Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study of Ad-Hoc Network: A Review

Vanita Rani PG Student, Dr. Renu Dhir

Dr. B R Ambedkar National Institute of Technology Jalandhar (Pb.)

ABSTRACT: This paper focus on the study of Ad Hoc network its protocols and different types of networks in detail, as we know this is an emerging field which places lot of contribution in networking. The concept of dynamic mobility is also introduced in Ad Hoc network because nodes are moving from one place to another place, within this network any node can join the network and can leave the network at any time. Nodes can be the form of systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. At same time these nodes can act as host/router or both. The WiFi IEEE 802.11 and WiMAX IEEE 802.16 wireless standard supports different data rates at the first physical layer. Security and immediate reply of different types of nodes (end to end nodes, intermediate nodes and wireless antenna) is the main concern in AD HOC networks.

Keywords: Ad Hoc network, WMN, WSN, MANET.

1. INTRODUCTION

A **wireless ad-hoc network** is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks.

It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link (aka "hop") range, and thus this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a route able IP network environment without additional Layer 2 or Layer 3 capabilities.

1.1 Ad Hoc NETWORK ROUTING PROTOCOL

An **ad-hoc routing protocol** is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network . In ad-hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The explanations of Ad Hoc Network routing protocols is as follows:

1.1.1 Table-Driven (Pro-Active) Routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

1.1.2 Reactive (on-demand) routing

This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

1.1.3 Flow Oriented Routing

This type of protocols finds a route on demand by following present flows. One option is to unicast consecutively when forwarding data while promoting a new link. The main disadvantages of such algorithms are:

1. Takes long time when exploring new routes without a prior knowledge.
2. May refer to entitative existing traffic to compensate for missing knowledge on routes.

1.1.4 Hybrid (both pro-active and reactive) Routing

This type of protocols combines the advantages of proactive and of reactive routing. The main disadvantages of such algorithms are:

1. Advantage depends on number of Math van nodes activated.
2. Reaction to traffic demand depends on gradient of traffic volume.

1.1.5 Hierarchical Routing Protocol

With this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The main disadvantages of such algorithms are:

1. Advantage depends on depth of nesting and addressing scheme.
2. Reaction to traffic demand depends on meshing parameters.

1.1.6 Backpressure Routing

This type of routing does not pre-compute paths. It chooses next-hops dynamically as a packet is in progress toward its destination. These decisions are based on congestion gradients of neighbor nodes.

1.1.7 Host specific Routing Protocol

This type of protocols requires thorough administration to tailor the routing to a certain network layout and a distinct flow strategy. The main disadvantages of such algorithms are:

1. Advantage depends on quality of administration addressing scheme.
2. Proper reaction to changes in topology demands reconsidering all parametrizing.

1.1.8 Power-aware Routing Protocol

Energy required to transmit a signal is approximately proportional to dα, where d is the distance and $\alpha \geq 2$ is the attenuation factor path loss exponent, which depends on the transmission medium. When $\alpha = 2$ (which is the optimal case), transmitting a signal half the distance requires one fourth of the energy and if there is a node in the middle willing to spend another fourth of its energy for the second half, data would be transmitted for half of the energy than through a direct transmission – a fact that follows directly from the inverse square law of physics.

The main disadvantages of such algorithms are:

1. This method induces a delay for each transmission.
2. No relevance for energy network powered transmission operated via sufficient repeater infrastructure.

1.1. CLASSIFICATION OF Ad Hoc NETWORK:

Wireless ad hoc networks can be further classified by their application:

1.2.1. Wireless Mesh Network ()

A **wireless mesh network** (**WMN**) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type.

Applications of Wireless Mesh Network

Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high speed mobile video applications on board public transport or real time racing car telemetry. Some current applications:

- U.S. military forces are now using wireless mesh networking to connect their computers, mainly ruggedized laptops, in field operations.
- Electric meters now being deployed on residences transfer their readings from one to another and eventually to the central office for billing without the need for human meter readers or the need to connect the meters with cables.
- The laptops in the One Laptop per Child program use wireless mesh networking to enable students to exchange files and get on the Internet even though they lack wired or cell phone or other physical connections in their area.
- The 66-satellite Iridium constellation operates as a mesh network, with wireless links between adjacent satellites. Calls between two satellite phones are routed through the mesh, from one satellite to another across the constellation, without having to go through an earth station.

1.2.2 Wireless Sensor Networks (WSN)

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Application of Wireless Sensor Network

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

1.2.3 Mobile Ad Hoc Network (MANET)

A **mobile ad-hoc network** is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad-hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid 1990s. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

The mobile ad hoc network has the following typical features

- Unreliability of wireless links between nodes.
- Constantly changing topology.

1.2.3.1. Types of MANET

Vehicular Ad-hoc Networks (VANETs)

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Internet Based Mobile Ad-hoc Networks (iMANET)

Internet Based Mobile Ad-hoc Networks are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly. Wireless networks can generally be classified as wireless fixed networks, and wireless, or mobile ad-hoc networks. MANETs (mobile ad-hoc networks) are based on the idea of establishing a network without taking any support from a centralized structure. By nature these types of networks are suitable for situations where either no fixed infrastructure exists, or to deploy one is not possible.

Intelligent vehicular ad-hoc networks (InVANETs)

InVANET, or Intelligent Vehicular Ad-Hoc Networking, defines an Intelligent way of using Vehicular Networking. InVANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track the automotive vehicles is also preferred. InVANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.

Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).

CONCLUSION

In this paper, we study about Ad Hoc networks, its different protocols, different types of network namely WMN, WSN, MANET and various features and advantage of these networks explained. Further types of MANET networks which explains the concept if moving nodes in networks also discussed in detail. So the study of this network will be helpful to understand Ad Hoc networks and its various application area. The future scope of this research paper is to concentrates on improving more accurate and effective communication of these different networks.

REFERENCES:

1. Vani A and Rao D, "*Providing of Secure Routing against Attacks in MANETs*" International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011.
2. Senthilkumar P., Baskar M. and Saravanan K., "*A Study on Mobile Ad-Hock Networks (MANETS)*", JMS, Vol. No.1, Issue No.1, September 2011.
3. Satria Mandala, Md. Asri Ngadi and A.Hanan Abdullah, "*A Survey on MANET Intrusion Detection*" IJCSS, Vol No 2, Issue 1, 2007.
4. Ruchi R., Dawra M., "*Performance characterization of AODV protocol in MANET*", IJARCET, Vol No 1, Issue No 3, May2012.
5. D.Sivaganesan1 and Dr.R.Venkatesan, "*Performance Analysis of Broadcasting in Mobile ad hoc networks using cluster approach*", IJASUC Vol No.1, Issue No.2, June 2010.
6. Sreerama M and Venkat D., "*Performance Evalution of MANET Routing Protocols using Reference Point Group Mobility and Random WayPoint Models*", IJASUC Vol No.2, Issue No.1, March 2011.
7. Murty S, Dastagiraiah C. and Kumar A, "*Analysis of MANET routing Protocols Using Random waypoint Model in DSR*", IJASUC Vol No .2, Issue No.4, December 2011.
8. Chaudhary D., "*Bee-Inspired Routing Protocols for mobile Ad HOC Network (MANET)*", JETWI, VOL No. 2, Issue No. 2, MAY 2010.
9. Koshti D and Kamoji S, "*Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks*" IJSCE, Vol 1, Issue 4, 2011W Lien and Feng Yi "*A Threshold-Based Method for Selfish Nodes Detection in MANET*", 978-1-4244-7640-4/10/2010 IEEE.
10. W Lien and Feng Yi, "A Threshold-Based Method for Selfish Nodes Detection in MANET", IEEE, 2010.
11. Sukumaran S, Venkatesh. J and Arunkorath, "*A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks*" IJICT, Vol 1, Issue No. 2, June 2011.

12. Roy B., Banik S., Dey P., Sanyal S and Chaki N, "*Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services*", JETCIS, Vol. No 3, Issue No. 1, January 2012.
13. P.V.Jani, "*Security within Ad-Hoc Networks*," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
14. K. Biswas and Md. Liaqat Ali, "*Security threats in Mobile Ad-Hoc Network*", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.