Journal of Computer Engineering and Information Technology

Perspective

A SCITECHNOL JOURNAL

Survey of Routing Protocols for Mobile Ad hoc Networks

Manish Kumar*

Department of Computer Engineering, University of Freiburg, Freiburg, Breisgau, Germany

***Corresponding author:** Manish Kumar, Department of Computer Engineering, University of Freiburg, Freiburg, Breisgau, Germany. E-mail: kumar28@gmail.com

Received date: 06 June, 2022, Manuscript No. JCEIT-22-61673;

Editor assigned date: 08 June, 2022, PreQC No. JCEIT-22-61673(PQ);

Reviewed date: 15 June, 2022, QC No JCEIT-22-61673;

Revised date: 13 July, 2022, Manuscript No. JCEIT-22-61673(R);

Published date: 27 July, 2022, DOI:10.4172/jceit.1000238.

Description

We represent a survey of various existing secure routing protocols for MANET's. A mobile ad hoc network is a self-configuring mobile nodes network. Significant progress has been made for making mobile ad hoc network secure and dynamic. Its infrastructure less and absence of any centralized authority makes these networks more vulnerable to security attacks. Due to these security threats, there is need for development of algorithm and protocols for a secured ad hoc network. In this paper a comparative study of different routing protocols is discussed as Ad Hoc on Demand Distance Vector routing (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) security threats within MANET network. MANET‟s, Denial of Services; DSR; AODV; TORA. In wireless ad hoc network there is no pre-deployed infrastructure for routing packets end to end and instead of this there are mobile nodes communicating via radio links that can temporarily form a network. The topology is highly dynamic and the nodes have a limited transmission range, so each node needs the assistance of its neighboring node for packet forwarding. The information is exchanged and updated dynamically from time to time. But on demand routing protocol instead of generating periodical updates, find the route to the destination node only when the source node have a data packet to be sent to the destination node. Therefore security in ad hoc is a challenge for basic network operations like packet forwarding and routing .In this paper we expose various security threats and find the way to route packet securely. This paper deals with various issues that lack in mobile ad hoc network and then with various protocols associated with routing in MANET‟s.

Network Medium

MANET‟s does not have fixed infrastructure therefore all the network details are obtained on fly and so are susceptible to the wireless network attacks. In mobile ad hoc network nodes are free to join, move and leave the network according to their need in the wired network, nodes must get physical access to the network medium, or even pass through several firewall. And gateway before their behavior becomes malicious to the targets. However, in MANET‟s, there is no need for physical access to visit the network once the node is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes. As a result MANET‟s does not provide secure boundaries. Because of the mobility of the ad hoc network, a compromised node cannot be easily determined, that node frequently change its attack target and perform malicious behavior in the network, thus it is very difficult to track the malicious behavior performed by a compromised node. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised. It is not easy to monitor traffic in a highly dynamic network because of absence of any centralized monitoring. Therefore failures like packet dropping, path breakage are common. These malicious failures are more difficult to detect, especially when topology changes frequently and their attack target also changes in different periods of time. However, we can easily find from a system point of view that the node has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this node should be malicious failure, though these failures occur in different nodes at different time.

Proactive Protocols

Mobile ad hoc network mainly work on battery power, sometime the nodes become selfish as they have limited battery power due to this selfishness some problems are caused, when there is a need for this node to cooperate with other nodes to support some functions in the network. As an example consider a cluster based intrusion detection technique. In this, there is no need that every node in the ad hoc network is the monitoring node all the time; instead, a cluster of neighboring MANET nodes can randomly elect a monitoring node that will observe the abnormal behaviors in the network traffic for the entire cluster. However, an important precondition for the success of this technique is that every node in the cluster is willing to take their responsibility as a monitoring node and serve for all other nodes in a period of time. There may be some nodes that behave selfishly and do not want to cooperate in the monitoring node election process, which will make the election fail if there are too many selfish nodes. In a traditional wired network no of node connected does not change frequently so its scale is generally predefined but in ad hoc network nodes are mobile numbers of nodes connected in network changes frequently so its scale keeps on changing frequently. As a results its protocols and services such as key management, routing protocols should be compatible to this change. Routing is a term that defines the route from source node to destination node. Routing in MANETs is more difficult than routing in wired networks. In MANETs there are two types of routing. Table-driven ad hoc routing protocols maintain the routing information of each and every node connected to all other nodes in the network. Also known as proactive, these protocols allow every node to have a clear and consistent view of the network topology by transmitting updating messages periodically. Another approach is the source-initiated on-demand routing. According to this approach, a route is created only when the source code requires a route to a specific destination. A route is obtained by initiating the route discovery procedure by the source node. While route discovery, the data packets transmitted are buffered and are sent when the path is established. An established route is maintained as long as it is required through a route maintenance procedure. There is no routing protocol which is perfect for all kinds of MANETs. Each routing protocol has its own strengths in some specific networking environments, but mobile nodes should be able to operate in every environment. A challenge is how to achieve security in routing as high as possible when it crosses over different environments.

Dynamic source routing belongs to the class of reactive routing protocols which is based on the theory of source based routing rather than table-based. This protocol is source-initiated rather than hop-by-hop. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. It allows a node to dynamically discover a route having multiple hops to any destination. Each packet in its header carries a complete ordered list of nodes through which the packet must pass. When a node wants to send a packet to a destination, it checks the source route to the destination in its cache. If no route is found in its cache, it requests a route by broadcasting Route request Packet (RREQ) broadcast. This packet includes the destination address, the source address and an identification number. Each node receiving the RREQ looks for the destination in its cache. Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. In wireless networks acknowledgments are often provided. An existing standard part of the MAC protocol in use, such as the link layer acknowledgment frame. Its first advantage is the small overload in terms of packets to obtain routes, since DSR only manages the routes between nodes who want to communicate. Besides, DSR uses caching and that can reduce the load of future route discovery. Another advantage is that only one RREQ process can produce some routes to the destination, thanks to the responses of the caches of intermediate nodes.