ISSN (online): 2250-141X
Vol. 2 Issue 4, September 2012

A Review on Security issues in Routing of a Mobile Ad Hoc networks – A Survey Paper

J RAJESHWAR[1]
Research Scholar, Department of Computer Science and Engineering
JNTUH College of Engineering
JNTUH, Kukatpally, Hyderabad A.P, INDIA.

Dr G NARSIMHA[2]
Assistant Professor, Department of Information Technology
JNTUH College of Engineering,
Kondagattu, Jagityal, Karim Nagar, A.P, INDIA,

ABSTRACT

Mobile Ad Hoc Networks (MANET) are new design of wireless communication for mobile nodes which has computation capability. Now a day's MANET has gained a lot of attention due its flexibility in forming a network with less infrastructure requirement and speed of configuration. Due to mobility of the nodes which join and leave the network as and when they require the MANET is prone to insecure. Due to vulnerability of MANET security has became the major concern. It should provide security from external attacks as well as internal attacks, from these routing attacks gained a lot of attention as routing is very complex aspect of data delivery. In this paper we try to explore basics of routing and attack on routing and suggest some possible solutions.

Keywords: MANET, basics of routing, routing attacks.

1. INTRODUCTION:

A self configured moving nodes forming as a group to communicate each other is called as Mobile Ad Hoc Networks (MANET). The nodes can join and leave the MANET whenever they want; it has got no fixed infrastructure, due to this mobility factor MANET's more prone to attack from various kind. The MANET has to make a secure communications in this environment out of which routing is the very basic functionality,

Routing is used for sending data from one point to other by choosing the most appropriate path. As we know that in a network many paths exist for one destination and data can be send by choosing any path. It follows certain criteria for selecting a path and delivering data in a secure way. As there exist many paths to transport the data in a most vulnerable environment security for routing is playing a very important role.

The paper is organized in the following way chapter 1 tells about the importance of routing, chapter 2 tells about attacks on routing, chapter 3 tells security for routing chapter 4 with conclusion.

2. BASICS OF ROUTING AND ATTACKS

The topic of routing has been covered in computer science literature for more than two decades, but routing achieved commercial popularity as late as the mid-1980s. The primary reason for this time lag is that networks in the 1970s were fairly simple, homogeneous environments. Now a day's large-scale internetworking with heterogeneous environment has become popular, that's where routing task became complex.

ISSN (online): 2250-141X
Vol. 2 Issue 4, September 2012

Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as switching. Although switching is relatively straightforward, path determination can be very complex to perform well in most circumstances. Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. The routing metrics have been used are Path Length, Reliability, Delay, Bandwidth, Load and Communication Cost

Routing in MANET [1] consists of two phases: one is Route Discovery and Route Maintenance. Route discovery is the mechanism by which a node intending to send a packet to destination obtains a route. Route maintenance is the mechanism by which a node is able to detect while using route to destination that one or more links along the route have failed, when broken link is discovered the source can use another route or can revoke Route Discovery.

There are several attacks which MANET has to face they are mainly on the basic mechanisms of MANET such as [1] routing, security and key management. **These attacks can be can be classified as two types** [2]:

(i). External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

(ii). Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions. However, due to the pervasive communication nature and open network media in the mobile ad hoc network,[3][4] internal attacks are far more dangerous than the external attacks because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when

ISSN (online): 2250-141X
Vol. 2 Issue 4, September 2012

we consider the security issues in the mobile ad hoc networks.

The main attack types that emerge in the mobile ad hoc networks are Denial of Service (Dos), Impersonation, and Eavesdropping

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, **attacks against routing are generally classified into two categories:**

(i). attacks on routing protocols

(ii).attacks on packet forwarding/delivery [2].

The first category of attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack [2]. There are some attacks against routing that have been studied and well known [5] [6] [7] [8]:

(a).Impersonating another node to spoof route message.

(b).Advertising a false route metric to misrepresent the topology.

(c).Sending a route message with wrong sequence number to suppress other legitimate route messages.

(d).Flooding Route Discover excessively as a DoS attack.

(e). Modifying a Route Reply message to inject a false route.

(f). Generating bogus Route Error to disrupt a working route.

(g). Suppressing Route Error to mislead others.

Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages [2]. There are some more sophisticated routing attacks, which include Wormhole attacks [9], Rushing attacks [10] and Sybil attacks [11].

The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented [2]. There are two main attack strategies in this type one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save its own battery power, the other is denial-of-service, in which the adversary sends out overwhelming network traffic to the victim to exhaust its battery power.

3. SECURITY FOR ROUTING

There are so many solutions have been proposed by researchers depending upon type of the attack. Specifically In order to meet with security challenges of routing in MANET malicious and compromised node must be identified or at least their behavior must be traced in order to have a secure routing

The possible solution are admission control [12], it refers to decision process that is performed prior to the incorporation of the devices to the MANET. A node that wishes to use network for transporting data must make a request to cluster head informing its characteristics if the cluster head detects is to be genuine then it gives the connection else the nodes requests will be discarded.

Per-node based intrusion detection technique [13] inspects each node's behavior and exchanges the results with other nodes if malicious node behavior is found it is discarded.

There is also cluster-based intrusion detection technique by in which few node forms clusters and they elect cluster head

ISSN (online): 2250-141X
Vol. 2 Issue 4, September 2012

and cluster head will be held responsible for detection of malicious behavior. From the comparative study we can find that the CPU speedup is increased for the cluster-based IDS method than the per-node based IDS method, at the same time the network overhead for the cluster-based IDS methods is lower than that for the per-node based IDS method. However, the detection rate of the cluster-based IDS method is slightly lower than that of the per-node IDS method, which may be reasonable because from a whole cluster point of view, there will only be one node that monitor the traffic for the whole cluster, which can make some inaccurate judgments because of the limited processing power of just one node.

There is the cross-layer analysis method presented by Parker et al. [14]. in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account.

Next we briefly introduce the concept of community based security, in the secure ad hoc routing. The concept of community based security is based on the observation that wireless packet forwarding typically relies on more than one immediate neighbor to relay packets. Community-based security explores node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is seamlessly converted to a new per-community based forwarding scheme. Since a community based security is functional as long as there is at least one cooperative "good" node in the community, there is no requirement that how many nodes in the community should be available to provide reliable packet forwarding services.

4. CONCLUSION.

In this survey paper we tried to introduce the MANET, We have briefly explained the basics routing and its importance in the network. Then we have briefed about the type of attacks and specially the attacks on the routing and finally we have discussed few method of providing security to the routing. We have to further explore deep into the various method of providing security while transporting the data.

REFERENCES:

[1] Jean-Pierre Hubaux,Levente Buttyyan, Srdan Capkun, The Quest for Security in Mobile Ad-hoc Networks

[2] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9),* Springer, 2005.

[3] The Terminodes project www.terminodes.org

[4] S.marti. T.Giuli, K. Lai, and M.Baker, Mitigating routing misbehavior in mobile ad-hoc networks.in proc. Of MOBICOM, 2000

[5] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS),* San Antonio, TX, January 2002.

[6] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in *Proceedings of ACM MOBICOM'02,* 2002.

[7] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in *Proceedings of ICNP'02,* 2002.

[8] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc

ISSN (online): 2250-141X
Vol. 2 Issue 4, September 2012

Networks, *Ad Hoc Networks*, 1 (1): 175–192, July 2003.
[9] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in *Proceedings of IEEE INFOCOM'03*, 2003.
[10] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in *Proceedings of ACM MobiCom Workshop - WiSe'03,*2003.
[11] J. R. Douceur, The Sybil Attack, in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02),* pages 251–260, March 2002, LNCS 2429.
[12] Puneet Kumar, A.K Vasta " Secure and Priority Based Routing Mechnism in MANET through Mobile Agent", Journal of computing Vol.3 Issue 3 March 2011, ISSN 0320-1113
[13] Wenjia Li and Anupam Joshi- "Security Issues in Mobile Ad Hoc Networks - A Survey"
[14] Jim Parker, Anand Patwardhan, and Anupam Joshi, Detecting Wireless Misbehavior through Cross-layer Analysis, in *Proceedings of the IEEE Consumer Communications and conference on Mobile*