Chief Editor
Dr. A. Singaraj, M.A., M.Phil., Ph.D.
Editor
Mrs.M.Josephin Immaculate Ruba

Editorial Advisors

1. Dr.Yi-Lin Yu, Ph. D
   Associate Professor,
   Department of Advertising & Public Relations,
   Fu Jen Catholic University,
   Taipei, Taiwan.
2. Dr.G. Badri Narayanan, PhD,
   Research Economist,
   Center for Global Trade Analysis,
   Purdue University,
   West Lafayette,
   Indiana, USA.
3. Dr. Gajendra Naidu.J., M.Com, LL.M., M.B.A., PhD. MHRM
   Professor & Head,
   Faculty of Finance, Botho University,
   Gaborone Campus, Botho Education Park,
   Kgale, Gaborone, Botswana.
4. Dr. Ahmed Sebihi
   Associate Professor
   Islamic Culture and Social Sciences (ICSS),
   Department of General Education (DGE),
   Gulf Medical University (GMU), UAE.
5. Dr. Pradeep Kumar Choudhury,
   Assistant Professor,
   Institute for Studies in Industrial Development,
   An ICSSR Research Institute,
   New Delhi- 110070.India.
6. Dr. Sumita Bharat Goyal
   Assistant Professor,
   Department of Commerce,
   Central University of Rajasthan,
   Bandar Sindri, Dist-Ajmer,
   Rajasthan, India
7. Dr. C. Muniyandi, M.Sc., M. Phil., Ph. D,
   Assistant Professor,
   Department of Econometrics,
   School of Economics,
   Madurai Kamaraj University,
   Madurai-625021, Tamil Nadu, India.
8. Dr. B. Ravi Kumar,
   Assistant Professor
   Department of GBEH,
   Sree Vidyanikethan Engineering College,
   A.Rangampet, Tirupati,
   Andhra Pradesh, India
9. Dr. Gyanendra Awasthi, M.Sc., Ph.D., NET
   Associate Professor & HOD
   Department of Biochemistry,
   Dolphin (PG) Institute of Biomedical & Natural Sciences,
   Dehradun, Uttarakhand, India.
10. Dr. D.K. Awasthi, M.SC., Ph.D.
    Associate Professor
    Department of Chemistry, Sri J.N.P.G. College,
    Charbagh, Lucknow,
    Uttar Pradesh. India

ISSN (Online) : 2455 - 3662
SJIF Impact Factor :3.395 (Morocco)

EPRA International Journal of

Multidisciplinary Research

Volume: 2 Issue: 8 August 2016

Published By :
EPRA Journals

CC License

EPRA International Journal of Multidisciplinary Research (IJMR) ISSN (Online): 2455-3662

SJIF Impact Factor: 3.395 (Morocco) Volume: 2 Issue: 8 August 2016

RELEVANCE OF MANET IN WIRELESS ADHOC NETWORK

Sapna Khatter[1]

[1]Lecturer,
Computer Department
Christ Polytechnic Institute
Rajkot, Gujarat, India

Nymphea Gogia [2]

[2] Principal,
Electronics and Communications Department
Christ Polytechnic Institute
Rajkot, Gujarat, India

ABSTRACT

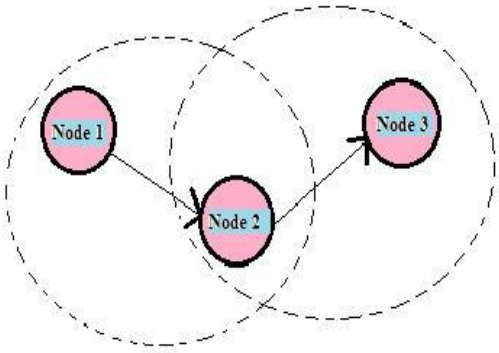
The Enhancement in Wireless Communication have given rise to several Wireless Networks like Mobile Adhoc Networks (MANETS), Wireless Sensor Networks and numerous more. Mobile Adhoc Network (MANETs) is a group of mobile nodes which are connected by a wireless medium, without having necessity of a centralized authority. MANET is an "infrastructure less" dynamic adhoc network which includes collection of wireless mobile nodes that communicate with each other without any centralized entity. Considering the fundamental and unique properties of MANET like wireless medium, dynamic topology, shared physical medium, distributed operations, MANET is vulnerable to varieties of security attacks like worm hole, black hole, rushing attack etc. In this paper review about mobile adhoc network, its characteristics, challenges, applications, and distinct type of security attacks at different layers are generated.

KEYWORDS: *MANET, Mobile Adhoc Network, Blackhole, rushing attack, Jamming, Eavesdropping, Dropping Attack.*

I. INTRODUCTION

MANET actually stands for Mobile Adhoc Network. MANET is the local area network created with a collection of mobile nodes. MANET is a wireless network, so there is no need of physical infrastructure. MANET is a set of autonomous mobile nodes that communicate with each other via radio waves. The wireless mobile nodes that are in radio range of each other can directly communicate with each other whereas the nodes that are not in the radio range needs intermediate nodes to route their packets. Each of the node has a wireless route to communicate with each other. MANET is wireless, infrastructure less, so can be worked from any place without any help of access points or base stations.

Devices in MANETs should be capable of detecting the presence of other devices and creates mandatory set up to facilitate communication and sharing of data and service. Ad hoc networking permits the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Because of nodal mobility, the network topology may change rapidly and unpredictably over time.



Above Figure depicts the adhoc network with three nodes, of which node1 and node2 are in then radio range while node1 and node3 are not in the radio range of each other, so node3 can be used to forward information between node1 and node2. Here node2 acts as a router to route packets between node1 and node3 and all three nodes together forms an adhoc network. Adhoc network is the combination of mobile computers and systems which is actually temporary formed networks and exchange data through radio waves or any other satellite technology.

II.PROPERTIES OF MANET

1)Infrastructure -less: - MANET does not require any well-equipped infrastructure or any central administration.

2)Autonomous: - MANET is a set of autonomous mobile nodes that communicate with each other via wireless

medium called radio waves. The wireless mobile nodes that are not in radio range of each other can act as an independent router and every node can generate independent data.

3)Multi-Hop Routing: - In Multi-hop routing no default routers are available, so every node can act as a default router and their function is to route packets from one node to another.

4)Dynamic Topology: - The wireless mobile nodes in MANET dynamically establishes routing among themselves, creates their own network, moves arbitrarily and so the network topology changes randomly and unpredictably.

5)Light –weight Nodes: - In most of cases, the nodes in MANET are mobiles with less CPU capability, low power storage and small memory size.

6)Shared Physical Medium: - The wireless communication medium is accessible to any entity with the required equipment's and adequate resource, so access to the channel cannot be restricted.

7)Link and Node's Varying Capability: - Each nodes contains different capabilities for transmission/receiving and operates across different frequency bands which results in possibly asymmetric links. In addition to this each wireless node might have different hardware/software configurations with varying processing capabilities. Developing network protocols and algorithms for this heterogeneous network can be complex, which requires dynamic adaptation to the varying conditions like traffic load distribution variations, channel conditions, congestion etc. As each of the mobile node is acting both as the end system and router, additional energy is required to forward packets from other nodes.

III.MANET CHALLENGES

1)Autonomous: - The operation of various wireless mobile nodes can be managed and works independently without the use of centralized authority.

2)Device Discovery: - To facilitate automatic optimal route selection, dynamic updation is necessary and can be done by identifying new wireless moved in nodes and informing about their existence.

3)Limited Bandwidth: - MANET is wireless adhoc network which simply means significantly lower capacity than the wired network and in addition the throughput of wireless communication after calculating for effect of overhead (noise, fading, interference condition) is significantly less than the radio's maximum transmission rate.

4)Dynamic Topology: - Because of dynamic topology, the trustable relationship among nodes cannot be created.

5)Routing Overhead: - In MANET topology changes frequently, so maintaining the information of topology at all nodes involves overhead which results in wastage of bandwidth.

6)Scalability: - when the number of wireless nodes increases, is network able to provide the acceptable level of service, refers to as scalability.

7)Hidden terminal issue: - The hidden terminal issue means the collision of packets at a receiving node due to the concurrent transmission of those mobile nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

8)Battery Constraints: - Devices used in these wireless networks have restrictions on the power source in order to maintain portability, size, storage capacity and weight of the device.

9)Poor Transmission Quality: - Mobile Ad hoc wireless networks experience a much higher packet loss due to factors such as increased collisions because of presence of hidden terminals, presence of interference, uni-directional links, constant path breaks due to mobility of nodes.

IV.MANETs VULNERABILITIES

The Weak spot of any security system is vulnerability. To allow data access, the system must verify user's identity otherwise the particular system would be vulnerable to unauthorized data manipulation. MANET is more vulnerable than a wired network. Vulnerabilities of MANET are as follows:

1)Absence of centralized management: - MANETs does not have any centralized authority for monitoring. Because of lack of management makes the detection and identification of attacks difficult because it is not easy to monitor the traffic in a fully dynamic and large scale adhoc network.

2)No predefined Boundary: - Boundaries are not available in Mobile Ad-hoc Network. The nodes join and leave the wireless network in a roaming environment. When any of the node enters into the network radio range, it will be automatically able to communicate with other nodes in the network.

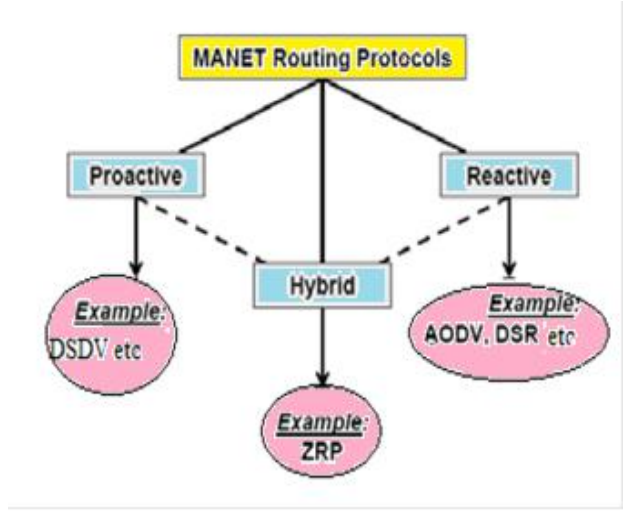
3)Cooperativeness –MANET's routing algorithm usually believes that nodes are totally cooperative and non-malicious. As the result a malicious attacker can easily become an important routing agent and can disrupt network operation.

4)Limited Power supply: - The major and severe problems in mobile ad-hoc network are caused by restricted power supply because nodes in MANET's have limited power supply. when power is limited the nodes may behave in the selfish manner.

5)Adversary inside the Network: - The mobile nodes in the network can join any time and leave anytime the wireless radio network. Wireless mobile nodes also behave malicious in network range.so there are no means to identify whether the node behaviour is malicious or not. Hence internal attacks are more dangerous than external attacks.

VMANETs ROUTING PROTOCOLS

Mobile Adhoc routing protocols are divided into three main categories; Proactive, Reactive and Hybrid protocols as shown in above figure.



1)Proactive Protocols: - proactive protocols are table driven routing protocols. In proactive routing, one or more tables are maintained by each node to store routing information and any changes in network topology needs to be send back by broadcasting updates throughout the network in order to maintain a consistent network view. Example Destination Sequenced distance vector(DSDV) which is the conventional routing scheme, which maintains up-to-date and consistent information of the entire network. This scheme minimizes the delay in communication and allow nodes to quickly determine which of nodes are available or reachable in the network.

2)Reactive Protocols: - On demand routing protocol also known as reactive routing protocols doesn't need to maintain routing information or routing information at the network nodes if there is no communication. If a mobile wireless node wants to send a packet to another mobile node, then this scheme finds for the route in an on-demand manner and initiates the connection in order to transmit and receive the packet. The route locating occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR).

3)Hybrid Protocols: -Hybrid model means combination of reactive and proactive routing protocols. The network that is divided into zones is a hybrid routing protocol know as Zone Routing Protocol. ZRP gives hybrid architecture where additional topological information is maintained by each node which requires extra memory.

VI. CLASSIFICATION OF SECURITY ATTACKS

Attacks can be categorized into passive or active attacks on basis of their behaviour.

1) Passive attacks: - A passive attack does not change the data propagated within the network. But it involves the unauthorized "observing" to the network traffic or gathers data from it. Passive attacker does not interrupt the working of a routing protocol but tries to locate the important information from routed traffic.

2) Active attacks: - Active attacks are very critical attacks on the network that block message flow between the nodes. Moreover, active attacks can be internal or external. Active external attacks can be transferred by outside sources that are not part of network. Internal attacks are from malicious nodes which belong to network, internal attacks are more critical and tuff to detect than external attacks. These attacks create unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. Active attacks can be classified into following groups:

1) Dropping Attacks: - Compromised nodes or selfish nodes can put all packets that are not destined for them. Dropping attacks can block end-to-end communications between nodes.

2) Modification Attacks: - These attacks modify packets and interrupt the entire communication between nodes in network. Sinkhole attacks are the example of modification attacks.

3) Fabrication Attacks: - In fabrication attack, the attacker sends fake message packet to the adjacent nodes without receiving any related message packet. The properties of MANETs make them vulnerable to many new attacks. These attacks can occur in various distinguish layers of the network protocol heap.

A. Attacks at Physical Layer

Few of the attacks that are identified at physical layer include eavesdropping, interference, and jamming etc.

1) Eavesdropping: - It can be defined as interception and reading of messages and conversations by unintended receivers. The main objective of such attacks is to gather the confidential information that should be kept secret during the communication.

2) Jamming: - Jamming is a special and important class of DoS attacks which are started by malicious node after determining the frequency of communication. Jamming attacks also blocks the reception of legitimate packets.

3) Active Interference: - An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications.

B. Attacks at Data link layer

The data link layer can classify attacks as to what effect it has on the state of the network as a whole.

1) Selfish Misbehaviour of Nodes: - The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and to conserve of battery power.

2) Malicious Behaviour of Nodes: - The main purpose of malicious node is to interrupt normal operation of routing protocol. The impact of such attack is raised when the communication takes place between neighbouring nodes. Attacks of such types falls into following categories.

3) Denial of Service (DoS): - The prevention of authorized access to resources or the delaying of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent authorized users of a service from using the desired resources and attempts to "overflow" a network, thereby preventing legitimate network traffic.

4) Misdirecting traffic: - A malicious node advertises wrong routing information in order to get secure data before the actual route.

5) Attacking neighbour sensing protocols: -malicious nodes advertise fake error messages so that important links interface is marked as broken.

C. Attacks at Network Layer

The main goal in network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

1)Blackhole Attack: - In Networks Black holes refers to places in the network where incoming traffic is dropped without informing the source that the data didn't reached its intended recipient. In Blackhole attacks a node uses the protocol and advertise itself as having the shortest path to the destination node where the packet is destined to.

2)Grey hole Attack: - Grey hole is a node that can switch from behaving correctly to behaving like a black hole. This is done to avoid detection.

3)Wormhole Attack: - In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network. Wormhole attacks depend on a node misrepresenting its location. Hence location based routing protocols have the potential to prevent wormhole attacks.

4)Rushing Attack: - In rushing attacks when compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet.

5)Sinkhole Attack: - In Sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic, it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node attempts to attract the secure data from all neighbouring nodes.

D. Attacks at Transport Layer

1)Session Hijacking: - Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks.

E. Attacks at Application Layer

1)Malicious code attacks: - Malicious code attacks include, Viruses, Worms can attack both operating system and user application.

VII.MOBILE ADHOC NETWORK APPLICATIONS

Application	Possible scenarios/services
Academics	Universities campus settings colleges/school campus settings Virtual classrooms In meeting or lectures that can use adhoc communications.
Military communication	Network between the soldiers, their vehicles and head quarter for military information. Automated battlefields
Entertainment	Multi users Games Internet Access outside Wireless P2P networking Theme Park
Emergency Services	Search and rescue operations Disaster relief efforts like fire, flood or earthquake Replacement of fixed infra structure in case of environmental disasters Supporting doctors and nurses in hospitals Policing and Fire Fighting
Home and Enterprise Networking	Wireless Networking used in Home and Office Meetings and Conferences Personal networks (PN), Bluetooth Construction site that uses networks.
Commercial use	E-commerce: electronic payments can be done from anytime and anywhere Business: Access database dynamically, mobile offices
Civilian Environments	Sports Stadium, shopping mall, trade fair Network of visitors at airport Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks
Wireless Sensor Networks	Home applications: smart sensors and actuators embedded in consumer electronics. Data tracking of environmental conditions, chemical/biological detection
Context aware services	Follow-on services: call-forwarding, mobile workspace Information services: location specific services, time dependent services
Coverage extension	Extending cellular network access Linking up with the Internet, intranets, etc.

VIII.CONCLUSION

The Enhancement in the area of wireless networking is driving a new alternative way for mobile communication, in which wireless mobile nodes form a self-creating, self-organized, self-configuring, self-routed, self-administrating wireless network called a mobile adhoc network. Mobile adhoc networks are generally more vulnerable to physical security threats than fixed or hard-wired or infra structure – less networks. This review throws a light on different concepts of MANETs which includes its properties, challenges, vulnerabilities, applications, different kind of security attacks at various layers. Because of dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to attacks. Its inherent flexibility, infrastructure-less, ease of deployment, self and auto configuration, cheap cost and potential applications make it a necessary part of future pervasive computing environments. As the invention goes on, especially the need of dense deployment such as battlefield and sensor networks, the mobile nodes in mobile ad-hoc wireless networks will be smaller, cheaper, more capable, and will come in variety of forms.

In all, although the widespread deployment of ad- hoc networks is still year away, the research in this field will continue being very active and imaginative.

IX.REFERENCES

1. *Mahima Chitkara, Mohd. Waseem Ahmad," Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 2, February 2014, pp..432 – 437.*
2. *Mr. L Raja, Capt. Dr. S Santhosh Baboo," An Overview of MANET: Applications, Attacks and Challenges", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 1, January 2014, pp.408 – 417.*
3. *Anuj Rana, Sandeep Gupta," Review on MANETs Characteristics, Challenges, Application and Security Attacks", International Journal of Science and Research (IJSR), Volume 4 Issue 2, February 2015, pp.2203-2208.*
4. *Priyanka Goyal, Vinti Parmar, Rahul Rishi," MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, pp.32-37.*
5. *Aarti, Dr. S. S. Tyagi," Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 252-257.*