ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 10, October 2017

Attacks and Exploits on the Existing Routing Protocols in a MANET

A.VANI

Abstract— MANETs have certain unique characteristics that make them vulnerable to several types of attacks. In MANET, mobile nodes without adequate protection are easy to compromise; an attacker can listen, modify and attempt to disrupt all the traffic on the wireless communications channel as one of the legitimate node in the network. Since they are deployed an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is quite difficult to design a secure protocol when compared to wired or infrastructure-based wireless networks. In this paper, primary goals of a secure routing protocol – confidentiality, integrity and availability, authenticity and non-repudiation are discussed.

Index Terms—Routing, Attacks, Security, AODV, MANET.

I. INTRODUCTION

Mobile adhoc networks are a new generation of networks offering unrestricted mobility without any underlying infrastructure. Primary application of wireless ad hoc networks is in military, tactical and other security-sensitive operations. Hence, security is a critical issue. Due to the nature of ad hoc networks, make them vulnerable to various forms of secret information, data tampering, impersonation and denial of service. Hence, conventional security measures cannot be used. New techniques of security measures are essential for high survivability networks than conventional wired and static networks. The performance of the protocol will be severely affected in the presence of compromised nodes that inflict unpredictable and undetectable Byzantine failure. Visualizing a secure ad hoc network routing protocols are implemented and also need to implement intrusion detection and intrusion prevention model to present to present several identified attacks in the network.

II. ROUTING IN MANETs

Routing is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance from the application point of view - application requirements- while minimizing the cost of network itself in accordance with its capacity. The application requirements are hop count, delay, throughput, loss rate, stability, jitter, cost; and the network capacity is a function of available resources that reside at each node and number of nodes in the network as well as its density, frequency of end-to-end connection (i.e. number of communication), frequency of topology changes (mobility rate). The four core basic routing functionality for mobile ad hoc networks is:

• ***Path generation*:** This generates paths according to the assembled and distributed state information of the network and of the application; assembling and distributing network and user traffic state information.

• ***Path selection*:** This selects appropriate paths based on network and application state information.

• ***Data Forwarding*:** This forwards user traffic along the select route forwarding user traffic along the selected route.

• ***Path Maintenance*:** Maintaining of the selected route.
figures and tables.

III. CLASSIFICATION OF ATTACKS ON MANET ROUTING PROTOCOLS

The attacks on routing protocols can generally be classified as *routing disruption* attacks (attacker tries to disrupt the routing mechanism by routing packets in wrong paths) and *resource consumption* attacks (some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth). Both these attacks are examples of Denial of Service (DoS) attacks.
Table 1. Depicts a broader the classification of the possible attacks in MANETs.

Attack on MANET routing protocols			
Attacks using Modification	Attacks using Impersonation	Attacks using Fabrication	Special Attacks.
1.Redirection by modified route. 2.Redirection with modified hop counts. 3.DoS with modified source routing. 4. Tunneling.	Forming loop by spoofing	1.Falsifying route errors in AODV and DSR 2.Route cache poisoning in DSR	1.Wormhole Attack 2.Black hole Attack

Table 1: Classification of attacks on MANET routing protocols

Mobile ad hoc Networks are susceptible to having their effective operation compromising a variety of security attacks.

E.g.: Misbehaving nodes can cause a general network disruption by not forwarding packets on behalf of other nodes in the network.

Nodes may misbehave either because they are malicious and deliberately wish to disrupt the network, or because they are Selfish and wish to conserve their own limited resources such as a power or for other reasons.

- Different attacks can be classified based on their nature as
  1. Passive attacks
  2. Active attacks
     a. Internal attacks
     b.External attacks
- External attacks
  - Injecting erroneous routing Information.
  - Replaying old routing Information.
  - Distorting routing Information.
- Internal attacks[inside the network]
  - Dropping attack [packet]
  - Modification attack
  - Denial of service attack
  - Eaves dropping attack
  - Masquerading
  - Block hole attack
  - Gray hole attack
  - Stealth attack
  - Timing attack
- Attacks are passive (release of contents, traffic analysis) or
- active (masquerade, replay, modification, denial of service)
- Attacker are interruption for security mechanisms like
  - Interception—Confidentiality
  - Modification—Integrity
  - Fabrication—Authenticity
  - Interruption—Availability

Most of the attacks depicted are focused on the on-demand and reactive protocols such as AODV[3], DSR[2], etc. The following sections look at these attacks in more detail.

IV. Attacks using Modification

In this type of attack, the protocol fields of the messages passed among the nodes is modified, thereby resulting in traffic subversion or Denial of Service (DoS) attacks. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.The following sections discuss some of these attacks-

(a) *Redirection by modified route sequence numbers*: This attack is possible against the AODV protocol. Consider the network shown in figure 2 [4]. If M is a malicious node that overhears the broadcast RREQ packet for the destination node X originated by source node S, then it sends a false RREP packet with a longer route to node X (adding itself to the list) and a greater destination sequence number than that last advertised by node X. This will make S to route all its packets through M, since node M advertises a fresher route to node X.

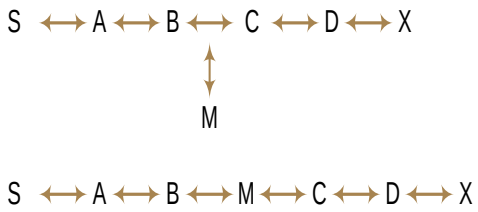

Figure 2: Example of MANET with a malicious node [5]

(b) *Redirection with modified hop count:* This type of attack is targeted against the AODV protocol in which a malicious node can increase the chances that they are included on a newly created route by resetting the hop count field of a RREQ packet to zero.

(c) *Denial of Service with modified source routes*: This attack is possible against DSR which uses source routes and works as follows - in figure 2, assume that a shortest path exists from node S to node X. Also assume that C and X and nodes B and C cannot hear each other, and that node M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to node X with the source route S-A-B-C-D-X. If M intercepts this packet, removes D from the list and forwards it to node C, C will attempt to forward this packet to node X which is not possible since C cannot hear X. Thus Malicious node M has successfully launched a DoS attack on node X.

V. Attacks using Impersonation

These types of attacks act against authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the path of the network topology as perceived by another node. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a begin node can gather. Such attacks can result in the formation of loops as described below –

(a) *Formation of loops by spoofing*: As shown in figure 3. [5], assume that path exists from A to X. Further let's assume that A can hear B and D (which means that A is in the radio range of B and D), B can hear A and C; D can hear A and C; and C can hear B, D, E. Also suppose a malicious node M can hear A, B, C and D. The attack can be described as follows:

"To start the attack, M changes its MAC address to match A's, moves closer to and out of the range of A. It then sends

an RREP to B that contains a hop count to X that is less than the one sent by C, e.g., zero. Therefore B changes its route to the destination, X, to go through A, as illustrated in Figure. 3. M then changes its MAC address to match B ' s, moves closer to and out of range of B , and then sends to C an RREP with a hop-count to X lower than what was advertised by E. C then routes to X through B. At this point a loop is formed and X is unreachable from the four nodes. The attack is possible with a single malicious attacker; however, multiple attackers may collaborate for the same result."

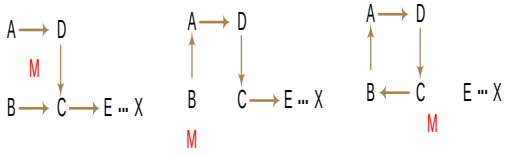

Figure 3: Formation of loops by spoofing

VI. Attacks using Fabrication

In this type of attack, routing mechanism is disturbed by a malicious node that tries to inject fake messages or routing packets to disrupt the routing mechanism. Such attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. The following attacks are examples of attacks by fabrication [5]–

(a) *Falsifying route errors*: This type of attack exploits the broadcast mechanism of sending route error (RERR) packets in AODV and DSR routing protocols (described in chapter 2). Again consider the network shown in Figure. 2. Suppose that M is a malicious node that overhears broadcast packets from B and C. M can launch a fabrication attack against X by broadcasting false RERR packets to node B indicating a broken link between nodes C and X. B receives the spoofed route error message as it came from C. Thus, B deletes its routing entry to node X and forwards the RERR packet to node A, which also follows suit. If M repeats this procedure whenever node S establishes route to node X, it prevents node S from communicating with node X.

(b) *Route cache poisoning*: It refers to attacks which modify or corrupt the routing tables by injecting fake routing packets. Such an attack is possible against an optimized version of the DSR protocol, in which nodes discover routes from neighboring nodes by listening promiscuously on the broadcast channel. For example in figure 2, if any node overhears the route from S to X, it will add that entry to its routing table. Suppose a malicious node M advertises routes to X via itself, i.e. S-A-B-C-M-C-D-X, it creates false route entries in the listening node's routing table.

VII. Special Attacks

Apart from the attacks described above there are two other severe attacks which are possible against routing protocols such as AODV, DSR, etc. They are described below-

(a) Wormhole Attack: The wormhole attack is a severe type of attack in which two colluding malicious nodes can tunnel packets through a "tunnel" or vertex cut in the network as shown in figure 4.

It exploits the following two properties:

1. In AODV protocol when a node (source) needs to communicate with another ode (destination) but the source does not have the route, it broadcasts RREQ to its neighbors. The process continues until an immediate node having the fresh route to the destination is found (or the destination itself is found). To prevent unnecessary processing of same RREQ packet from different neighbors, each node processes the RREQ packets that first arrives, thereby ignores other copies
2. A direct (tunneling) link (wired/wireless) is faster than a general hop-by-hop propagation.

Usually it involves two attackers, one near the source and another near the destination. When a source broadcasts an RREQ packet, the first attacker records it and transmits directly through a tunnel to the second attacker (who is near the destination)[6]. Any neighbor of destination receives the RREQ from the attacker it normally processes. In the meantime, the original RREQ comes to it by hop-by-hop propagation, it simply discards it. Because, already it has received the packet.

This can cause DoS attack. Further, it bounds the source and destination to use the attacker nodes.

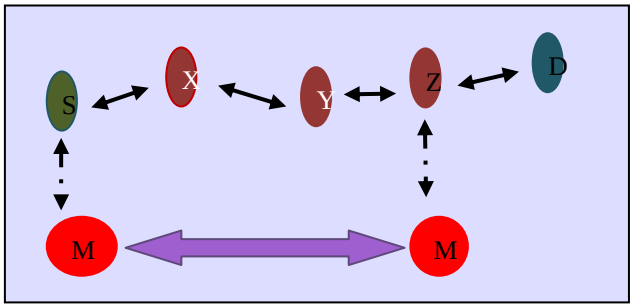

Figure 4: Illustration of Wormhole Attack

S wants to communicate with D, so, it broadcasts a RREQ packet to its neighbor X. In wireless transmissions, it is quite trivial to be transparent for another node within the radio signal of the sending node. So an attacker M1 records the request and tunnels it through a fast link-to-link channel to another attacker M2 placed near the destination as shown in the figure 4.Obviously, node Z will get the request first from M2 without any detection; this is because link-to-link communication is faster than multi-hop communication. Therefore, Z processes the request. Thus, the attackers force nodes S to use the route via M1 and M2 to reach D. furthermore, when Z gets the original RREQ from its neighbor Y it will drop the packet as specified by the routing algorithm.

(b) Black hole attack: The black hole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. The AODV protocol is

vulnerable to such an attack. More details on this attack can be found in [8].

In fig.5. Node 1 wants to send data packets to node 4 and initiates the route discovery process. We assume that node 3 is a malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches, first to node 1 then one thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 3. As a result, all packets through the malicious node is consumed or lost

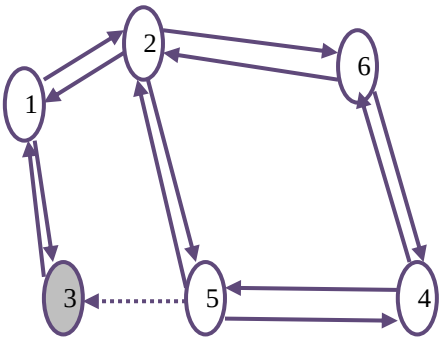

Figure 5: Illustration of Black hole attack

VIII. CONCLUSION

Mobile ad hoc networks are one of the most emerging areas in research over the past few years. The communication within in MANET are between the networks is highly dependent on cooperation of all it connected nodes or devices. Due to this MANETs are highly vulnerable to selfish nodes. In this paper, how the malicious and selfish nodes attack the network and affect the security services is presented.This is helpful for research against different security services in detail.

REFERENCES

[1] C. Siva Ram Murthy, B.S. Manoj, "*Ad Hoc Wireless Networks : Architectures and Protocols*", Prentice Hall Publishers, May 2004, ISBN 013147023X

[2] D B. Johnson, D A. Maltz, and Y. Hu, "*The dynamic source routing protocol for mobile ad hoc network*," Internet-Draft, April 2003. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[3] C.E. Perkins, E. Royer, and S.R. Das, "*Ad hoc on demand distance vector (AODV) routing*," Internet Draft, March 2000. http://www.ietf.org/internetdrafts /draft-ietf-manet-aodv-05.txt

[4] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[5]M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks". In proceedings of Workshop on Dependable Network Computing and Mobile system In Conjunction with 28th IEEEInternational Symposium on Reliable Distributed Systems:2009.

[6]A.Peerig, Y.C. Hu, and D.B.Johnson.Worm hole Protection in Wireless Ad hoc Networks. Technical Report TRo1-384, Department of Computer Science, Rice University, 2001.

[7]H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "*Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Pages 38- 47, 2004.

[8]P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[9]S. Kurosawa et al., "Detecting Black hole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic", IEEE Military Communications Conference, Vol. 2,page(s):1054-1059, Oct 2003