AN OVERVIEW OF MANET AND ITS APPLICATIONS, SECURITY & THREATS

Dharavath Ravindar[1], Dr. Satheesh Kumar Nagineni[2]
Department of Computer Science and Engineering
[1,2]OPJS University, Churu (Rajasthan) – India

Abstract

Wireless Networks give association adaptability between clients at better places. Also, the network can be stretched out to any place or building without the need of a wired association. Wireless networks are classified into two categories; Infrastructure networks and Ad-Hoc networks. Wireless mobile devices are used in many application areas, for example, disaster relief, military services, and conferences and so on. In a MANET, hubs inside each other's remote transmission range can confer straightforwardly; in any case, hubs outside each other's range need to rely upon some extraordinary hubs to hand-off mess ages. Thusly, a multi-hop circumstance happens, where a couple of widely appealing has hand-off the parcels sent by the source host to influence them to accomplish the goal hub. MANET is one that gets together as required, not by any means with any assistance from the current foundation or whatever other kind of settled stations. This declaration can be formalized by describing an uncommonly designated system as a free arrangement of portable hosts (MHs) (additionally filling in as switches) related by remote connections, the union of which shapes a correspondence compose exhibited as a discretionary correspondence diagram. This is as opposed to the eminent single bounce cell arrange show that support the prerequisites of remote correspondence by presenting base stations (BSs) as get to centers. In these cell systems, correspondences between two adaptable hubs totally rely upon the wired spine and the settled (BSs).

1. INTRODUCTION

In a MANET, no such foundation exists and the system topology may dynamically change unconventionally since hubs are permitted to move. As for the strategy for operation, uniquely designated systems are on very basic level shared multi-bob portable remote systems where information parcels are transmitted in a "store-and-forward" route from a source to a subjective goal, by methods for transitional hubs as showed up in Figure 1. As the MHs move, the resulting change in arranges topology must be made known to exchange hubs with the goal that out of date topology information can be either revived or ousted. For example, MH2 in Figure 1 changes its motivation of association from MH3 to MH4, distinctive hubs in the system should now use this new course to forward parcels to MH2 [1].

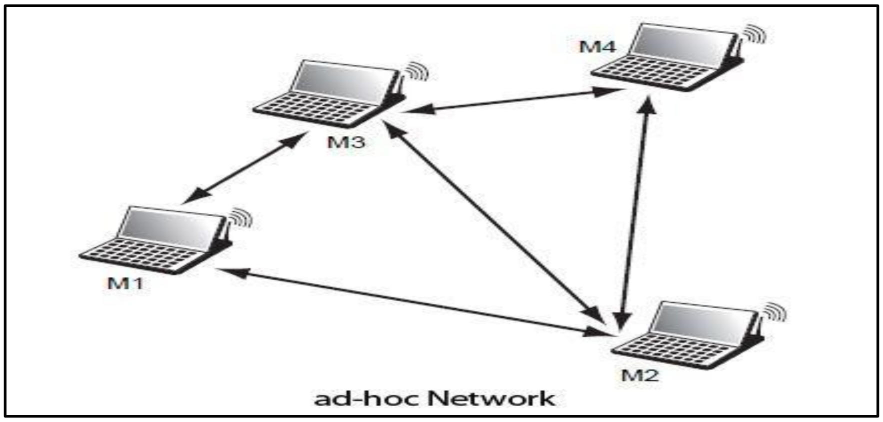

Figure 1: A Mobile Ad-Hoc network (MANET)

In Figure 1, it is acknowledged that it is unreasonable to have all MHs inside scope of each other. If all MHs are close-by inside radio range, no guiding issues to be tended to. In honest to goodness conditions, the power anticipated that would get complete accessibility may be, at any rate, infeasible, additionally issues, for instance, battery life and spatial reusability. Figure 1 raises another issue of symmetric (bi-directional) and lopsided (unidirectional) joins. As it will be seen later on, a part of the conventions that think about symmetric connections with cooperative radio range, i.e., if (in Figure 1) MH1 is inside radio scope of MH3, by then MH3 is additionally inside radio scope of MH1. Thus, finding a protected and dependable end-to-end route in MANETs is a certifiable test. At whatever point the hubs in the MANET are incorporated into correspondence, battery vitality of those hubs will get diminished. The going with are the attributes of the portable hubs in MANET [2]:

- Nodes are persistently moving.
- Limited radio transmission range.
- Limited network bandwidth.
- Limited battery power.
- No brought together administration.
- Open medium and absence of foundation.
- Lack of security.

2. APPLICATIONS OF MANETs

The arrangement of a MANETs is basic in view of the nonattendance of setting up any system for correspondence. For the most part such kind of systems is required in military application and emergency shield operations [3]. Regardless, gradually MANETs have entered with the zones of gaming, detecting and conferencing, community oriented and appropriated figuring. This dynamic system is yet to get a vast part of the business applications. Research is up 'til now proceeding toward this way with the goal that the MANET can be sent in any territory where a speedier and more affordable system can be setup in a glimmer for data correspondence. In the going with Table 1, audit of a part of the utilizations of Mobile Ad-Hoc Networks is given [4].

Application	Description
Military Services	Military services are one of the most discussed and common application areas of mobile Ad-Hoc networks: Where installation of any fixed infrastructure is not Possible in the enemy territories or inhospitable Terrains. In this environment MANET provides the Required communication mechanism in no time. Here, The soldiers are considered to be the mobile nodes. So The network is required to remain connected even Though the soldiers move freely. This support is Provided by the MANET. Another application in this Area can be the coordination of the military objects And the personnel in the battlefield. For example, the Leader of a group of soldiers may want to pass a Message to all the soldiers or a group of soldiers Involved in the operation. In this situation, a secure And reliable routing protocol should be able to do the Job.
Emergency Services	These arise as a result of natural disasters when the entire communications infrastructure is in disarray (for example, Tsunamis, hurricanes, earthquake etc.) where restoring communications quickly is essential. By using ad hoc networks, an infrastructure could be set up in hours instead of days/weeks required for wire-line communications.
Education	Universities and campus settings, Virtual classrooms, Ad-Hoc communications during meetings or lectures Sensing and Sensor network is a special case of Ad-Hoc networks
Gaming	Where mobility is generally not considered. However The battery power is a key factor in sensors. Each Sensor is equipped with a transceiver, a small micro- Controller and an energy source. The sensors relay Information from other devices to transport data to a Central monitor. The sensors are used to sense the Environmental condition such as temperature, pressure, humidity etc. In this case they form an ad hoc network to collect intended information. The mobility can also be incorporated into the sensor network where they are meant to study the behavior of tornados or to study the behavior of patients in the hospital. Multi-user games, robotics pets.
Personal Area Networking	Personal communicating devices like laptops, PDAs, mobile phones create a network to share data among one another called the Personal Area Network (PAN). The PAN covers a very short range for communication and can be used for ad hoc communication among the devices or for connecting to a backbone network.

Table 1: Application of Mobile Ad-Hoc Networks

3. CHARACTERISTICS AND FEATURES OF MANET

Ad hoc networks have many features, which make them very particular from wired networks and along these lines require innovative approaches to execute the network functionalities. Table 2 compresses a portion of the characteristics of MANETs [5].

Autonomous and infrastructure less
Multi-hop routing
Dynamic Network Topology
Device Heterogeneity
Energy Constrained Operation
Bandwidth Constrained variable capacity links
Limited Physical Security
Network Scalability
Self-creation, Self-organization and self-administration

Table 2: Characteristics of MANETs

4. CHALLENGES OF MANETs

MANETs have been an extremely prominent field of research for most recent couple of years. Relatively every normal for the network has been investigated to some level. However, no extreme resolution to any of the issues has been found. Despite what might be expected, more inquiries manifest which should be addressed Table 3 blueprints a portion of the significant challenges that should be addressed [6].

Absence of Centralized Management	Due to lack of coordinator, centralization and highly dynamic nature of ad-hoc networks detection of attacks becomes difficult, it also obstructs the trust management for the nodes in the MANET
Power Supply	Due to this denial-of-service attacks are possible. The adversary may continuously send more meaningless packets to a target node and ask this node to route in extra packets. By this way, battery of will be wasted and it may results in out of service
Internal Threats	The compromised nodes inside the network may uses the flaws in the routing protocols to degrade the routing mechanism of the network, may provide wrong link state information which are bad for security scenarios.
Insecure Boundaries	The nature of the MANET’s promotes freedom to join or leave any network. An insecure boundary makes the MANET susceptible to much type of attacks like passive eavesdropping, active interfering and DoS

Table 3: Major Challenges of MANETs

5. ADVANTAGES OF MANET ARE [7]:

- **Quick deployment**: MANETs are easy to deploy when compared to the wired networks because no cables are used. It also uses minimum deployment time.
- **Reduced cost of deployment**: since MANET does not use any costly infrastructure like copper wires, etc., the cost involved is minimum.
- **Dynamic topology**: the continuously movable devices like laptops, pdas, etc. Can also still communicate with its neighbors by using MANET. So the topology of MANET is dynamic.

6. SECURITY ROUTING PROTOCOLS IN MANETs: THREATS, VULNERABILITIES AND ATTACKS

Any system which is required to be secured may have shortcoming or vulnerabilities which would be focused by an attacker [8].

- **Threat**: Threat is the methods through which the capacity or expectation of an operator to adversely influence an automated system, office or operation can be showed. All techniques or things used to abuse a shortcoming in a system, operation or constitute threat operators. Cases of threats incorporate attackers, intelligence service and so on. Following factors cause threat in MANETs.
- **Nonappearance of infrastructure** — accreditation/verification creator capacities are missing.
- **Dynamically changing network topology** — this puts security of routing protocols under threat.
- **Power and computational constraints** — these can keep the utilization of complex encryption calculations.
- **Vulnerability**: Vulnerability is any equipment or software defect that leaves a data system open for potential exploitation. The exploitation can be of different sorts, for example, increasing unapproved access to data or upset basic preparing.
- **Channel vulnerability** — broadcast remote channels permit message roof dropping and injection effectively.
- **Node vulnerability** — when nodes don't live in physically ensured places, they effortlessly fall under attack.
- **Attack:** Attack is an endeavor to bypass the security controls on a PC system. The attack may change, discharge, or deny data. Cases of attacks incorporate activities, for example, acquiring illegitimate benefits, embedding data erroneously, altering data, investigating network movement, getting illegitimate access to the system or upset network operation utilizing malicious software. These attacks can be characterized into following kinds:
- **External Attacks**: External attacks are completed by nodes that don't have a place with the network. They cause congestion, send false routing data or cause inaccessibility of

services.

- **Internal Attacks**: Internal attacks are from traded off nodes that are a piece of the network. In an internal attack the malicious node from the network increases unapproved access and imitates as a honest to goodness node. It can break down movement between other nodes and may take an interest in other network exercises.

7. SECURITY ISSUES

The mobile ad hoc networks are more vulnerable to security problems than the wired networks [9].

- **No Predefined Boundary:** In mobile Ad-Hoc networks, we cannot precisely define the physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node, it will be able to communicate with that node. The attacks include eavesdropping, impersonation; tempering, replay and Denial of Service (DoS) attack.
- **Advisory inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus, this attack is more dangerous than the external attack. These nodes are called compromised nodes.
- **No Centralized Control Facility:** MANETs do not have any centralized control facility which may lead to many security problems. It becomes very difficult to detect any attack. Traffic cannot be monitored from a centralized point; instead the control is distributed at each node. The detection becomes more difficult when the advisory changes the attack pattern and the target of the attack. To the node a failure may be caused by an adversary or due to some network problem. Due to the lack of security association, we cannot classify the nodes as trusted node or untrusted node.
- **Limited Energy Resource:** Every one of the hubs in a versatile Ad-Hoc arrange relies upon battery control for their operation. The other power sources are thought to be missing. The enemy can send tremendous activity to the objective hub. The objective hub might be ceaselessly occupied in dealing with these parcels; this will cause the battery energy to be depleted. This will cause a foreswearing of administration (DOS) assault since now the hub won't have the capacity to give benefits inside the system. Now and again the aggressors request that the hubs play out some pointless tedious calculation causing its battery energy to be lost.
- **Changing Scale:** The scalability of the mobile ad hoc network keeps changing all the time. It is very difficult to predict the number of

nodes in a mobile ad hoc network at some future time. The protocols and services designed for MANETs must be made compatible to this changing scalability.

8. CONCLUSION

An overview on Mobile ad hoc networks (MANETs) is presented including need of MANETs, its applications and characteristics that distinguish it from other wireless networks. Due to these characteristics, there is need of separate routing protocols for MANET. Classification of routing protocols for MANET has been done on the basis topology of the network i.e. proactive or table- driven and reactive or demand-driven. A summarized overview of routing protocols belonging to each type of classification has also been presented hoping that it will be useful and helpful to students and researchers in the field. From this, we concluded that MANET routing protocols are designed based on the application area and environment and it is not possible to design a single protocol, which is suitable for all MANETs.

REFERENCES

[1]. Agrawal, Piyush; Ghosh, R. K. and Das, Sajal K. (2008). “Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks”, ICUIMC '08, Pages 310-314, ACM New York, NY, USA.

[2]. Banerjee, Sukla (2008). Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. Proceedings of the World Congress on Engineering and Computer Science 2008, October 22 - 24, San Francisco, USA.

[3]. Bhalaji, N.; Banerjee, Sinchan and Shanmugam, A. (2008). A Novel Routing Technique against Packet Dropping attack in Adhoc networks. In Journal of Computer Science, USA Volume 4 (7), pp. 538-544.

[4]. Y. Khamayseh, O. M. Darwish, and S. A. Wedian, “MA-AODV: Mobility Aware Routing ProtocolsforMobileAdhoc htruoF fo .corP ni “,skrowteN C lanoitanretnIonference on Systems and Networks Communications IEEE, pp. 25-29, 2009

[5]. W. Wang and C. Amza, - “Motion citsinutroppO rof gnituoR desab Ad-hoc Networks,”in Proc. of 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, October 31–November 4, 2011, pp. 169-178.

[6]. C. Liu and,S.Chang fo yduts ehT” sseleriw coh-da rof ssenevitceffe 2009 SICI fo .corP ni “,krowten no ecnerefnoC lanoitanretnI dn2 noitamrofnI :secneicS noitcaretnI ,namuH dna erutluC ,ygolonhceT ,2009 ,.voN 26-24 ,aeroK ,luoeS .417-412 .pp

[7]. F. Maan andN. Mazhar, “MANET Routing Protocols vs Mobility Models: A Performance

Evaluation,” drihT fo .corP ni no ecnerefnoC lanoitanretnI skrowteN erutuF dna suotiuqibU ,17-15 enuJ ,anihC ,nailaD ,EEEI .184-179 .pp ,2011

[8]. Alam, M. Rafiqul and Chan, K. S. (2010). RTT-TC: A topological comparison based method to detect wormhole attacks in MANET. 12th IEEE International Conference on Communication Technology (ICCT), 2010, pp.991-994.

[9]. D. Dharmaraju, M. Karir, J. S. Baras, and.S,saB nA” tsacitluM fo ydutS noitatnemelpmI Extensions of AODV,” in Proc. of International Symposium on Performance Evaluation of Computer and Telecommunication Systems, Montreal, Canada, July 20-24, 2003, pp. 122-130