Research Paper Computer Science

Study on Security Issues & Challenges in MANET

Dr. Banta Singh Jangra | Asstt. Professor, Deptt. Of Computer Science, FGM Govt. PG College, Adampur (Hisar) Haryana, India

Manish Kumar Naga | Research Scholar, PhD-Computer Science, Deptt. Of Computer Science, Jyoti Vidyapeeth Women University, Jaipur, Rajasthan, India

ABSTRACT

Ad hoc network is a group of nodes that is associated through a wireless medium forming swiftly varying topologies. Attacks on ad hoc network routing protocols interrupt network routine and consistency with their solution. In this paper we have discussed about challenges and authentication in ad hoc network. A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi -hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is rapidly thinning out for, security challenges have become a primary concern to make available secure communication. In this paper, we are trying to examine and revise the MANET issues, characteristics, challenges application, security goals and different type's security attacks at different layers.

KEYWORDS MANETS, Hop, Ad-hoc Networks, Routing, Topology, Routing Protocols.

INTRODUCTION-

An Adhoc network is a assortment of mobile nodes forming a temporary network without any supplementary infrastructure and no centralized control. Wireless networks consist of a number of nodes which communicate with each Other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, Cellular networks and satellite networks. . Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movablity and organize themselves arbitrarily.

This means that the topology of the ad hoc network changes dynamically and unpredictably. Adhoc network can be created on the fly, each node in the Adhoc network acts both as a router and host. The Adhoc networks can adjust its topology dynamically. Attacks from both external and internal nodes can easily affect the stability of the ad hoc networks. A new alternative way for mobile communication, in which mobile devices form a self creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program. Ad hoc networks have played an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available. The other type of wireless network, infrastructure less networks, is knows as Mobile Ad-hoc Networks (MANET). These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. Nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and requires an extremely flexible technology for establishing communications in situations which demand a fully decentralized

Network without any fixed base stations, such as battlefields, military applications, and other emergency and disaster situations. Since, all nodes are mobile; the network topology of a MANET is generally dynamic and may change frequently. Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, Direct single-hop transmissions between two hosts can require significant power, causing interference with other such transmissions.

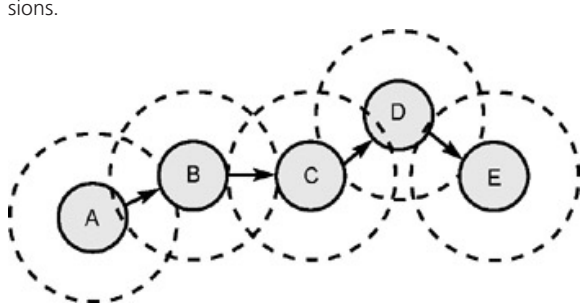

Figure1: Communication in MANET

Background

The definite features of MANETs present a challenge for security solutions. Many obtainable security solutions for conventional networks are unproductive and incompetent for many envisaged MANET consumption environments. As a result, researchers have been working for the last decade on emergent new security solutions or varying current ones to be relevant to MANETs. Since many routing protocols do not think about security, some research focuses on developing secure routing protocols or introducing security extensions to the accessible routing protocols. Routing protocols have been projected to counter selfish activities by forcing the selfish nodes to collaborate. Accessible key management mechanisms are regularly based on central points where services such as guarantee authorities or key servers can be placed. Since MANETs do not

have such points, new key management mechanisms have had to be developed to accomplish necessities. Lastly, since avoidance techniques are perpetually restricted in usefulness, interruption recognition systems are usually used to harmonize other security mechanisms. This applies to MANETs too and researchers have planned new IDSs to identify spiteful behavior on these networks. If we are to expand more universal solutions we must first have a inclusive understanding of probable vulnerabilities and security risks in opposition to MANETs. They distribute the vulnerabilities of wired networks, such as eavesdropping, denial of service, spoofing and the like, which are accentuated by the ad hoc situation. They also have additional vulnerabilities such as those that take benefit of the supportive nature of routing algorithms.

MANET ISSUES
In this segment the MANET research issues are discussed and classified. Various essential and recurrently discussed aspects of MANETs are identified and grouped -:

1) Routing:
Routing is an indispensable practice in this field, for the reason that changes in group topology happen regularly. A well-organized routing protocol is requisite to cope with highly fluid network conditions.

2) Multicasting/ Propagation:
Multicast service supports users communicating with other members in a multicast group. Broadcast service supports users communicating with all members on a network.

3) Location Information:
Location information uses the Global Positioning System (GPS) or the network-based geo-location practice to get hold of the physical location of a target.

4) Clustering:
Clustering is a method to division the hosts into numerous clusters and provides a suitable structure for resource organization, routing and virtual circuit hold up.

5) Mobility Management:
In the ad-hoc network environment, mobile hosts can travel unobstructed from place to place. Mobility management handles the storage, maintenance and recovery of the mobile node location information.

6) TCP/ UDP:
TCP and UDP are the regular protocols used in the Internet. Data application successively over MANETs, such as http and real audio require transport layer protocols like TCP and UDP to launch packets above the links.

7) IP Addressing:
One of the most significant issues is the set of IP addresses that are assigned to the ad-hoc network. IP addressing and address auto Configuration have paying attention in MANETs.

8) Multiple Accesses:
A major issue is to expand resourceful medium access protocols that optimize ghostly reuse, and therefore, capitalize on collective channel consumption in MANETs.

9) Radio Interface:
Mobile nodes rely on the radio interface or antenna to broadcast packets. Packet forwarding or getting via radio interface or antenna techniques in MANETs are helpful investigations.

10) Bandwidth Management:
Bandwidth management in MANETs is a classic classification. Because the bandwidth is typically inadequate, efficiently supervision and using it is a very significant subject.

11) Power Management:
A power management approach would help reducing power consumption and hence prolonging the battery life of mobile nodes. Because most devices operate on batteries, power management becomes an important issue.

12) Security:
The mobile nodes in MANETs are extremely vulnerable to spiteful injure. Security issues are important in MANETs to avoid possible attacks, threats and system vulnerabilities.

13) Fault Tolerance:
This issue involves detecting and correcting faults when network failures happen. Fault-tolerance techniques are bring for preservation when a breakdown occurs during node faction, joining, or send-off the network.

14) QoS/ Multimedia:
Quality of Service (QoS) and Multimedia necessitate sky-scraping bandwidth, low delay, and high reliability.

15) Standards/ Products:
The standards and products issues that permit the expansion of small scale are promising for this field. For example, Bluetooth is a low-cost technology designed for short-range communication techniques.

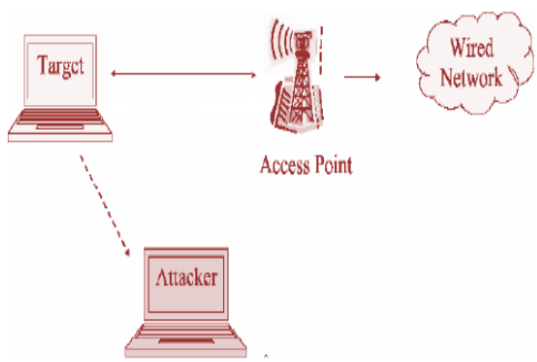

Figure2.Adhoc Network

5. Advantages, Applications & characteristics of Adhoc Networks

A. Advantages of MANETs:
The benefits of an Adhoc-network include the following:

- Linking to files on other computers and the Internet exclusive of the need for a wireless router is the most important advantage of via ad hoc network. Because of this, running an Adhoc network can be more affordable than a traditional network.
- Adhoc networks can be shaped on the fly in almost any condition where there are multiple wireless devices.
- Creating an Adhoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an Adhoc network is a perfect way out.
- Enhanced flexibility.
- Scalable because it accommodates the addition of more nodes.
- Robust due to decentralize administration.

B. Applications of MANET It includes:
a) Military Battlefield
b) Sensor Networks
c) Personal Area Network
d) Medical Service
e) Commercial Sector

C. Characteristics of MANET
Adhoc networks have some characteristics which make them dissimilar from wired and wireless networks. They are as follows Security Aspects and Challenges in Mobile Adhoc Networks.

1. Mobility Induced Link Breakages: As the nodes in an Adhoc network are usually mobile, the nodes may go out of range of neighboring nodes resulting in break in the links between the nodes. These may leads to break in the route between source and destination nodes.

2. Sleep Period of Process: To preserve energy, nodes in an Adhoc network may enter inactive state whereby they do not transmit at some instants of time.

3. Highly unfavorable environmental conditions: Adhoc networks are generally used in environments which are highly unfavorable for transmission and reception

4. Looping Problem: Due to mobility temporary loops may result.

5. Misbehavior: Some nodes may misbehave transmitting their own data and refusing to broadcast data from other nodes. Since Adhoc network uses multi hop routing this has to be controlled.

6. SECURITY CHALLENGES AND GOALS IN AD HOC NETWORKS

A. MANET Challenges

Vulnerability of Channels: As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

Vulnerability of nodes: Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be captured and fall under the control of an attacker.

Absence of Infrastructure: Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable.

Dynamically Changing Topology: In mobile ad hoc networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an additional challenge. A particular difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

For high survivability Ad hoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the dynamic and not static and should be scalable.

B. Goals/Requirements of a Security System

C. Security is a significant issue for Adhoc networks, more than ever for those security-sensitive applications. To protect an ad hoc network, we believe in the following attributes:

Availability: Ensures survivability despite Denial of Service (DOS) attacks. On physical and medium access control layer attacker can employ jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

Confidentiality: Ensures confident information is never disclosed to illegal entities.

Integrity: Message being transmitted is never ruined.

Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would pretend to be a node, thus gaining unauthorized access to resource and responsive information and intrusive with procedure of other nodes.

Non-repudiation: Ensures that the origin of a message cannot reject having sent the message.

Non-impersonation: No one else can imagine being another allowed member to find out any helpful information.

Attacks using fabrication: Creation of fake routing messages is termed as fabrication messages. Such attacks are complicated to notice routing.

Layer	Attacks
Application Layer	Data corruption, Viruses & worms.
Transport Layer	TCP/UDP SYN flood
Network Layer	Hello flood, blackhole
Data Link Layer	Monitoring, traffic analysis
Physical Layer	Eavesdropping, active interference

Table1: Some attacks on Protocol Stack

7. ATTACK ON AD HOC NETWORK--

There are various types of attacks on ad hoc network which are describing following:

Location Disclosure: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

Black Hole: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Wormhole: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private Communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender .An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful In such cases since it binds a node to the messages it generated.

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture.. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the par-

ticipating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Routing Table Poisoning: Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes.

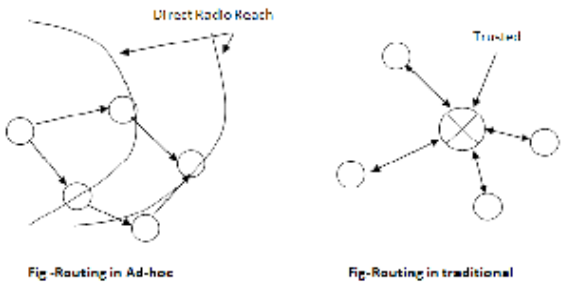

Figure 3: Network Using Router

For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

Rushing Attack: Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. Develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

Breaking the neighbor relationship: An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.

Masquerading: During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

Passive Listening and traffic analysis: The intruder could passively gather exposed routing information. Such a attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of Protocol.

8. Conclusion and Future Scope

The speedy development in the ground of mobile computing is pouring a new substitute for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. Its fundamental suppleness, lack of infrastructure, ease of deployment, auto-configuration, low cost and potential applications makes it an essential part of expectations pervasive computing environments. As a result, the seamless combination of mobile ad hoc networks with other wireless networks and fixed infrastructures will be an indispensable part of the development towards future fourth generation communication networks. From a industrial point of view, the awareness of this visualization still requires a large number of challenges to be solved connected to devices, protocols, applications and services. The concise discussion in this paper shows that, despite the large labors of the MANET investigate community and the speedy advancement made all through the last years, a lot of tricky technological issues leftovers unanswered. From an economical point of view, mobile ad hoc networks unlock up innovative business opportunities for telecom operators and service providers. To this conclusion, suitable business scenarios, applications and economical models need to be acknowledged, together with technological advances, making a changeover of ad hoc networks to the marketable world feasible.

MANET is additional exposed to many attacks due to dynamic topology, distributed operation and restricted bandwidth. In this paper we have studied MANET and its characteristics, advantages, application, security goals and a variety of security attacks in its routing protocols.

REFERENCES

IEEE Std 802.11 – 1999: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, Inst. Elec. Electron. Eng., New York, USA, 1999.ISBN 0-7381-1658-0 | | [2] IPN Progress Report, August 15, 2002, Analysis of Energy Consumption for Ad Hoc Wireless Sensor Networks Using a Bit-Meter-Per-Joule Metric, J.L.Gao | | [4] M. Satyanarayanan. Fundamental challenges in mobile computing. Submitted paper. | [5] M. Haardt W. Mohr R. Becher, M. Dillinger. Broadband | Wireless access and future communication networks. Proceedings of the IEEE, 89(1), 2001. | | [6] David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996. | [7] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). Internet-Draft, draft-ietf-manet-dsr-07.txt, February 2002. Work in progress. | [8] Stephen Kent, Charles Lynn, Joanne Michelson, and Karen Seo. Secure Border Gateway Protocol (S-BGP)—Real World Performance and Deployment Issues. In Symposium on Network and Distributed Systems Security (NDSS'00), pages 103–116, February 2000. | [9] Stephen Kent, Charles Lynn, and Karen Seo. Secure Border Gateway Protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 18(4):582–592, April 2000. | [10] Young-Bae KO and Nitin Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98), pages 66–75, October 1998. | [11] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. In 9th International Conference on Network Protocols (ICNP'01), 2001. | | [12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003. To appear. | [13] Yih-Chun Hu, Adrian Perrig, David B. Johnson Ariadne: "A Secure On-Demand Routing Protocol for Ad Hoc Networks" MobiCom'02, September 23–26, 2002, Atlanta, Georgia, USA. | [14] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA. | [15] Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93-B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004. | [16] S.W. Smith, "A Case (Study) For Usability in Secure Email Communication" IEEE Computer Society 2007 | [17] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005 | [18] S.Chessa, P.Santi, "Comparison Based System-Level Fault Diagnosis in Ad-Hoc Networks", Proc. IEEE 20th Symp. On Reliable Distributed Systems (SRDS), New Orleans, pp. 257-266, October 2001 |