A REVIEW ON MANET: ATTACKS ON IT & NEED OF SECURITY

Ashish Aggarwal*

Anshu Chauhan**

Ms. Shabnam Sangwan***

***Abstract*—**

A Mobile Ad hoc (MANETs) is a Dynamic protocol wireless network that can be created without any pre-existing infrastructure in which each node can operate as a router. In MANET's there will be no centralized authority to manage the network. Nodes have to rely on other nodes to keep the network connected. Many routing protocols have been designed and implemented for proper functioning of mobile adhoc networks. The prime objective of these routing protocols is to provide a specific and much effective route in a network. One of the major reasons to address the security aspects in MANETS is the usage of wireless transmission medium, which is highly susceptible or vulnerable to attacks. There is a need to detect and prevent these attacks in a timely manner before destruction of network services. In this survey paper we study the different security attacks to ad-hoc networks and also discussed available solutions.

Keywords— MANET, Security, Attacks, Wireless Networks.

* M. Tech Student, Computer Science & Engineering, MDU, Haryana, India.

** M. Tech Student, Computer Science & Engineering, UPTU, Lucknow (U.P.), India.

*** Assistant Professor, Computer Science & Engineering, Sat Kabir Institute of Technology and Management, MDU, Haryana, India.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of mobile node connected through wireless links. It is dynamic in nature due to topology changes every time. Nodes participating in networking are independent and can freely move. They act as host as well as router. In wired network security protocols will be implemented in router node. But implementing security in MANET is a challenging task. Because here node itself will be acting as a router node. So identifying neighbor node as a legitimate node or malicious node is a difficult thing in MANET.

Characteristics of Ad hoc networks include:

1) Lack of fixed infrastructure: An ad-hoc network is a collection of nodes that do not rely on pre-existing infrastructure for their connectivity. So these types of networks are flexible and easily reconfigurable.

2) Limited resources: Due to lack of fixed infrastructures, these networks have limited resources for their use. Resources like battery power, bandwidth, computation power, memory etc have to be used judiciously for the survival and proper functioning of the network.

3) Dynamic Topology: Nodes in the ad hoc networks are often mobile wireless devices like laptops, PDAs, smart-phones etc resulting in frequent change of their location, resulting in a dynamic topology.

4) Autonomous Networks i.e. stand-alone self-organized system: Due to their decentralized nature, these networks eliminate the complexities of infrastructure setup, enabling devices to create and join networks "on the fly" anywhere, anytime, for any application. A node in the ad hoc networks can communicate with all other nodes which are in its transmission range. Nodes in the network are self-sufficient for the purposes like routing application messages, assuring security of the network and so on.

5) Cost effective: All the above described features make these networks cost effective by removing the necessity of servers, cables for internet connectivity, routers etc.

6) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

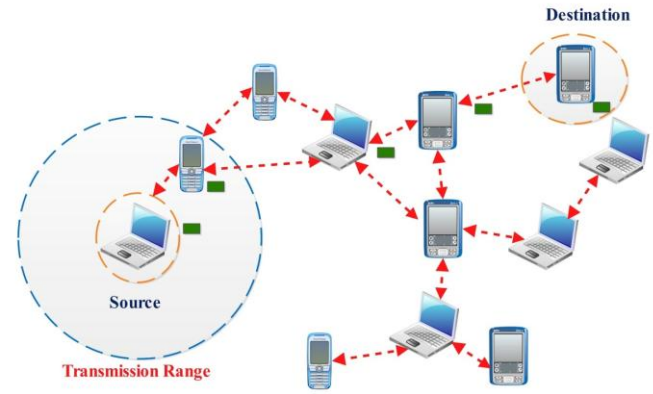

Figure: Mobile Ad Hoc Network

II. MANET APPLICATIONS

Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking, allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

Military battlefield: The modern digital battlefield demands robust and reliable communication in many forms. Most communication devices are installed in mobile vehicles, tanks, trucks etc. Also soldiers could carry telecomm devices that could talk to a wireless base station or directly to other telecom devices if they are within the radio range.

Sensor Networks: This technology is a network Composed of a very large number of small sensors. These can be used to detect any Number of properties of an area. Examples include temperature, pressure, toxins, Pollutions, etc. Applications are the measurement of ground humidity for agriculture, Forecast of earthquakes.

Automotive Applications: Cars should be enabled to talk to the road, to traffic lights, and to each other, forming ad-hoc networks of various Sizes. The network will provide the drivers with information about road conditions, congestions, and accident-ahead warnings, helping to optimize traffic flow.

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld.

Personal Area Network: Personal Area Networks (PANs) are formed between various mobile (and immobile) devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home, for example, but PANs will become more meaningful when connected to a larger network.

III. CURRENT CHALLENGES

Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security and other issues in Manets-

Distributed network: A MANET is a distributed wireless network without any fixed infrastructure. That means no centralized server is required to maintain the state of the clients. Due to lack of centralized management the detection of attacks is very difficult.

Dynamic topology: The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.

Packet Loss: There are many reasons of packet loss problem in Manets. Packet loss may happen due to mobility of nodes, bit rate error, due to interference.

Power awareness: Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life.

No network boundary: Since Manets have no network boundary because the nodes are movable this may lead to increase in number of attacks on them. Any node may enter the network and may hinder the network communication.

Resource Availability: For manets providing secure communication in such a challenging environment where the network is mobile and is vulnerable to attacks requires various resources and architectures [9].

Addressing scheme: The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology requires a ubiquitous addressing scheme, which avoids any duplicate addresses. In wireless WAN environments, Mobile IP [10] is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.

Variation in nodes: Each node has different transmission and receiving capabilities. In addition each mobile node has different software/hardware configurations which cause trouble in operating in a network. [1]

Security: Security in an ad hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation - are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

Network size: The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

IV. CATEGORIZING NETWORK ATTACKS

A survey of available attacks reveals a list of MANET attacks, both applied and theoretical. There are different types of attacks which are vulnerable to manets and which are active at different layers of network.

Active Attacks: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network.

1. **Wormhole Attack** – a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node.

2. Sinkhole: It is a service attack that prevents the base station from obtaining complete and correct information [8]. In sinkhole attack, a compromised node tries to attract the data to it from his all neighboring node. Selective forwarding, modification or even dropping of data can be done by the sinkhole attack [11].

3. Sybil Attack: In Sybil attack, attacker pretends to have manifold identities or nodes. A malicious node can act as if it were a multiple number of nodes either by impersonating other nodes or simply by claiming false identities. This allows him to forge the result of a voting used for threshold security methods for more information.

4. Denial of service – DOS is one of the most studied attack as it can be launched at any layer of the network. In this attack the communication signal is jammed which disrupts the normal communication process. It can be carried out in many ways. It can be achieved by transmitting false routing packets or by flooding the routing packets to any intermediate node so that normal communication is no longer done. This attack basically hinders the availability of a node or even the entire network.

5. Spoofing – The spoofing attack occurs when a malicious node pretends other node's identity at times. This in turn misguides a non malicious node in order to alter the vision of the network topology that it can gather.

Passive Attacks: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected.

1. Traffic Analysis: In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis.

2. Eavesdropping: It aims to obtain some confidential information that should be kept secret during the communication. The 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.

3. Cryptographic attacks – Cryptography provides security to the network and is also considered as a powerful tool to maintain confidentiality and authentication of the information which is to be send. It also hinders the illegal access of data by attackers by its key management system .These types of attacks include digital signature attack, pseudorandom number and hash collision attacks.

4. Monitoring: Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

Few Advance Attacks:

1. Replay Attack: It is a network attack in which a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. Suppose node S want to send some data to R. For this S has to prove his identity to R. This way S sends his password to R for identification. At that time, an attacker an intercept the password of S and a presenting itself as S, when asked for the proof of identity.

1. Black hole Attack – In this attack, malicious nodes trick all their neighboring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes.

3. Byzantine Attack – In Byzantine attack there is a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

4. Location Disclosure Attack: Malicious node collects the information about the node and about the route by computing and monitoring the traffic. This way malicious node may perform more attack on the network [12].

5. Rushing Attack: In rushing attack, an attacker comes between the route of sender and receiver. When sender send packet to the receiver, then attacker intercept the packet and forward to receiver. Attacker performs duplicate suppression mechanism and then sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so that receiver will be busy continuously. This way, it reduces the efficiency of receiver [7].

V. SECURITY IN MANET

Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of interrouter authentication prior to the exchange of network control information. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure based authentication

mechanisms will be explored by the group. As an adjunct to the working groups efforts, several optional authentication modes may be standardized for use in MANETs.

Security Requirements of Ad-Hoc Network are:

• Route signaling can't be spoofed

• Fabricated routing messages can't be injected into the network

• Routing messages can't be altered in transit

• Routing loops can't be formed by through malicious action

• Routes can't be redirected from the shortest path by malicious action

• Unauthorized nodes should be excluded from route computation and discovery.

The following are five major security goals which require prevention from attacks are:

Confidentiality: It ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

Integrity: It ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

Authentication: It enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

Non-Repudiation: It ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

Availability: It guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

VI. CONCLUSION

Due to nature of mobility and open media wireless, Ad-hoc network are much more prone to all kind of security risks as covered. As ad hoc networks are vulnerable to many types of attacks the

security of this network is a major issue. Many researchers are trying to prevent the attacks done on ad-hoc networks at various levels. A variety of such attacks have been discussed. We have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. As a result, the security needs in the wireless Ad-hoc network are much higher than those in the traditional wired networks.

VII. REFERENCES

[1] Imrich chlamtac , marco conti, jennifer j.-n. liu "mobile ad hoc networking: imperatives and challenges" in proceedings of 2003 elsevier.

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Carde "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" in proceedings of WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - – °c 2006 Springer.

[3] Shushan Zhao, Akshai Aggarwal , Richard Frost, Xiaole Bai , A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks , IEEE communications surveys & tutorials, vol. 14, No. 2, Second Quarter 2012.

[4] Lu Li, Ze Wang, Wenju Liu and Yunlong , A Certificate less Key Management Scheme in Mobile Ad Hoc Networks , 2011 IEEE.

[5] A.Rajaram , Dr.S.Palaniswam, A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks , International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5, July 2010.

[6] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks ," Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[7] S. Albert Rabara1 and S.Vijayalakshmi2, "Rushing Attack Mitigation In Multicast MANET (RAM3)", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 4, December 2010.

[8] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless, Sensor Networks; the Intruder Side". Athens Information Technology, 19002 Peania, Athens, Greece.

[9] Priyanka Goyal, Vinti Parmar, Rahul Rishi " MANET: Vulnerabilities, Challenges, Attacks, Application" in proceedings of IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[10] C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, May 2004, ISBN 013147023X.

[11] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. "An Overview Of security Problems in MANET".

[12]K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[13] Pradeep Kumar, A. K. Vatsa, (2011) "Novel Security Architecture and Mechanism for Identity based Information Retrieval System in MANET", International Journal of Mobile Adhoc Network|, Vol.1,No.3.