ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

The Technological Challenges of Mobile Ad-Hoc Network

G.Nathiya[1], A.Kiruthika[2], A.Aruna[3]

PG Scholar, Department of CS & IT, Dhanalakshmi Srinivasan College of Arts & Science for Women, Perambalur, Tamil Nadu, India[1,3]

Assistant Professor, Department of CS & IT, Dhanalakshmi Srinivasan College of Arts & Science for Women, Perambalur, Tamil Nadu, India[2]

ABSTRACT: Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. This paper provides insight into the potential applications of ad hoc networks, various attacks and discusses the technological challenges that protocol designers and network developers are faced with.

KEYWORDS: Mobile device, Wireless, Network, Attacks, Protocol.

I. INTRODUCTION

MANET is a self configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET. MANET have given rise to many applications like Tactical networks, Wireless Sensor Network, Data Networks, Device Networks, etc. With many applications there are still some design issues and challenges to overcome. The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes which may be combined routers and hosts--they form the network routing infrastructure in an ad hoc fashion. Lot of security vulnerabilities in a wireless environment, such as MANET, has been identified and a set of countermeasures were also proposed. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge. Taking these factors into concern, the main vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. MANETS are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETS consist of a peer-to-peer, self-forming, self-healing network. MANETS circa 2000-2015 typically communicate at radio frequencies (30 MHz -

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

5 GHz).System supports mobile ad hoc network ,point-to-point and point-to-multipoint network configuration with one waveform. Coverage 0-30km depending on antenna configuration, antenna height, and frequency. Adaptive data transfer capacity shared between connected nodes.

II. HISTORY OF MANET

MANET can be categorized into first, second and third generations. The first generation came up with "packet radio" networks (PRNET), and were sponsored by DARPA in the early 1970s. It has evolved to be a robust, reliable , operational experimental network. The PRNET used a combination of ALOHA and CSMA approaches for medium access, and a kind of distance-vector routing to provide packet-switched networking to mobile battlefield elements in an infrastructure less, hostile environment.

The second generation evolved in early 1980's when SURAN (Survivable Adaptive Radio Networks) significantly improved upon the radios (making them smaller, cheaper, power-thrifty), scalability of algorithms, and resilience to electronic attacks. Important developments during this period include Gloms (Global Mobile Information System) and NTDR (Near Term Digital Radio) The goal of Gloms was to provide office-environment Ethernet-type multimedia connectivity anytime, anywhere, in handheld devices. Channel access approaches were now in the CSMA/CA and TDMA molds, and several novel routing and topology control schemes were developed. The NTDR used clustering and link- state routing, and self-organized into a two-tier ad hoc network. Now used by the US Army, NTDR is the only "real" (non-prototypical) ad hoc network in use today.

The third generation evolved in 1990's also termed as commercial network with the advent of Notebooks computers, open source software and equipments based on RF and infrared. IEEE 802.11 subcommittee adopted the term "ad hoc networks." And the concept of commercial (non-military) ad hoc networking had arrived. Within the IETF, the Mobile Ad Hoc Networking (MANET) working group was horn, and sought to standardize routing protocols for ad hoc networks. The development of routing within the MANET working group and the larger community forked into reactive (routes on- demand) and proactive (routes ready-to-use) routing protocols 141. The 802.1 1 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable, if not optimal, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards. HIPERLAN and Bluetooth were some other standards that addressed and benefited ad hoc networking.

III. TYPES OF MANET

Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

Smart phone ad hoc networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.

Internet-based mobile ad-hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's Cloud Relay.

IV. APPLICATIONS OF MANET

To increase of portable devices as well as progress in wireless communication, adhoc networking is gaining importance with the increasing number of widespread applications in the commercial, Military and private sectors. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

1)Military Sector
2)Sector:
3)Networks
4)Traffic Analysis

Military Sector : Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field Commercial.

Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. This may be because all of the equipment was destroyed, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc. Low Level: Appropriate low level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

Networks: A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use. 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. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security**.**

Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function.

V.ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.

Passive attack: In this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information . This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping: Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking.

Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance .

Black hole Attack: Route discovery process in the black hole attack. The mechanism, that is, any intermediate node may respond to the message if it has a fresh enough route, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists.

Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages.

Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with no neighbors to disrupt routing operations.

Malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks.

VI. FEATURES OF MOBILE AD HOC NETWORKS

The mobile Ad hoc networks has the following features-

- Autonomous terminal
- Distributed operation
- Multihop routing
- Dynamic network topology
- Fluctuating link capacity
- Light-weight terminals

3.3.1 Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, beside the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

3.3.2 Distributed Operation

Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed to implement functions like security and routing.

3.3.3 Multihop Routing

Basic types of Ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

implementation, with the lesser cost of functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

3.3.4 Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the Ad hoc network, but may require access to a public fixed network (e.g. Internet).

3.3.5 Fluctuating Link Capacity

The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subjected to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

3.3.6 Light Weight Terminals

In most of the cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

VII. CHALLENGES IN MANET

Autonomous: No centralized administration entity is available to manage the operation of the different mobile nodes.
Dynamic topology: Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

Device discovery: Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

Bandwidth optimization: Wireless links have significantly lower capacity than the wired links. Routing protocols in wireless networks always use the bandwidth in an optimal manner by keeping the overhead as low as possible.
Limited resources :Mobile nodes rely on battery power, which is a scarce resource. Also storage capacity and power are severely limited.

Scalability: Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

Limited physical security: Mobility implies higher security risks such as peer-to- peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

Infrastructure-less and self operated: Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

Poor Transmission Quality: This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

Ad hoc addressing: Challenges in standard addressing scheme to be implemented.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Network configuration: The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

Topology maintenance: Updating information of dynamic links among nodes in MANETs is a major challenge.

VIII. CONCLUSION

The evolution in the field of mobile computing is driving 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. Mobile Ad hoc networks are generally more vulnerable to physical security threats than fixed or hardwired networks. This paper throws a light on different concepts of MANETS that can help researchers to the maximum. Its intrinsic flexibility, lack of infrastructure, ease of deployment, auto-configuration, low cost and potential applications make it an essential part of future pervasive computing environments. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all 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.

REFERENCES

[1] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester " An Overview of Mobile ad hoc Netwroks: Applications & Challenges " .
[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02,2002.
[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communications, IEEE In Wireless Communications, IEEE, Vol. 14, No. 5. (06 December 2007), pp. 85-91.
[4] Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.
[5] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBECOM '06.

ACKNOWLEDGEMENT

The author deeply indebted to honorable SHRI A.SRINIVASAN(Founder Chairman), SHRI P.NEELRAJ(Secretary) Dhanalakshmi Srinivasan Group of Institutions, Perambalur for giving me opportunity to work and avail the facilities of the College Campus. The author heartfelt and sincere thanks to Principal Dr.ARUNA DINAKARAN, Vice Principal Prof.S.H.AFROZE, HoD Mrs.V.VANEESWARI, (Dept. of CS & IT), Department staff, (Dept. of CS & IT) of Dhanalakshmi Srinivasan College of Arts & Science for Women,Perambalur.The author also thanks to parents, Family Members, Friends, Relatives for their support, freedom and motivation.

BIOGRAPHY

Ms.G.NATHIYA is presently pursuing M.Sc., Final year the Department of Computer Science from Dhanalakshmi Srinivasan College of Arts and Science for Women, perambalur, Tamil Nadu India.

Ms.A.KIRUTHIKA - Received M.C.A., M.Phil Degree in Computer Science. She is currently working as Assistant Professor in Department of Computer Science in Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur Tamil Nadu, India.She has Published papers in **IJSTM** & **IJIRCCE** journals and also Published two books Namely " Computer Basics and Internet " and "Introduction to Languages C,C++,Java" Her research areas are Networking,Web Technology and Cloud Computing.

Ms.A.ARUNA is presently pursuing M.Sc., Final year the Department of Computer Science from Dhanalakshmi Srinivasan College of Arts and Science for Women, perambalur, Tamil Nadu India.