Survey of Security Threats and Counter Measures in Mobile Ad-Hoc Networks

Sunil Kumar Jangir[1], Naveen Hemrajani[2]

Department of Computer Science & Engineering, JECRC University, Jaipur, Rajasthan, India

ABSTRACT: Mobile ad hoc networks (MANET) are pervasive, self-configuring, infrastructure-free, and ubiquitous devoid of any centralized authority. Mobile ad hoc networks have proved their efficiency in the deployment for different fields, but they are highly vulnerable to security attacks which is particularly challenging in wireless networks. The existing research that has been carried out provides authentication, confidentiality, availability, and secure routing in ad hoc networks. This paper is an attempt to review the prevailing mobile ad hoc network security threats and the existing solutions.

Keywords: Authentication, Confidentiality, Routing etc.

1. INTRODUCTION

A MANET is constituted by a group of self-dependent mobile nodes with dynamic topology, infrastructure less network and is self-configurable. It is less secure as comparative to centralized systems for it has more chances of wireless attacks. However, it is useful in many industrial and corporate sectors as it leads to increase in productivity for its less complex structure. Here, mobile nodes communicate directly or via intermediate nodes (known as multibox communication) [1], where the node acts both as a router and the host that are dynamic in nature (i.e. change positions frequently). In case of any breakage in link, the nodes themselves manage the communication dynamically [2].

There are several challenges in designing protocols for MANET security for it is a wireless network where the problems faced include battery life, resource limitation in memory size, eavesdropping, vulnerability, unreliable communication bandwidth, high security threats and rapid changes in topologies [3][4][5].There is a stringent need for a more secure MANET in military which requires additional factors in designing protocols as there are high tempo operations. It needs a fully heterogeneous network with rapid and dynamic changes in topology and favorable environment all the time [6].Some attacks can easily occur in MANET due to its wireless topology, like DOS(Denial of service), where blank packets flood and congest the network [7].

1.1 SECURITY CRITERIA

Earlier, encryption software and firewalls were used to protect the network that did not prove much efficient for a MANET infrastructure, for the major concern in MANET security is integrity, authentication, confidentiality, non-repudiation, availability to mobile users and anonymity as described below:

1.1.1 Availability

Availability maintains the activeness of the network despite various attacks. Its major concern is the unauthorized and illegal access of resources. In some attacks, there could be possible disruption of routing protocol and continuity of services in the network [8].

1.1.2 Confidentiality

Confidentiality ensures protection from passive attacks. In military, the leakage of information can't be compromised. Confidentiality ensures authorized access of information that protects data. Even it ensures the confidentiality of router location and packet information.

1.1.3 Integrity

Integrity guarantees that message delivered is neither modified nor duplicated or reordered for replay of original message. It also ensures that only the authorized parties retrieve the information or messages and the message is not corrupted or lost. Integrity ensures that messages are delivered to the authorized parties as sent.

Sunil Kumar Jangir[1]
[1]Research Scholar, Department of Computer Science & Engineering ,JECRC University, Jaipur
sunil.jangir07@gmail.com[1],
Naveen Hemrajani[2]
[2]Prof.,Department of Computer Science & Engineering ,JECRC University, Jaipur
naven_h@yahoo.com[2]

1.1.4 Authentication

Authentication ensures that communicating parties are authorized parties by verifying their identity before communication. Ubiquitous networks require mutual authentication and for which mutual authentication protocols are required to prevent from attacks. [8].

1.1.5 Scalability

Although the scalability does not affect security directly but as ad hoc network may consist of hundreds or even thousands of nodes and if the network is not scalable enough to add new nodes within it then newly added nodes can be compromised by the attacker by which it can gain access to the whole system.[9]

1.1.6 Nonrepudiation

Nonrepudiation ensures that sender can't deny about its previous communications. Receiver can always prove later that the particular message was sent by that alleged sender. It is also used for isolation and detection of nodes.

1.1.7 Anonymity

This simply helps in ensuring privacy of personal information about the owner or user and it is not disclosed by the node.

2. CLASSIFICATION OF ATTACKS

Attacks can be broadly classified into passive and active attacks. Categorization can be seen in several contexts such as network topology, functionality and security goals. Categorization can also be done for different layers of networks [2].

2.1 Passive attack

Passive attack is an act of secretly observing the data which is being transferred between two parties for snooping, eavesdropping, traffic analysis and monitoring . These type of attacks do not interfere in the functionality of the whole network but confidentiality of the message can be lost if the attacker succeedes. In this type of attack the attacker secretly observes the network in such a way that it becomes very difficult to identify passive attacks, but with theuse of powerful encryption techniques such attacks can be reduced.

2.2 Active attack

In the active attack the data being transferred between two parties is modified or destroyed. Modification of routing information or packets, replay of old packets, denial of service and impersonation are some example of such type of attacks. There are two types of active attacks, one which is initiated by the compromised nodes (earlier a legitimate and authorized node) is an internal attack, and the attack which is initiated by adversaries (which do not belong to the network) are external attacks. These attacks can be prevented by using powerful encryption techniques and firewalls.

Table 1. Types of Security Issues for MANET[18]

MANET Layers	Security Issues
Application	Detecting and preventing viruses, worms, malicious codes and application abuses
Transport	Authentication and securing end to-end or point-to-point communication through data encryption
Network	Protecting the ad hoc routing and forwarding protocols
Data Link	Protecting the wireless MAC protocol and providing link layer security support
Physical	Preventing signal jamming denial-of-service attacks

MANET Layers	Type of attack
Application	Repudiation, Data corruption
Transport	Session hijacking, TCP/UDP SYN Flooding
Network	Black hole, Gray hole4, worm hole, Byzantine, flooding, resource
Data Link	Traffic, Analyzer, monitoring disruption (MAC (201-11)
Physical	Jamming, interception, eavesdropping

Table 2. Types of attacks in MANET different layers

3. ROUTING ATTACKS IN MANETS

MANET is totally dependent on active nodes that provide routing among them and build a network. In case any node becomes malicious, attacker can easily attack the network that may disrupt the routing and ad-hoc network becomes vulnerable to attacks due to its dynamic, distributed infrastructure and not having any centralized body.DOS (Denial Of Service)[10] attacks are easily possible for attacker in

such cases. Both active and passive attacks are possible here. It's our assumption in ad-hoc networks that all nodes are trustworthy but this is not necessary always true.Our first approach, therefore, is to understand and analyze the potential threats and then understand the capabilities of potential attackers.

3.1 Flooding attack

The node that is being attacked by attacker floods false route creation packets to fake nodes and thus produces excessive route advertisements that prevent new routes from being created. This effects proactive routing where routes are created and maintained to all possible destinations [11].

3.2 Wormhole attack

This type of attack includes two attacking nodes [14] in which one attacker captures one node routing traffic and tunnels it to another point and shares a high speed communication link between nodes and inject tunnel traffic back to network. Thus these two attacks at different points distort the topology over the wormhole link.

3.3 Blackhole attack

This type of attack deals with two major concern. First, the node attacks on the ad-hoc routing protocol such as AODV and do false advertisement of itself as having some route to destination even though no such route exists, this intercepts the packets and secondly the attacker either consumes the intercepted packets or forwards them by modifying the data from some nodes. However, since the neighbouring nodes may monitor and expose the ongoing attacks it leaves other nodes' data intact that reduces the suspicion.

3.4 Node Isolation attack

This type of attack is against OLSR protocol. As the name specifies it isolates the node from the network. The idea behind node separation is that it prevents the node link information to reach other nodes and thus other nodes are not able to build a route to the victim node and to send data to the attacked node[12].

3.5 Routing Table Poisoning attack

Routing table poisoning attack is possible where routing protocols maintain tables that hold the network information. This attack aims to put in false entries in the table that leads to selection of non optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network. Here the attacked nodes change the valid messages from other nodes. Another way is to inject a RREQ packet with high sequence number that deletes the other RREQ having low sequence number [13].

3.6 Rushing attack

In this attack, the attacker node initializes the route discovery process to a target node. If all its ROUTE REQUESTs are the first to reach the neighbors of that target node then any route discovered by this Route Discovery includes a hop through the attacker and the neighboring nodes discard any legitimate requests and d0 not forward any further REQUESTs from this Route Discovery. Thus the initiator does not find any route that does not include attacker. [15]

3.7 Blackmail

This attack is relevant for those routing protocols that use mechanisms for the identification of malicious nodes. This attack is basically due to lack of authenticity. This permits any node to corrupt other node's useful information by fabricating reporting messages that are used by routing protocols and tells other nodes to add attacker node in their network. Thus legitimate node is isolated from the network [16].

3.8 The Invisible Node attack

This attack is different from other existing attacks as here the attacking node is invisible to other nodes. It is relevant for those protocols that depend on the identification of the functionality of nodes. Ifany node is participating in this protocol without revealing its identity then it becomes invisible to other nodes and is termed as INA. This type of attack is unsolvable so far [17].

3.9 Snare attack

This attack is proposed by Lin et al. It is related to military specific applications. In this attack, a node could be physically compromised similar to that as a soldier caught by enemy in a battlefield. Later, the attacker can easily prevent any transmission in the network with the help of that compromised node, trace the location of VIN and analyze routes. Thus the attacker can easily win the battle by launching a Decapitation Strike on those VINs [31].

4. SECURITY MEASURES

In view of the various security attacks discussed, security becomes a major concern in MANET to provide secure communication among nodes.

Security is essential to maintain network functions like routing and packet forwarding. Without any countermeasures network operations can easily be compromised at the early stages of their design [19].

Many security measures have been developed to prevent these malicious attacks. The most widely used are as follows:

4.1 Preventive mechanism

In this mechanism technique used are authentication, access control, digital signature and encryption. Also

some other modules including smart card or tokens or biometric verification.

4.2 Reactive mechanism

In this mechanism, the techniques used are like intrusion detection system(IDS) to detect misuse and anomalies, cooperation enforcement mechanisms such as Confidant, Nuglets, CORE and Token-based to reduce selfish node behavior.

5. COUNTER MEASURES AGAINST ROUTING ATTACKS IN MANETS

Here, we shall suggest prevention against the routing attacks and secured routing protocols in MANETs.

5.1 Flooding Attack Solutions

One adaptive technique which has been suggested by DE Silva et al. [23] is to mitigate the effect of a flooding attack in the AODV protocol. This technique uses statistical analysis to detect malicious RREQ floods and block malicious packets. It uses process as suggested by P.Yi, Z.Dai, S.Zhang, Y.Zhong[24] to detect attack but the slight difference between them is that instead of a fixed threshold, this approach determines the threshold based on a statistical analysis of RREQs. The main advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.
Other technique as proposed by V.Balakrishnan [25] is model Fellowship to reduce the flooding and packet drop attacks in MANETs. In this technique some parameters called parameters of Fellowship are defined like Rate Limitation, Enforcement and Restoration. Trust or security protocols are better than Fellowship and improve the security in MANET.

Some router-based Schemes have been proposed to defend against such attacks [36–38], Effectiveness of these schemes may be limited because they cannot be widely deployed to the Internet immediately. Like LFA has been used by attackers to flood selected links of four major Internet exchange points in Europe and Asia [36]

5.2 Worm Hole Attack Solutions

A scheme named Distance bound based Approach has been suggested by R Matam, et al [26].In this approach of Geographical and Temporal packet leashes were introduced first for the detection and prevention of wormholes.

Another technique to overcome Worm Hole Attack is suggested by Gorlatova et al[27].This technique uses the anomaly in the MANET traffic behaviour. Detection of worm holes depends on anomalies in protocol. A simple jitter function is used to set HELLO message interval to 0.3 seconds by randomly adding 0.03 seconds of delay overlaid upon it. The entire Hello message which are received at a particular node, are indexed. Difference between arrival times of HELLO messages is calculated and it is sent to neighbors. The detection of attacker node is done by The HELLO Message Timing Interval HMTI profile obtained. The frequency profile of HMTI is at a set frequency, a violation of OLSR protocol specifications. The packet interval is repeatedly much larger than a genuine mode.

A technique has been proposed by Su et al.[28] on the basis of propagation speeds of requests and statistical profiling. Requests should be transmitted at a higher priority for on demand route discovery schemes that use flooding. Therefore time to exchange information will be increased implicitly among malicious nodes. 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) a distributed and adaptive statistical profiling technique is suggested. Most normal packets remain intact and most falsified packets are filtered as it is based on calculation of different RREQs/RREPs that take varying number of hops and the upper bound on the per hop time of RREQ/RREP packets. In this approach, no network wide synchronized clocks are required and no additional control packet overhead is imposed. A simple calculation is required by the sources or destinations of connections.

A Scheme Proposed by A. Khan et.al NWLID (Normalized Worm-hole Local Intrusion Detection Algorithm) with slight modification in the AODV protocol shows that a single run of algorithm can detect the presence of wormhole peers.[35]

5.3 Blackhole Attack Solutions

A technique is proposedby Tamilsevan et al [32] that the requesting node waits for replies with next hop details from the other neighbouring nodes without sending the DATA packets to the reply node. On receiving the first request, a timer is set in the 'TimerExpiredTable' which is used for collecting the further requests from different nodes. The time of the arrival of the packet and the sequence number is stored in a 'Collect Route Reply Table' (CRRT). The timeout value is calculated on the basis of arriving time of the first route request. Now, if any repeated next hop is found when CRRT is checked then is it assumed that paths are correct and if no repetition occurs then a random route is selected.

M.Patel, et al.[33] have suggested a system used SVM to classify behavior of the nodes. system gather the behaviors of each node in the network and then check behavior of each node and compare it with the threshold values T and validate by the SVM.[33]

Shurman et al. [34] have suggested that the source node has to wait until the RREP packet is received from more than two nodes. When source node receives multiple RREPs it checks about a shared hop. The source node only judges safe route when at least one hop is shared. There is only one drawback of this technique that source node waiting time is increased.

5.4 Node Isolation Attack Solutions

In node isolation attack, attacker node can isolate a specific node and prevent it from receiving any information from other nodes by withholding a TC message in OLSR protocol. A detection technique is proposed by Kannhavong et al.[29] that is based on observation of both a TC message and a HELLO message. This technique proposes that if a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, then that node judges that the MPR node is suspicious and thus it can be avoided from being attacked by selecting other MPR nodes.

5.5 Rushing Attack Solutions

This technique is suggested by Hu et al. [30]. This technique is used to protect against the rushing attack by a set of generic mechanisms: Secure neighbour detection, secure route delegation, and Randomized ROUTE REQUEST forwarding. Secure neighbour detection uses a verification of each neighbour by taking conformation that the other is within a given maximum transmission range. ROUTE REQUEST is forwarded by a node when it receives a delegation message from its neighbour node that lies within its allowable range; it also signs an Accept Delegation message. Traditional duplicate suppression in 'on demand discovery' is replaced by Randomized selection of ROUTE REQUEST message.

5.6 Snare Attack Solutions

Lin et al. [31] suggested a technique that defines snare attack proposed ASRPAKE (An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks) and Decoy node deployment to reduce this attack. This routing protocol compromises five phases namely the key pre-distribution phase, the neighborhood discovery phase, the route discovery phase, the route reverse phase, and the data forwarding phase. Major Concerns of ASRPAKE include security, achievable end-to end anonymity and the integration of the authenticated key exchange operations into the routing algorithm.

6. CONCLUSION

Limited resource capability, bandwidth, power back up and computational capacity is limitations of the MANET. Invisible node attack, no centralized authority, absence of infrastructure, vulnerability of channels and nodes, dynamically changing topology are threats to the security of MANET. In this paper, the challenges and countermeasures of the security threats in mobile ad hoc networks have been overviewed. Identifying new security threats and new countermeasures demand more research in MANET and future research is required for improving the effectiveness of the security schemes and minimizing the cost to suite them for a MANET environment.

REFERENCES

[1] C. E. Perkins, "Ad Hoc Networks", Addison Wesley, 2001.

[2] C. Siva Ram Murthy & B. S Manoj, "Mobile Ad Hoc Networks - Architecture & Protocols", Pearson Education, New Delhi,2004

[3] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[4] J. Jubin and J. Tornow, "The DARPA Packet Radio Network Protocols," Proc. IEEE, vol. 75, no. 1, Jan. 1987, pp. 21-32.

[5] A. J. Tardiff and J.W. Gowens, Editors, "ARL Advanced Telecommunication and Information Distribution Research Program (ATIRP)," Final Report, 1996-2001, June 2001.

[6] T. Plesse, J. Lecomte, C. Adjih, M. Badel, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, and A. Plakoo, "OLSR Performance Measurement in a Military Mobile Ad Hoc Network," Proc. 24th Int'l Conf. on Distributed Computing Systems, 2004, pp. 704-709.

[7] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.

[8] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044.

[9] IEEE Std. 802.11i/D30, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security," 2002.

[10] A.Shevtekar, K.Anantharam, and N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, pp. 363–65, April 2005.

[11] 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, 2005.

[12] B. Kannhavong, H. Nakayama, N.Kato, Y.Nemotoand 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.
[13] 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.
[14]] Y.C.Hu, A.Perrig, and D.B.Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks," Proceedings of 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, vol.3, pp. 1976-1986, April 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] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks," IEEE Network Magazine, vol. 6, no. 13, pp. 24-30, November/December 1999.
[17] T.R.Andel and A.Yasinsac, "The Invisible Node Attack Revisited," Proceedings of IEEE SoutheastCon 2007, pp. 686 – 691, March 2007.
[18] 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, Page(s): 38- 47, ISSN: 1536-1284.
[19] P. Michiardi, R. Molva, "Ad hoc networks security,"IEEE Press Wiley, New York, 2003.
[20] C. Kaufman, R. Perlman, and M. Speciner, "Network Security Private Communication in a Public World," Prentice Hall PTR, A division of Pearson Education, Inc., 2002
[21] IEEE Std. 802.11i/D30, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security," 2002.
[22] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044.
[23] 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.
[24] 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.
[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] R Matam, S Tripathy, in Proceedings of the 8th International Conference on Information Systems and Security. Defence against wormhole attacks in wireless mesh networks (Springer LNCS, Guwahati, 15–19 December 2012), pp. 181–193.
[27] 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.
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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
[33] M.Patel, S.Sharma "Detection of Malicious Attack in MANET A Behavioral Approach" 3rd IEEE International Advance Computing Conference (IACC).pp388-393. 2013
[34] 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.
[35] Aarfa Khan,Shweta Shrivastava, Vineet Richariya "Normalized Worm-hole Local Intrusion Detection Algorithm(NWLIDA)" International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA
[36] S. Lee, M. Kang, and V. Gligor, "Codef: collaborative defense against large-scale link-flooding attacks," in Proc. ACM CoNEXT, 2013.
[37] S. Lee and V. Gligor, "Floc: Dependable link access for legitimate traffic in flooding attacks," in Proc. IEEE ICDCS, 2010
[38] A. Athreya, X. Wang, Y. Kim, Y. Tian, and P. Tague, "Resistance is not futile: Detecting ddos attacks without packet inspection," in Proc. WISA, 2013