Dynamic Security Implementation in MANETS

Anshu, Suman Sangwan

Abstract: **Security has become a primary concern in order to provide reliable communication between mobile nodes. Inherent characteristics of Mobile ad hoc networks like open peer-to-peer network architecture, shared wireless medium, resource constraints, and dynamic network topology make them more vulnerable to security threats. This calls for elaborated security solutions that achieve both broad protection and desirable network performance. This paper identifies the security issues related to MANET, the known routing attacks and the proposed solutions to these attacks in various Scenarios.**

Index Terms: **attacks, manet, measures, security**

I. INTRODUCTION

Mobile ad hoc network (MANET) is a set of mobile devices also known as nodes which over a wireless channel communicate with each other without the presence of a physical media or a central authority. The nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is having a transmitter and receiver, with the help of which it communicates with the other mobile devices in its wireless environment.

The key features and challenges of the MANETs [2] are presented in Table 1.The rest of the paper is organized as follows: Section 2 demonstrates the present routing attacks, and Section 3 shows the various counter measures to these. Finally Section 4 summarizes the report

Manuscript received June 10, 2014

Anshu, Computer Science & Engineering , Deen Bandhu Chotu Ram University, Sonepat, India, +91-9991666556, (mca706@gamil.com).

Suman Sagwan, Computer Science & Engineering , Deen Bandhu Chotu Ram University, Sonepat, India, +91-946034005 , (suman2222@yahoo.com)

Table 1:Characteristics of MANETS

Sr. No.	Characteristics	Description
1	Autonomous terminal.	In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router
2	Distributed operation	Since there is no the central control of the network operations, the control and management of the network is distributed among the terminals.
3	Dynamism of Topology	The nodes of MANET are randomly and frequently may leave or join the network at any point of Time. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable.
4	Resource constraints:	MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc.
5	Light-weight terminals	In most cases, the MANET nodes are mobile devices with less CPU processing capability, Small memory size, and low power storage.

II. ROUTING ATTACKS IN MANETS

Due to dynamic nature of MANETs, and lack of centralized authority, the ad hoc networks are prone to

various kinds of attacks. The attacks on MANETs can be both active as well as passive. In passive attacks the attacker does not send any data, but just listens to the channel ideally. Passive attacks are only for getting important information but on the contrary active attacks can interrupt Operation of the Node and sometimes whole Network also. As the passive attacker does not induce any traffic so it is nearly impossible to detect this sort of attack. While actions of active attackers include Adding, Deleting and Modifying Packets, and communicating with other nodes which hampers availability, authenticity of the Network. In [5], the authors have analyzed various attacks on MANETs and their solutions on protocol layer wise criteria. In [6] author has found newer attacks like flooding, black hole, link spoofing, replay, wormhole, colluding misrelay and their measures. In [7], [8] the authors have presented an overview of secure routing protocols (Authenticated routing for ad hoc networks (ARAN)[9], Ariadne[10], Secure AODV (SAODV)[11], Secure Efficient Ad hoc Distance vector routing protocol (SEAD)[12], Secure Routing Protocol (SRP)[13], Secure Link-State Protocol (SLSP) [14]) in MANETs.

The well known routing attacks in MANETs are discussed as follows:

A. Routing Table Overflow:

In this Attack, attacker node floods the network with fake route creation packets to fake (non-existing) nodes or simply sends too much route advertisements to the network. The purpose is to overcome the routing-protocol implementations, by creating enough routes to prevent new routes from being created or to overcome the protocol implementation. This exploits the limited capacity of mobile devices. Proactive routing protocols, as they create and maintain routes to all possible destinations are more susceptible to this attack.

B. Sleep Deprivation:

In sleep deprivation attack, the resources of the specific node/nodes of the network are exhausted by continuously keeping them busy in routing decisions. The attacker node constantly requests for either existing or non-existing nodes, forcing the nearby nodes to process and send these packets. So it consumes the battery and network bandwidth obstructing the normal functioning of the network.

C. Impersonation Attack:

Impersonation attacks are induced by using the identity of other node, like IP or MAC address. A malicious node can impersonate an authorized user and provide fake information or change the configuration of the network.

D. Node Isolation Attack:

As the name suggests, the main role of this attack is to block a given node from communicating with other nodes in the network. By doing so the attacker can prevent link information of particular node with Whole Network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

E. Routing Table Poisoning Attack:

Various routing rules maintain tables which hold information regarding route of the network. In this attack, faulty node sends fictitious routing update and error messages or modified legal updates to certified nodes in the network. It may result in forwarding packets along sub optimal routes, blocking in the network, formation of loops. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other genuine RREQ packets with lower sequence numbers to be deleted [17].

F. Black Hole Attack:

In this attack, the attacker node inserts false route Response to the route requests claiming to have the shortest path to the destination node whose packets it wants to interrupt. Once the pretended route has been established attacker node is then in a state to misuse or reject any or all of the network traffic being routed through it.

G. Byzantine Attack:

This attack involves multiple attackers that work in collusion to degrade the network performance such as creating loops, selectively dropping packets, choosing non optimal paths for packet forwarding.

H. Information Disclosure:

A compromised node can breach the confidentiality principle of security and share important information like private and public keys, node status, password, optimal route to authorized nodes, location of node and other control information in packet headers to unauthorized nodes in the network. The revealed location information gives understanding of the network topology. Routing packets are then sent with insufficient hop-limit and ICMP error messages returned by the halfway nodes are recorded [4]. So it gives blueprint of the network to the target nodes.

I. Wormhole Attack:

The wormhole attack involves the collaboration in two attacking nodes [31]. One attacker node captures routing traffic at one point of the network and tunnels it to another point in the network that shares communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link.

J. Blackmail:

The main reason of this type of attack is lack of authenticity and having provision for any node to distort

other node's legitimate information. Nodes keep information of supposed malicious nodes in a blacklist. An intruder may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and segregate legitimate nodes from the network [19].

III. SECURITY MEASURES AGAINST ROUTING ATTACKS IN MANETS

This section is discussed below:

A) Solutions to the Flooding Attack:

In [21], author has proposed a simple mechanism to Prevent the flooding attack in the AODV protocol.He proposed that every node monitors its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the threshold already defined, the node records the ID of that neighbor in a blacklist. Every prospect RREQs from the blacklisted nodes is then dropped. But its drawback is that a flooding threshold has to be set less so that the attack cannot be detected. Also if an authentic nodes ID is impersonated by a malicious node and a huge number of RREQs are broadcast, other nodes might put the ID of this genuine node on the blacklist.

In [22] Author has proposed a technique to lessen the effect of a flooding attack in the AODV protocol. It uses an arithmetical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. The difference between this approach to attack detection and as discussed in [21.] is that instead of a fixed threshold, this approach determines the threshold based on a statistical analysis of RREQs. The key benefit of this approach is that it can decrease the impact of the attack for varying flooding rates. In [23], Author has proposed a flow based detection mechanism against the flooding attacks in MANETs using the CUSUM algorithm.

B) Solutions to the Blackhole Attack:

In [26] Author has proposed that the requesting node without sending the DATA packets to the respond node at once waits for other replies with next hop details from the other adjacent nodes. After receiving the first request a timer is set in the 'TimerExpiredTable', for collecting the further requests from different nodes. The 'sequence number', and the time at which the packet arrives is stored in a 'Collect Route Reply Table' (CRRT). Now the 'timeout' value based on arriving time of the first route request are calculated. Now CRRT is checked for any repeated next hop node which if found, it is assumed the paths are correct. If there is no replication then any arbitrary route from CRRT is selected.

In [27] Author has proposed the route confirmation request and route confirmation reply to avoid the blackhole attack. In addition to sending RREPs to the Source node the transitional node also sends CREQs to its next-hop node towards the destination node. The next-hop node on receiving of a CREQ looks up its cache for a path to the destination. If a path is found, it sends the CREP to the source. After receiving the CREP, the source node compares the path in RREP and the one in CREP. If two are identical the source node pronounces the path to be correct.

In [28], Author anticipated that Source node has to wait until the arrival of a RREP packet from more than two nodes. After receiving multiple RREPs, the source node checks about a shared hop. If at least one hop is shared, the source node considers that the route is secure. The negative aspect here is time delay due to the wait till the arrival of multiple RREPs.

In [29], Author anticipated that the destination Sequence number must adequately be augmented by the enemy node in order to influence the source node that the path provided is optimum. On the basis of differences between the destination sequence numbers of the received RREPs, the authors advise an arithmetical based anomaly detection approach to detect the blackhole attack.

C) Solution to Node Isolation Attack:

In [20] it is shown that a faulty node can block a specific node and prevent it from receiving data packets from other nodes by preserving a TC message in OLSR protocol. On Observation of TC message & Hello message a detection technique is proposed. If a node is unable to hear a TC message from its MPR node on regular basis but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

In [30], Author has suggested an IDS that detects TC link and message preservation in the OLSR protocol. Each node is set to observe whether a MPR node produces a TC message regularly or not. If a MPR node produces a TC message regularly, the node checks whether or not the TC message actually contains itself to detect the attack. The disadvantage of this technique is that they cannot detect the attack if it that is launched by two colluding next hop nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

D) Solutions to the Worm Hole Attack:

In [31], packet leashes are proposed to detect and defend against the wormhole attack. Author in their work have anticipated temporal leashes and geographical leashes. In case of temporal leashes every node is to calculate the packet expiry time (te) based on the speed of light c and is to include the expiration time (te') in its packet to prevent the packet from going further than a specific distance, L. At the receiver node, the packet is checked for packet expiry by matching its current time and the te in the packet. The authors also introduce TIK, which is used for authentication of the expiration time that can be changed by the malicious node. But the limitation here is that all nodes have to be in tight clock synchronization. For the geographical leashes, each node must know its own location and can be loosely synchronized. In this method, a sender of a packet includes its current position and the transmitting time. Therefore, a receiver can measure neighbor relations by calculating distance between itself and the sender of the packet. The benefit of geographic leashes over temporal leashes is that the synchronization of time is not that important.

In [32] Author has Suggested a Statistical Analysis of Multipath (SAM), which is a technique to detect the wormhole attack by making use multipath routing. The attack is detected by computing the relative frequency of each link that appears in all of the received routes from one route discovery. If highest Relative frequency is found in a link then that has termed as wormhole link.

In [33] Author has suggested a method based on propagation speeds of requests and statistical profiling. In discovery schemes in which Flooding is used, there is need of requests to be send at high priority than other packets. This implicitly increases the time to exchange information among faulty nodes. A scattered and adaptive statistical profiling technique to filter RREQs (each destination node filters RREQs that are targeted to it and have excessively large delays) or RREPs (each source node monitors the RREPs it receives and filters those that have excessively large delays) is suggested. Since various RREQs/RREPs take different number of hops, the upper bound on the per hop time of RREQ/RREP packets is so computed that most normal packets are retained and most fallacious packets are filtered. The main benefit of this approach are that no requirement of synchronized clocks, no additional control packet overhead is forced, only simple calculations by the sources or destinations of connections is required.

IV. CONCLUSION:

In this paper, security attacks in mobile ad-hoc network have been discussed. As The security-sensitive applications of MANETs require high degree of security therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The existing proposals are typically attack-oriented because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and Efficient routing security. Work is being carried towards designing an algorithm which can provide the dynamic security in MANETs.

REFERENCES

[1] C.S.R.Murthy and B.S.Manoj, *Ad Hoc Wireless Networks*, Pearson Education, 2008.

[2] George Aggelou, *Mobile Ad Hoc Networks*, McGraw-Hill, 2004.

[3] E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," *AusCERT2006 R&D Stream Program, Information Technology Security Conference*, May 2006.

[4] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Communications*, vol. 11, pp. 38-47, Feb., 2004.

[5] B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, Springer, vol. 17, 2006.

[6] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour,"A Survey Of Routing Attacks In Mobile Ad Hoc Networks," *IEEE Wireless Communications*, vol. 14, issue 5, pp. 85-91, October 2007.

[7] Y.C.Hu and A.Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security and Privacy*, vol. 2(3), pp. 28-39, May 2004.

[8] D. Wang, M. Hu, H. Zhi, "A Survey of Secure Routing in Ad Hoc Networks," *IEEE Ninth International Conference on Web-Age Information Management, 2008, (WAIM '08)*, pp.482-486, July 2008.

[9] K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "Authenticated Routing for Ad Hoc Networks," *Proceedings of IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, March 2005.

[10] Y.C.Hu, A.Perrig, and D.B.Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. MobiCom'02*, Atlanta, GA, pp. 12-13 September 2002.

[11] M.G.Zapata and N.Asokan, "Securing Ad-Hoc Routing Protocols," *Proceedings of ACM Workshop on Wireless Security*, pp. 1–10,September 2002.

[12] Y.C.Hu, D.B.Johnson and A.Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, pp. 3-13. June 2002.

[13] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02)*, IEEE Press, pp. 78-87, 2002.

[14] P.Papadimitratos, and Z.J.Haas, "Secure Link State Routing for Mobile Ad hoc Networks," *Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks*, IEEE Press, pp. 27-31, 2003.

[15] Y.C.Hu, A.Perrig and D.Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, SanDiego, California, pp. 30-40, September 2003.

[16] T.R.Andel and A.Yasinsac, "The Invisible Node Attack Revisited," *Proceedings of IEEE SoutheastCon 2007*, pp. 686 – 691, March 2007.

[17] M.Drozda, H.Szczerbicka., "Artificial Immune Systems: Survey and Applications in Ad Hoc Wireless Networks," *Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06)*, Calgary, Canada, pp. 485-492, 2006.

[18] X.Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen and Z.Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," *IEEE International Conference on Communications, ICC '07*, pp. 1247 – 1253, June 2007.

[19] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks," *IEEE Network Magazine*, vol. 6, no. 13, pp. 24-30, November/December 1999.

[20] B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks," *Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06)*, pp. 30-35, June 2006.

[21] 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.

[22] S.Desilva, and R.V.Boppana, "Mitigating Malicious Control Packet Floods In Ad Hoc Networks," *Proceedings of IEEE Wireless Communications and Networking Conference 2005*, , vol. -4, pp. 2112-2117, March 2005.

[23] Y.Guo, S.Gordon, S.Perreau, "A Flow Based Detection Mechanism Against Flooding Attacks In Mobile Ad Hoc Networks," *Wireless Communications and Networking Conference, IEEE (WCNC 2007)*, pp.3105-3110, March 2007.

[24] T.Peng, C.Leckie, R.Kotagiri, "Proactively Detecting Distributed Denial Of Service Attacks Using Source IP Address Monitoring,"*Proceedings of IFIP-TC6*, 782 Athens, Greece, pp. 771-782, May 2004.

[25] V.Balakrishnan, V.Varadharajan, U.K.Tupakula, "Fellowship: Defense Against Flooding And Packet Drop Attacks In MANET," *Network Operations and Management Symposium, NOMS 2006*, pp. 1-4, 2006.

[26] L.Tamilselvan, V.Sankaranarayanan, "Prevention of Blackhole Attack in MANET," *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, AusWireless*, pp. 21-26, August 2007

[27] S.Lee, B.Han, and M.Shin, "Robust Routing in Wireless Ad Hoc Networks," *2002 International. Conference on Parallel Processing Workshop*, Vancouver, Canada, pp. 73-78, August 2002.

[28] M.A.Shurman, S.M.Yoo, and S.Park, "Black Hole Attack in Mobile Ad Hoc Networks," *ACM Southeast Regional Conference*, pp. 96-97, 2004.
[29] S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," *International Journal of Network Security*, vol. 5, no. 3, pp. 338-346, November 2007.
[30] D.Dhillon, J.Zhu, J.Richards and T.Randhawa, "Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs," *Proceedings Of The 2006 International Conference On Wireless Communications And Mobile Computing*, pp. 45-50, 2006.
[31] Y.C.Hu, A.Perrig, and D.Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, February 2006.
[32] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," *IEEE Wireless Communication and Networking Conference '05*, vol. 4, pp.2106-2111, March 2005.
[33] X.Su, R.V.Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks," *IEEE International Conference on Communications, ICC '07*, pp. 1136-1141, June 2007.
[34] M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," *Military Communications Conference, MILCOM 2006*, pp. 1-7, October 2006
[35] Y.Sun, Z.Han and K.J.R.Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Communications Magazine*, vol. 46, issue 2, pp.112-119, February 2008.
[36] V.Balakrishnan, V.Varadharajan, U.K.Tupakula and P.Lucs, "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks," *15th IEEE International Conference on Networks, ICON 2007*, pp. 182-187, November 2007.
[37] V.Balakrishnan, V.Varadharajan, U.K.Tupakula and P.Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks," *4th International Symposium on Wireless Communication Systems, ISWCS 2007*, pp. 592-596, October 2007