Trusted Load Balancing Mechanism for MANET

Bittu Ann Mathew
PG Scholar
Amal Jyothi College
Kottayam
Kerala, India

Sneha Sebastian
PG Scholar
Amal Jyothi College
Kottayam
Kerala, India

Varsha Sabu
PG Scholar
Amal Jyothi College
Kottayam
Kerala, India

Sumy Joseph
PG Scholar
Amal Jyothi College
Kottayam
Kerala, India

ABSTRACT
A mobile ad hoc network (MANET) is a self-configuring, infrastructure less network of wireless mobile devices. Malicious nodes are those nodes that create attacks like denial of service attacks, impersonation attacks, etc. Due to increase in communication in the network, overloading of nodes may happen. MANET is also vulnerable to node overloading due to malicious nodes. In this paper, an efficient load balancing mechanism has been proposed. This method has been designed using Trust Based Malicious Node Detection (TMND). Here load balancing is performed by rejecting the malicious nodes below a certain trust cutoff value. The system has been analyzed by calculation of throughput, delay and load.

General Terms
Adhoc network security

Keywords
Trust, Load Balancing, Malicious Node

1. INTRODUCTION
A MANET [1] is a type of ad hoc network that can change locations and configure itself on the fly. It has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

Node overloading is one of the major issues in MANET. So there is a need for some load balancing mechanism to be present in the network. The load should be efficiently distributed through the network. Otherwise, heavily-loaded nodes may make up a bottleneck that lowers the network performances by congestion, packet loss, degradation in throughput and larger delays.

There are a lot of security issues in MANET [2]. The two types of security attacks are passive attacks and active attacks. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. The malicious nodes may cause denial of service attacks, impersonation, etc. This may lead to node overloading.

In this paper, a load balancing mechanism has been proposed which uses Trust Based Malicious Node Detection (TMND). The remaining of the paper is organized as follows. Section II contains some related work, section III explains the proposed load balancing mechanism, section IV deals with analysis and section V deals with the conclusion.

2. RELATED WORK
Routing protocols [3] can be used to provide load balancing. Proactive and reactive routing protocols can be used for this. These take into account nodes degree of centrality. These mechanisms improve the load distribution and significantly enhance the network performances in terms of average delay and reliability.

Another method for load balancing is the cell breathing technique [4]. In this, the load of congested nodes is reduced by reducing the transmission power of the congested node. This forces the nodes near the congested cells boundaries to shift to less congested nodes.

In Best SNR heuristic method [5], a node is associated with a node from which it receives highest power. When the load on a node increases, the power received from it is low. So, only lightly loaded nodes are used for communication. In this way, load balancing is performed. However, none of these methods can find the malicious nodes that may have caused the node overloading.

3. PROPOSED APPROACH
In the proposed method, first a trust value for each node is computed using Trust Based Malicious Node Detection (TMND) method. Then based on the trust value, the nodes are identified as either malicious or trusted nodes. The requests from malicious nodes are discarded. In this way, the loads due to the malicious nodes are eliminated. The proposed method consists of two phases.

3.1 Trust Based Malicious Node Detection (TMND)
The trust value of a node can be computed in two ways- direct and indirect.

3.1.1 Direct Trust
Direct trust calculation comes under direct observation of neighbors. In this, every node in the network monitors the behavior of its neighbors and determines direct trust value. Direct trust value is computed as follows:

If a node x want to calculate the trust value on node y, then

Direct trust value of X and Y = Successful packet sent from the node X / Successful packet received from the node Y.

3.1.2 Indirect Trust
The task of indirect trust monitor is to collect or request the trust related information of target node from the neighboring nodes. While requesting the trust information of the target node from neighbors, the direct trust value of that neighbor node should be considered.

To obtain indirect trust on node Y from node N through any intermediate node(s) X.

Step 1: Node N sends REQ to node(s) X.

Step 2: If node X has direct trust value on Y, then it will reply back with REP.

Step 3: Else If X does not have direct trust value, it will forward the REQ to its neighbors.

Step 4: The node which has the direct trust value of Y, will send REP back to N through all intermediate nodes.

3.2 Load Balancing

Node overloading may be caused by malicious nodes and sometimes by trusted nodes.

3.2.1 Malicious nodes

Malicious nodes may cause node overloading by repeatedly sending unnecessary request messages. This may lead to denial of service attacks. So there is a need to identify malicious nodes and perform load balancing. After calculating the trust value, the proposed load balancing is performed. If a route request message comes from a node, the trust value of that node is checked. If the trust value is below a cutoff, then

the node is identified as malicious and the request from this node is discarded. In this way, any node overloading that may have been caused by the malicious node can be avoided.

3.2.2 Trusted nodes

Sometimes trusted nodes in the network may also cause overloading due to heavy traffic. If the number of requests received by a node exceeds its capacity, then it becomes overloaded. So load balancing has to be performed. When a route request comes from a node, its trust value is checked. If the trust value is above the cutoff, then the node is identified as trusted node and the route request is accepted. If node overloading is caused by trusted nodes, then load balancing is performed by finding the next shortest path.

4. ANALYSIS

Some of the existing loads balancing methods are routing protocols, cell breathing technique, Best SNR heuristic method.

4.1 Routing protocols

In this, the malicious nodes may also be included in the routing. Thus, the load is not balanced efficiently. The proposed method can efficiently perform load balancing by identifying malicious nodes.

4.2 Cell breathing Technique

In this, the load of congested nodes is reduced by reducing the transmission power of the congested node. This forces the nodes near the congested cells boundaries to shift to less congested nodes. This may cause malicious nodes to be included in the communication which may lead to further overloading. In the proposed method, malicious nodes are identified before communication begins and thus the problem of cell breathing technique can be overcome.

4.3 Best SNR heuristic method

In this, a node is associated with a node from which it receives highest power. So there is a possibility for communication with malicious nodes that have high power. This problem can be overcome in the proposed method.

5. CONCLUSION

Malicious nodes are those nodes that create attacks like denial of service attacks, impersonation attacks, etc. Due to increase in communication in the network, overloading of nodes may happen. MANET is also vulnerable to node overloading due to malicious nodes. In this paper, an efficient load balancing mechanism has been proposed. This method has been designed using Trust Based Malicious Node Detection (TMND). Here load balancing is performed by rejecting the malicious nodes below a certain trust cutoff value.

6. REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Application and Challenges”.

[2] Pradeep Rai, Shubha Singh“A Review of MANETs Security Aspects and Challenges”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010

[3] Oussama Souihli, Mounir Frikha, “Load-balancing in MANET shortestpath routing protocols”,Sciencedirect,March 2009

[4] Y. Bejerano and S. J. Han, “Cell breathing techniques for load balancing in wireless LANs”, IEEE Trans. Mobile Comput., vol. 8, no. 6, pp. 735749, June 2009.

[5] S. Corroy, L. Falconetti, and R. Mathar, “Dynamic cell association for downlink sum rate maximization in multi-cell heterogeneous networks”, in Proc. 2012 IEEE Intl. Conf. Commun., to be published after Apr.2012.