International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Survey of Defending Schemes against Attacks in MANET

Ashwini Magardey*, Pratyoosh Rai, Tripti Arjariya*****

[*] *M. Tech Scholar, Department of Computer Science, Bhabha Engineering Research Institute, RGPV, Bhopal. **HOD & Guide, Deptt. of Computer Science & Engineering, Bhabha Engineering Research Institute, Bhopal. ***Professor, Deptt. of Computer Science & Engineering, Bhabha Engineering Research Institute, Bhopal.*

ABSTRACT

This Mobile Ad hoc Network is a self organized network. No monitoring system is used in such kinds of network so that security is the one of the major problem in Mobile Ad hoc Network (MANET). Due to unique characteristics of MANET, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a security scheme that achieves both extensive protection and desirable network performance from jamming attack. The multipath routing are solve the problem of jamming but in case of jamming attack multipath routing are also prevent from attack. In this work we study and analyze the effect of jamming attack which is the behaviour of attacks in ad hoc networks. By applying different security concept, we expect the malicious node can divest the traffic from the source node. In mobile ad hoc networks where the network topology animatedly changes, straight methods cannot be used efficiently. In this paper we study the already proposed methods to detect and healing of routing misbehaviour of different attacks attack in Mobile Ad-Hoc Network and identified the schemes are proving the better results in case in presence of attack and also gives the ides about to proposed a new scheme in future against jamming attack.

Keywords: - *Routing, attack, Security, MANET, Multipath*

I. INTRODUCTION

This consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. On the contrary to traditional wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals [1].

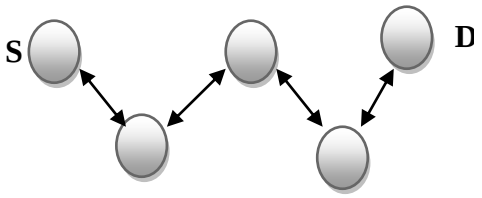

Fig. 1 Mobile Ad hoc Network

In the MANET shown in figure 1 nodes move randomly so the network may experience rapid and random topology changes. In addition, because nodes in the MANET generally have concise transmission ranges, some nodes do not able to communicate face to face with others nodes. Hence, routing paths in MANETs potentially contain various multiple hops, and each and every node has the liability to act as a router.

Mobile ad-hoc networks are inclined to a large number of security threats. The basic reality that mobile ad-hoc networks lack permanent infrastructure and use wireless link for interaction makes them very predisposed to an adversary's spiteful attacks. Attackers are severe security threats in ad-hoc networks which can be employed with no trouble by exploiting susceptibility of on-demand routing protocols such as AODV. This try to use Intrusion Detection (ID) to prevent attacks imposed by both single and multiple nodes and the Detection and healing routing misbehaviour under MANET. we try to reach up to the specific solution maximizes network performance by the help of minimizing production of control (routing) packets as well as successfully opposing attacks against mobile ad-hoc networks [1].

The rest of the paper is summed as that the Multipath Routing is described in section 2 and Section 3 has discussed in detail Types of Attacks. The section 4 has illustrated the Literature Survey and Section 5 Conclusion is enclosing this paper.

II. MULTIPATH ROUTING

Mobile ad hoc networks are characterized by a dynamic topology, limited channel bandwidth and limited power at the nodes. Because of these characteristics, paths connecting source nodes with destinations may be very unstable and go down at any time, making communication over ad hoc networks difficult. On the other hand, since all nodes in an ad hoc network can be connected dynamically in an arbitrary manner, it is usually possible to establish more than one path between a source and a destination. When this property of ad hoc networks is used in the routing process, we speak of multipath routing [11].

In most cases, the ability of creating multiple routes from a source to a destination is used to provide a backup route. When the primary route fails to deliver the packets in some way, the backup is used. This provides a better fault tolerance in the sense of faster and efficient recovery from route failures.

Multiple paths can also provide load balancing and route failure protection by distributing traffic among a set of disjoint paths.

Paths can be disjoint in two ways: (a) link-disjoint and (b) node-disjoint. Node-disjoint paths do not have any nodes in common, except the source and destination, hence the do not have any links in common. Link-disjoint paths, in contrast, do not have any links in common.

III. ATTACK TYPES IN MOBILE AD HOC NETWORKS

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types [15]:

A. External attacks,

In External attacks the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

B. Internal attacks,

Internal attack 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, internal attacks are far more dangerous than the internal 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 we consider the security issues in the mobile ad hoc networks. In the following, we discuss the main attack types that emerge in the mobile ad hoc networks.

1) Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the practice, the attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

2) Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network [16]. As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to

conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access

4) Attacks against Routing

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: attacks on routing protocols and attacks on packet forwarding/delivery [15]. 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.

5) Black hole Attack

A black hole attack is a type of routing attack in which malicious node advertise itself as having shortest path to destination in a network by sending fake route reply to the source node. Then it can dropping the received data packets. The malicious node can deprive the traffic from the source node [3]. Black hole attack is access by a malevolent node which makes all the traffic travel through it by guarantee to claiming to have the shortest route to all different nodes in the network. After that, in place of forwarding the packets, malevolent node simply leaves it. In a black hole attack, a malicious node impersonates a destination node by sending a spoofed root react packet to a source node that initiates a route invention. The source node traffic can be deprived by malicious node. A deviation of black hole is the gray-hole attack, which is generally selectively grant some packets and drops other packets. Other attacks towards an ad-hoc network include partitioning and replay attacks.

6) *Flooding Attack*

Flooding attack [13] is a denial of service type of attack in which the malicious node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network.

The flooding attack is possible in all most all the on demand routing, depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

a) RREQ Flooding

In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to the IP address which does not exist in the network and disable the limited flooding feature. On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In the route discovery the source node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher than data packet then at the high load also RREQ packet are transmitted. A malicious node exploits this feature of on demand routing to launch the RREQ flooding attack.

b) Data Flooding (Jamming)

In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication.

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack [15]. There are some attacks against routing that have been studied and well known [17]:

- ✓ Impersonating another node to spoof route message.
- ✓ Advertising a false route metric to misrepresent the topology.
- ✓ Sending a route message with wrong sequence number to suppress other legitimate route messages.

- ✓ Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages.

IV. LITERATURE SURVEY

Let's look out various researches already done by various researchers.

In this research [4] author focus on identified the vulnerabilities of routing protocols that fail to provide reliable routing and thus cause drastic degradation of data delivery performance under jamming. Pulse jamming that allows intermittent success in data delivery to jammed nodes is more efficient than constant jamming. Effective and efficient jamming attack can be executed through a careful selection of jamming rate based on routing protocol operations.

In this paper [5] we proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. We developed a probability model utilizing stochastic Petri nets techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. We demonstrated the feasibility of dynamic hierarchical trust management and application-level trust optimization design concepts with trust based geographic routing and trust-based IDS applications, by identifying the best way to form trust as well as use trust out of individual social and QoS trust properties at runtime to optimize application performance. Here trust-based IDS algorithm outperforms traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives.

The authors [6], discuss the different types of security attacks that can be launched easily in MANETs and related solutions needed for ensuring network security. This paper implements the secure ad hoc on-demand distance vector routing protocol (SAODV) and compares the performance of protocol with existing AODV protocol in the presence of black hole attack. Since public key cryptography is used in this scheme, it takes significant amount of time to compute digital signature at each node. Also, this leads to high overhead and processing power requirements.

In this paper author proposed FACES (Friend-Based Ad-hoc Routing using Challenges to Establish Security) [7], that provides a list of trusted nodes to the source node by sending challenges and sharing friend lists. Based on the extent of successful data transmission and

the friendship with other nodes in a network, the nodes in the friend lists are rated. The trust level of each node varies from -1 to 4. The nodes in the network are placed in one of the three lists, i.e. question Mark list, friend list and unauthenticated list. The periodic flooding of challenge packet and sharing of friend lists increases the control overhead.

In this paper [8] author proposed per-IP traffic behavioral analysis, in this they present a real-time DDoS attack detection and prevention system which can be deployed at the leaf router to monitor and detect DDoS attacks. The advantages of this system lie in its statelessness and low computation overhead, which makes the system itself immune to flooding attacks. Based on the synchronization of TCP and UDP protocol behavior, this system periodically samples every single IP user's sending and receiving traffic and judges whether its traffic behavior meets the synchronization or not. A new nonparametric CUSUM algorithm is applied to detect SYN flooding attacks. Moreover, this system can recognize attackers, victims and normal users, and filter or forward IP packets by means of a quick identification technique. It has three advantages shown as follows.

1. Based on per-IP traffic behavior analyses, it is easier to differentiate the attackers from the normal users.
2. Because our approach needs less computation and memory, the system could be deployed for on-line DDoS detection and prevention.
3. By applying the non-parameter CUSUM algorithm and decision algorithm, this system can detect attacks accurately at the earlier attack stage.

Moreover, this system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology.

In this [9] research, rejection of Service attack is applied in the network, evidences are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to find out the accuracy of detection engine by using support vector machine. Universal Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes similar to routing, and deciding the cluster head for scalable ad-hoc networks. Aspect takes out for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols..

In this approach [10] a message security approach in MANETs that uses a trust based multipath AOMDV routing combined with soft encryption, yielding our so-called T-AOMDV method. Replication results using ns2 exhibit that our scheme is much more secured than traditional multipath routing algorithms and a recently proposed message security scheme for MANETs. The performance criteria used are route selection time and trust compromise. This requirement poses a security challenge when malevolent nodes are present in the network. Indeed, the existence of such nodes may not simply disrupt the normal network operations, but cause serious message security issue concerns, from data availability, privacy, and/or integrity viewpoints.

In this paper [11], the current security issues in MANET are investigated. Universally, we have examined different routing attacks, like flooding, black hole, link spoofing, wormhole, and colluding miserly attacks, as well as existing solutions to protect MANET protocols. A MANET is a promising network technology which is based on a self organized and rapidly deployed network. Due to its excellent features, MANET attracts different real world application areas where the networks topology changes very rapidly. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks issues. In this paper author discussed present routing attacks and countermeasures against MANET protocols.

The goal of this [12] research is to investigate the efficiency of different classical clustering algorithms in clustering network traffic data for unsupervised anomaly detection. The clusters obtained by clustering the network traffic data set are intended to be used by a security expert for manual labeling. A second goal has been to study some possible ways of combining these algorithms in order to improve their performance. Due to the unique distinctiveness of MANET, mounting an intrusion detection system (IDS) in this network is demanding. An efficient and simple approach for defending the AODV protocol against Black Hole attacks is planned. This method can be used to find the secured routes and prevent the black hole nodes in the MANET by indentifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? Normally the first route respond will be from the malicious node with high destination sequence number, which is kept as the start entry in the RR-Table. Then measure up to the first target sequence number with the source

node sequence number, if there exists extreme differences among them, definitely that node is the malicious node, instantly take out that entry from the RR-Table. In addition, the proposed approached may be used to maintain the identity of the malicious node as MN-Id, Therefore that in future, it can be deny any control messages coming from that node. Now since malevolent node is recognized, the routing table and the control messages from the malevolent node, too, are not forwarded in the network.

In this paper [18] we consider a particular class of DoS attacks called Jamming. In fact, the mobile hosts in mobile ad hoc networks share a wireless medium. Thus, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications.

V. CONCLUSION

In this paper we surveyed the main security issues in MANET. Firstly we have presented specific Multipath routing to solve the possibility of normal jamming conditions. Then we have surveyed the attacks exploit these vulnerabilities and, possible proactive and reactive solutions proposed in the literature. Attacks are classified into passive and active attacks at the top level. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks and also been discussed and examined under insider and outsider attackers. Insider attacks are examined on our exemplar routing protocol AODV. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. In this paper we summarize secure routing approaches proposed for MANET. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic and the flooding of control and data packets cause the jamming condition that consumes the bandwidth of network. Then in future we try to propose security solutions well-suited to MANET environment against jamming attack, we recommend researchers investigate possible security risks to MANET most thoroughly.

REFERENCES

I. S.Madhavi, "An Intrusion Detection System In Mobile Adhoc Networks", International Journal of Security and Its Applications Vol. 2, No.3, pp. 1-16, July, 2008

II. Sunilkumar S. Manvi, Lokesh B. Bhajantri, and Vittalkumar K. Vagga, "Routing Misbehavior Detection in MANETs Using 2ACK" , journal of telecommunication and information technology (JTIT), pp. 105-111, 2010.

III. Subash Chandra Mandhata , Surya Narayan Patro "A counter measure to Black hole attack on AODV based Mobile Ad-Hoc Networks", International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, pp. 37 – 42, 2011.

IV. Jae-Joon Lee And Jaesung Lim, " Effective And Efficient Jamming Based On Routing In Wireless Ad Hoc Networks", IEEE Communications Letters, Vol. 16, Pp. 1903-1906, No. 11, November 2012.

V. Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", 2012 International Conference on Computer Communication and Informatics (*ICCCI* - 2012), Jan. 10 – 12, 2012, Coimbatore, INDIA.

VI. Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection IEEE Transactions On Network And Service Management, Pp. 169-182, Vol. 9, No. 2, June 2012.

VII. Preeti Sachan, Pabitra Mohan Khilar, "Security Attacks and Solutions in MANET", Proceedings of International Conference on Advances in Computer Engineering (ACEEE), pp 172-176, 2011.

VIII. Pravina Dhurandher, "FACES: Friend Based Ad hoc Routing Using Challenges to establish security in MANET Systems" IEEE SYSTEMS Journal ,Volume 5, No 2, June 2011,pp:176- 188.

IX. Yi Zhang, QiangLiu "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 163 – 167, 2010 .

X. Husain. Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection ", IEEE International Conference on Computer & Communication Technology (ICCCT), pp. 292-297, 2011.

XI. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", publication in the IEEE Globecom 2011.

XII. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume 2, 2008.

XIII. Lalit Himral, Vishal Vig, Nagesh Chand "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 5 May 2011.

XIV. P.Yi, Z.Dai, S.Zhang, Y.Zhong,"A New Routing Attack In Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, pp. 83-94, 2005.

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

XVI. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks , CRC Press LLC, 2003.

XVII. 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.

XVIII. Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution" IEEE International Conference on Communications (ICC), pp. 1-6, 14-18 June, 2009.