: A NOVEL APPROACH FOR CONTEXT BASED TRUST EVALUATION AND MALICIOUS NODE DETECTION IN MANET
Akshay Narayan Hegde, Vinay Kumar E, Prof. Vijayan R*
M. Tech IT, SITE, VIT University, Vellore, TN, India.
Assistant Professor (SG), SITE, VIT University, Vellore, TN, India.
Email: rvijayan@vit.ac.in

Received on 22-07-2016
Accepted on 28-08-2016

Abstract
Mobile ad-hoc network is a self-organizing, infrastructure less network in which mobile nodes communicate using wireless channel. In MANET, the network created by the mobile nodes is dynamic in nature i.e. it is not confined to a particular topology because devices are free to move independently. Since there is no centralized node for monitoring in MANET routing path needs to be found dynamically. Each node in MANET has to rely on its neighboring nodes for routing the information. Each node in the network must be trust worthy. Due to its dynamicity MANET is prone to many security attacks. One of the major issues in MANET is identifying malicious node. As malicious nodes can reduce the performance of the network by dropping the packets, providing false route information, being selfish etc. In this regard many techniques are being proposed- self-routing approach aims to find the malicious node in MANET.

Keywords: Mobile ad-hoc network, Security attack, malicious node, Topology.

1. Introduction
Identifying the malicious node in Mobile ad-hoc network is an important area in the field of wireless network security. Still it remained as a challenging task for the engineers to secure MANET. Distributed cooperation and sharing of information among the mobile nodes in MANET, finds the applications mainly when there is no availability of infrastructure based network. Nodes in the mobile ad-hoc networks are free to move independently and configure a network on their own. Due to this inherent features MANET are used for collaborative computing and sensing applications etc.

In many cases MANET are being set up in adverse condition like disaster management, military application, and sensor networks etc. Each node in network routes the information to the intended node by relying the data through the
neighboring nodes, due to this nature of information sharing in MANET each node should trust on other node for sharing the data. Therefore evaluating the behavior and quantifying the nature of the node in mobile ad-hoc network.

This is especially important in large scale networks, in which nodes are of different kind involved in communicating and sharing of the information. Operational differences of the nodes come from the fact of routing decisions, sensing capabilities etc.

Due to the limitations of the resources like battery power, resources for computation etc. the nodes in mobile ad-hoc networks are highly susceptible for exhibiting the malicious behavior in the network for their own advantage, which leads to a significant impact on the performance of the mobile Ad-hoc network. Because of this reason the field of MANET has attracted many scientists which are based on IEEE 802.11 communication technology. The malicious nature exhibited by the node may in the form of dropping the packets which are directed for other nodes for the sake of reducing the consumption of battery life, providing a false routing information for the node which is seeking for the routing information for transferring the data, misleading a node by providing false information about another packet, modifying the data packets which are intended for some other node in the network. MANET consists of dynamic nodes since there is no existence of the centralized or influence of the centralized node on the mobile nodes like in conventional wired network which makes protocols of the conventional networks unsuitable for MANET. In this regard various protocols had been proposed for ad-hoc networks.

This paper provides a detail view of the techniques proposed for detecting the malicious node in the MANET .This paper is organized in to following sections section I deals with Background of malicious node detection, Section II deals with Routing protocols in Ad-hoc networks, section III deals with Security attacks in MANET, Section IV provides details about related work. Section V deals with proposed technique. VI section gives the algorithm of the proposed work.

VII section deals with results and discussion.

1.1 Background of Malicious Node Detection

The MANET is a collection of mobile nodes of different kind. Malicious Node- Mobile node in Mobile ad-hoc network will be referred as a malicious node when the mobile node exhibits a malicious behavior. In general the mobile node in Mobile ad-hoc network exhibits the following behaviors:

- **Normal Behavior**
A mobile node will be said to exhibiting a normal behavior when none of the security principles is violated. i.e. for example when source is delivering a data to the destination during the transmission of the data if the node achieves the security principles like Authenticity, Availability, Integrity, Confidentiality, and Non-Repudiation etc.

- **Malicious Behavior**: When a mobile node fails to provide Confidentiality, Integrity, Availability, Authenticity or Non-Repudiation then it is called as malicious behavior. The malicious node may show any of the following behaviors.

  **Delay**: A malicious node may intentionally delay the packet transfer.

  **Stealing Information**: Malicious node may steal the information that being sent through it.

  **Unavailable**: A malicious node may get isolated whenever there is a route requirement.

  **Tampering**: A malicious node may change the content of the information in the message such that it may completely contradict the original statement.

  **Dropping the packet**: A malicious node may drop the packet that is sent through it.

  **Draining the Battery**: Malicious node may perform unnecessary operations so that battery will get drained out.

  **Buffer Overflow**: A malicious node may fill the buffer with fake packets so that a genuine update will be discarded.

  **Fake routing**: The malicious node forward the false routing information to the path requested node either for the sake of diverging the data packets form it or for receiving the packets for performing some malicious activity.

  **Bandwidth Consumption**: The malicious node unnecessarily floods the packets in the network for preventing the other nodes from sending the data packets.

1.2 Security Attacks

- **On-off attack (OOA)**- A node acts as normally at some point of time and maliciously at some other point of time this kind of behavior exhibited by the node is called as on-off attack. This attack can prohibited by taking the observation frequently and giving more weight to the recent observation than older one. It is also observed that during the trust computation recommendation from many nodes are taken, at least one node will be able to observe malicious behavior.

- **Bad mouthing attack (BMA)**- Bad mouthing attack is one in which a malicious node gives false claims about the other nodes. This happens only when trust is computed based on recommendation from the other nodes. In Most of
the cases this attack is well handled as trust is computed based on multiple observations or recommendation from many nodes.

- **Denial of service attack (DOS)** - A denial-of-service (DoS) attack attempts make a particular node unavailable such that any communication with a particular node is interrupted temporarily or permanently. A malicious node sends huge number of packets to a particular node so that it gets overloaded and useful communication is prevented. A slight variance of DOS attack is **distributed denial-of-service (DDoS)** attack where more than one malicious nodes attack a particular node. It is similar to number of people crowding the bus door preventing the legitmate traveler from boarding the bus.

- **Conflicting behavior attack (CBA)** - In this type of attack a malicious node gives different types of recommendation to different set of nodes. Because of this trust value of a node may be get reduced. Even a genuine node may be get considered as malicious node.

- **Camouflage attack (CA)** - A malicious node goes with the value agreed upon by the majority of the nodes for a long time, until it gains a higher trust value. After gaining the trust it acts maliciously in some occasions specifically. As long as large number of misbehavior is present they can be detected. But misbehavior is too less then, it is hard to detect this kind of attack. It affects recommendation based trust computation. Schemes with centralized trust computation mechanisms can easily detect this kind of attack.

- **Black hole attack or packet drop attack** - A router instead of forwarding the packet it drops them. There may be several reasons for it. For example Dos. This type of attacks is hard to detect.

- **Gray hole attack** - These are slight variation of Black hole attacks but in the case of gray hole attack instead of dropping all the packets only few number of packets are dropped for few amount of time. This kind of attacks is hard to detect.

- **Sybil attack** - In this type of attack large number of fake Ids. These pseudonymous nodes together form a group and conclude the malicious node as a genuine node. This type of attacks can be easily discovered if the trust computation mechanism is centralized. But it badly affects the recommendation or neighbor sensing trust computation mechanisms.
- **Collusion attack** In this type of attack two or more malicious nodes act together and conclude that a normal node to be malicious node. Neighbor sensing trust computation mechanisms can detect the attacks.

- **Newcomer attacks (NCA)** A malicious node gets out of the network and joins again after sometime so that it can have a new trust value or it can perform malicious activity till it get discovered. Once it gets discovered it go out again and same pattern continues. Recommendation methods are capable of detecting this type of attack. Neighbor sensing trust mechanism is the one which is going to get affected more.

- **Replay Attacks** In this type of attack A malicious node captures the control message so that later it can use it. It leads to stale route updating in the routing table of other nodes. Hence the network performance goes down.

2. Related Works

MANET is self-organizing, infrastructure less based network and is no central control in the network. The nodes in the network transfers and receive the data by co-operating and sharing the information. Some of the nodes take the advantage of the vulnerabilities of MANET for their own benefits like dropping the received packets for preventing the battery consumption, providing the false routing information etc. these nodes in the terminology of MANET referred as a malicious node. Various techniques had been proposed for detecting the malicious node in the network.

In this [1] method a query will be flooded to whole network by the query issuing node. Whichever node receives this information, it stores all the routes possible to source i.e. query issuing node. Then the data items will be replied to two neighbors with highest k value by the receiver node. The reply message consists of the actual message and information regarding forwarding route which includes sender node and the id of the next node. Using this information the query issuing node can easily detect attacks. Since In case of MANET, each node is in continuous motion there may be a chance of link breakage. In such scenario the receiver node sends the packet in a new route along which it has not yet sent the data. The malicious node will be narrowed down by the query issuing node using the replies it gets along different paths.

This [2] approach makes use of SOM model contains two Phases – Training and Initiation. It finally progresses towards results along the weight vectors. The allocation of weights, training and detection phases are done according to SOM model. For each input, activation functions are determined by all the neurons. Winners are the ones with low activation code. Model with winner and neurons which are neighbor will adjust their weight so that they can do better in future for the same input. This [3] method makes use of PDA algorithm for the detecting the malicious node in the MANET.
Every node in the network will monitor for packet drop in the network. Once it is detected, a distributed approach is used for investigating the attack. Once the packet dropping node is identified, this method makes use of a trust collector function which collects trust value of that particular node from all the neighbor nodes. If cumulative trust value is low then the node is considered to be a malicious node and a global alarm will be generated about the same. Hence each node will be aware of the malicious node and cluster head will also be informed about the same. The modules involved in this method Cluster head election algorithm-Cluster head is elected using the (CEMCA) algorithm, Monitoring neighbor nodes-Each node passively monitors each and every neighbor for packet dropping, Trust collector function-It collects the trust value of the probable malicious node and Global Alarm-A global alarm is invoked when a malicious node is detected.

![Diagram](image)

**Figure-1. PDA Approach.**

In this [4] method aims at quick and efficient detection of Attack and attacker. This method makes use of HP (Honey Pots). Honey Pots act as traps set up for the purpose of attracting attacker. The ADS main module of the system. It interacts with other modules of the system and enables the smooth operation. Some of the functions of this algorithm are MANET is divided into zones Information collection from the Node Misbehavior Identification procedure and Submitting it to the Honey pot Using Honey Pot Handler. Then locates the attacker with the help of “Attacker Locater Function”. Honey Pot communicates with attacker. It exchanges fake information to the attacker. Hence tries to trap the attacker.
The work is to detect and isolate the malicious node from the routing path by detecting the pollution attack in MANET. The implementation work is divided into Encoding/Decoding of the packets and identifying the malicious node.

- **Encoding and Decoding** - A class of Rate Less codes called Luby Transform code is used to disseminate the data chunks of a node. Pseudo Random number generator is used to encode the packets after splitting the packets generated at source. The number of blocks to be combined is determined based on the packet degree. Chunked data is generated using the XOR operation on packets selected randomly. Packets are transmitted after applying the Error correcting code.

- **Detecting Malicious Node** - The intermediate node decodes the received chunk and Ln denotes the report created by the nodes. This report contains a flag that indicates whether data part has been modified or not and contains a list of node ID and reports are shared among the neighboring node. Belief propagation (BP) algorithm evaluates a node by comparing initialized belief value 0.5 to the generated belief value. If belief value is greater than initialized value then node is trusted node else it is malicious node and node is isolated from the routing path.

In this the malicious node in the network is identified by using the modified AODV protocol. This is achieved by modifying the process model in AODV when the route is being established in the network. During the route establishment phase apart from counting the number of packets forwarded by node i.e. router, number of packets discarded by the node is also considered. Based on the number of discarded packets while establishing the route decision is taken to consider the node or not. The logic behind this technique is when the intermediate node receives a packet the process running in the node decides whether to discard the packet or not based on the parameters like Source address, destination address, sequence number of the packet received. If the received packet contains both Source address and destination address same then the node discard the packet and increments the parameter Number_of_packets_dropped.

While establishing the route only those packets are considered whose Number_of_packets_dropped<Number_of_forwarded_packets*0.20.

Here emphasized to identifying the malicious node in the MANET’s by observing the dropping of the packets by the particular malicious node using the Fuzzy logic.

The implementation is divided into four sections:
• Obtaining the fuzzy based parameters-Each node in the network listens to its neighbouring node and develops a neighbour table. The parameters maintained in table and input to the interference model Average Data Packet Dropped rate, Data Packet Forwarded Rate.

• Input to Interference System -The proposed technique makes use of Mumdani Fuzzy interference system. Based on the parameters received in the previous step verity level of the each node is calculated.

In decision step the calculated verity level in the previous step is compared with threshold of verity level results are passed to response module.

In response step If the verity level of a particular node is greater than the threshold the node is declared as malicious node and module alarms the IP address of the node and separates the node from the rest of the network.

Data Packet Forwarded Rate=no. of data packet forwarded/no. of data packet received

Average Data Packet Dropped rate=Number of data packet received by the node/Number of data packet Forwarded by the node

3. Proposed Work

The proposed should meet the following requirements:

- The system should effectively determine the entering node is malicious or not.
- The system should overcome the denial of service attacks.
- The system should not consume more network resources like Bandwidth, processing power etc.
- The system should not degrade the performance of the network.
- The system should provide the functionality by making use of the existing resources.

2.1 Selection of Master and slave nodes

Any two trusted nodes are selected as master and slave nodes based on any of the cluster head selection algorithms. But it must be taken care that both the nodes are in one hop distance from the new arrived node.

![Figure-2: Selection of master and slave.](image)
2.2 Generation of checker Packet

Checker packets are special kind of packets which contains data which ends with a particular kind of pattern. These packets will have slave node as the destination address.

![Source Address | Destination Address | 100010101111](image)

**Figure-3: Generation of checker packet.**

2.3 Forwarding and verification at slave node

The checker packet will be forwarded to new node. On receiving the packet if it is malicious node it will perform some sort of malicious activity on it. It may

- It may change the entire message
- It may change only few bits leaving the ending pattern as it is.
- May not forward the data right away.

When the slave node receives the packet it checks for the pattern. If found it forwards the data to master else it doesn’t.

2.4 Verification at the master node

The data is received in predefined time and if it matches with the originally sent data then the new node can be trusted. Since the master node itself verifies the packet it overcomes much kind of attacks. The Proposed algorithm involves master node, slave node, newly entering node and a checker packet. The algorithm performs extensive comparison operations for verifying data pattern and hence concludes whether the newly entering node is malicious or not.

1. Master node and a slave node are selected using any of the already available standard algorithms.
2. Master node generates the checker packet.
3. Master node assigns slave nodes address as destination address.
4. Master node forwards packet to newly arriving node and starts a timer.
5. New node forwards packet to slave node with or without changes.
6. If Specified pattern is found by Slave
   Forward the packet to master node.
7. Else
   Don’t forward the packet to master node.
8. End of if
i. If master node receives data in time
j. Verify data with original one
   i. If match is found
      New node is not a malicious node
   ii. Else
      New node is a malicious node
k. End of if
l. Else
   i. New node is a malicious node
m. End of if

4. Results and discussions

Following table summarizes the some of the attacks overcome by the self-routing approach.

<table>
<thead>
<tr>
<th>SL. No</th>
<th>Attacks</th>
<th>How the proposed technique overcomes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Black hole attack</td>
<td>Self-routing approach overcomes this attack by making use of a timer.</td>
</tr>
<tr>
<td>2</td>
<td>Grey hole attack</td>
<td>Self-routing approach overcomes this attack by transmitting the control packet more than once.</td>
</tr>
<tr>
<td>3</td>
<td>Collusion Attack</td>
<td>In self-routing approach cluster head verify whether node is malicious or not.</td>
</tr>
<tr>
<td>4</td>
<td>Replay Attack</td>
<td>Self-routing approach overcomes this attack by making use of a timer.</td>
</tr>
<tr>
<td>5</td>
<td>Conflicting behaviour</td>
<td>Self-routing approach overcomes this attack by transmitting the control packet more than once.</td>
</tr>
</tbody>
</table>

5. Conclusion

This approach provides a technique for detecting whether newly arrived node is malicious node or not it overcomes the some of the draw backs of the existing techniques for detecting the malicious node in terms of resource consumption like bandwidth, storage, processing power. In this technique network is split in two number of clusters where in each cluster the nodes are coordinated by the cluster head. Cluster head makes use of a control packet which is routed towards the newly arrived node for detecting its malicious behavior like modification of data or dropping of data packets. This technique can also be used for finding the malicious behavior of already existing node in the cluster.

References

2. V. Dinesh Kumar, Dr. S. Radhakrishnan, “Intrusion Detection in MANET using Self Organizing Map (SOM),” International Conference on Recent Trends in Information Technology, pp 1-8, April 2014.


Corresponding Author:
Prof. Vijayan R*,
Email: rvijayan@vit.ac.in