JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

Critical Study of Mobile Ad-Hoc Network

Abhay Raj Sahu[1], Dr. Jitendra Sheethlani[2]

[1] Research Scholar, Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

[2] Research Guide, Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

Received : 7.10.2020 Revised : 6.11.2020 Accepted : 7.12.2020

ABSTRACT:

MANET, often known as a wireless ad hoc network or an ad hoc wireless network, is an acronym for mobile ad hoc network. They are made up of a collection of movable nodes that are wirelessly connected in an autonomous, self-repairing network without a fixed infrastructure. Due to the frequent changes in network topology, MANET nodes are free to migrate anywhere they like. This paper reflects critical study of Mobile Ad-Hoc Network.

KEYWORDS: network, Mobile Ad-Hoc Network, infrastructure, wireless

I MOBILE AD-HOC NETWORK:

A relatively common wireless networking model for mobile hosts is an ad hoc network. A group of communication devices, or nodes, that seek to connect without a fixed infrastructure and a predetermined arrangement of accessible links constitute a Mobile Ad hoc Network (MANET). Wireless communication networks known as mobile ad hoc networks are utilised in the business, government, and private sectors. They enable users to communicate information and access it regardless of where they are in the world or how close they are to infrastructure. Dealing with a wireless network presents one of the biggest hurdles for modern developers because, in general, wireless networks are extremely sensitive to security assaults. Up to now, these networks' problems with scalability, mobility, bandwidth restrictions, and power limitations have not entirely been solved. Security is a major concern with MANETs as well because sensitive data will be transmitted for use in law enforcement, emergency relief efforts, and military applications.

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

For the purpose of protecting the MANET against various forms of assaults, including modification, impersonation, fabrication, etc., a number of well-known ad hoc routing protocols have been addressed. The aforementioned attacks were covered in detail under the topics of availability, confidentiality, authentication, and integrity in Bing Wu et al. (2006) and Su Mon Bo et al. (2007). Mobile ad hoc networks have some security design concerns that are challenging because of the lack of infrastructure, shared wireless medium, mobile nodes, resource limitations of mobile devices, and bandwidth restrictions. The creation of a dynamic routing protocol that effectively locates a path between mobile nodes is one of the key difficulties in the architecture of an ad-hoc network. Communication in dynamic topology is made easier by routing protocols as Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Node Transition Probability (NTP), etc.

II TYPES OF MANETS:

Vehicular Ad hoc Network (VANETs) –

Ensure clear communication with another car or the roadside machinery. InVANETs, or intelligent vehicular ad hoc networks, deal with other vehicles or equipment on the road.

Smart Phone Ad hoc Network (SPANC) –

To build peer-to-peer networks devoid of traditional network infrastructure, wireless access points, or cellular carrier networks. Peers may join or leave this network without causing it to collapse.

Internet based Mobile Ad hoc Network (iMANETs) –

TCP/UDP and IP are among the internet protocols that it supports. For connecting mobile nodes and create distributed, autonomous routes.

Hub-Spoke MANET:

A geographically distributed MANET can be created via hub-spoke VPN connections between several sub MANETs. The standard Ad-hoc routing algorithm does not directly apply.

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

Military or Tactical MANETs –

The military units make use of this. Data rate, real-time demand, quick rerouting while moving, security, radio range, etc. are all stressed.

Flying Ad hoc Network (FANETs) –

There are unnamed aerial vehicles in this (commonly known as drones). Provides mobility and connections to isolated locations.

III APPLICATION OF MOBILE AD-HOC NETWORK:

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. Some of the popular applications include (Siva Ram Murthy et al 2007).

Collaborative and Distributed Computing:

The creation of an ad hoc wireless network is necessary due to the need for a temporary communication infrastructure for speedy communication with minimal configuration among a group of people in a conference or gathering. The level of protection that would be expected in a military setting is not necessary for this. However, the security of data transport is more crucial. All of the desired receivers must each have a copy of the transmitted file in order for the transmission to succeed. Users favour affordable, portable, high-processing-power devices for these applications, which are typically powered by battery sources. Such apps may be run on laptops with add-on interface cards, upgraded personal digital assistants (PDAs), or powerful mobile devices. Interoperability is a crucial concern when such heterogeneity is present.

Military Applications:

Security upkeep, latency, dependability, deliberate jamming, and failure recovery are major issues in a military setting. Military networks are built to ensure a minimal likelihood of being intercepted and/or being discovered. Therefore, nodes prefer to broadcast as infrequently as possible and with the least amount of power possible to reduce the likelihood of discovery or interception. Quick and dependable communication is necessary for the

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

coordination of military objects moving quickly, such as fleets of aeroplanes or battleships. Additionally, they need the assistance of trustworthy and secure multimedia multicasting. The nodes may have several high-power transceivers, each of which has the capacity to switch between various frequencies for security. For effective communication and coordination, they can also employ other services like location tracking utilising the Global Positioning System (GPS) or other satellite-based systems. In some types of applications, resource limitations like battery life and transmission power might not apply. A MANET for emergency communications may function independently or in conjunction with a larger network. Mobile nodes run on a battery supply in an emergency telecommunication scenario, whereas static nodes may receive power from a generator. Therefore, obtaining a high packet success rate while still delivering messages reliably is obviously crucial for emergency MANETs. This can be done by adjusting the emergency telecommunication nodes' transmitter power to only use the amount required to keep the receiver's SNR within acceptable limits. Reusing the channel in space is made possible by lowering the transmitter power, which boosts network throughput. Since a transmission won't interfere with as many nodes, using power control in an emergency circumstance reduces multiuser interference. As a result, more emergency or rescue mission nodes will be able to interact at once. Conserving energy is essential in networks whose nodes run on batteries, such as a handheld radio used by a rescue worker, because battery life affects whether or not a network is functional. It is preferable to maintain a low chance of intercept or a low probability of detection for specific emergency telecommunication MANET applications, such as hostage scenario or terrorist assault. Rescue mission nodes would therefore prefer to broadcast as seldom and with the least amount of power possible to reduce the likelihood of being detected or intercepted.

Emergency Operation:

Ad hoc wireless networks are highly helpful in emergency situations like crowd control, commando operations, and search and rescue. The self-configuration of the system with little overhead, the freedom and flexibility of mobility, and the absence of traditional communication infrastructure are the main advantages of ad hoc wireless networks for such activities. Ad hoc wireless network deployment right away would be a useful alternative for coordinating rescue operations in contexts when the traditional infrastructure-based communication services are damaged due to a war or due to natural calamities like earthquakes. They only need a minimal amount of initial network configuration to work, and setting up the network to its maximum potential takes very little time, if any. The ad hoc

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

network needs to be widely dispersed and expandable to many nodes. Since voice communication often outweighs data transmission in these circumstances, real-time communication capabilities are particularly crucial.

Wireless Sensor Networks

Ad hoc wireless networks fall under the category of "sensor networks," which are used to offer a wireless communication infrastructure among the sensors deployed in a particular domain. Sensor nodes are minuscule devices that sense physical parameters, process the data collected, and connect to the monitoring station across the network. Sensing activity might be routine or intermittent. Sensor networks are a distinct subset of ad hoc wireless networks due to features including node mobility, network size, deployment density, power limitations, and traffic distribution. Sensor nodes are expected to function in challenging geographic or environmental situations with little to no human maintenance. It is occasionally impossible to recharge an energy source. There are three types of power sources that can be utilised in sensor networks: replenishable, non-replenishable, and regenerable.

Hybrid Wireless Networks:

Ad hoc wireless networks find extensive use in hybrid wireless systems including multi-hop cellular networks and integrated cellular ad hoc relay. If the cellular network combines the benefits of multi hop relaying and the assistance of the current fixed infrastructure, capacity can be boosted. These networks combine adaptability and multi hop relaying with the dependability and support of stationary base stations used in cellular networks. The main benefits of hybrid wireless networks include high capacity, enhanced flexibility and reliability in routing, and better coverage in connectivity.

Wireless mesh Networks:

Wireless mesh networks are created to provide nodes without the cellular network's spectrum reuse restrictions and network design limitations. A data transmission from source to destination can take several different paths because to the mesh architecture, which enables rapid path reconfiguration in the event of a failure. These networks can be easily installed in residential areas, on highways, in commercial areas, and on college campuses, and they require less capital investment than cellular networks. Wireless mesh networks ought to be able to maintain and organise themselves. It is convenient for supplying the communication infrastructure for strategic applications since it can withstand numerous node failures brought

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

on by disasters. Wireless mesh networks are very scalable and simple to expand, and they handle high data rates.

IV PROS AND CONS OF MANET –

Pros:

1. Separation from central network administration.
2. Each node can play both the roles (router and host showing autonomous nature).
3. Self-configuring and self-healing nodes do not require intervention of human.
4. Highly scalable and suits the expansion of more network hub.

Cons:

1. Resources are limited on account of various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks.
4. High latency.

V CHARACTERISTICS OF MANET:

- **Dynamic Topologies:**
  Network topology, typically multiloop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As some or all the nodes rely on batteries or other exhaustible means for their

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

energy. Mobile nodes are characterized by less memory, power, and lightweight features.

- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.

- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

REFERENCES :

C.F. Chiasserini and R.R. Rao. A distributed power management policy for wireless ad hoc networks. *IEEE Wireless Communication and Networking* Conf, pp. 1209-1213, 2000.

Jae-Hwan Chang and Leandros Tassiulas. Energy Conserving Routing in Wireless Ad-hoc Networks. *Proc. of IEEE Infocom*, Vol. 1, pp. 22-31, 2000.

Elizabeth, M.R. and T. Chai-Keong. A Review of Current Protocols for Ad Hoc Mobile Wireless Networks. *IEEE personal communications*, Vol.6, No.2, pp. 46-55, April 1999.

G. Aggelou. *Mobile Ad-Hoc Wireless Networks from Wireless LANs to 4G Networks.* McGraw-Hill, 2005.

Sharad Agarwal and Srikanth V. Krishnamurthy. Distributed Power Control in Ad-hoc Wireless Networks. *PIMRC01*, 2001.

D.P. Agrawal and Qing- An Zeng. Introduction to Wireless and Mobile Systems. *BrookdCole-Thomson Learning*, 2003.