Study of Ad hoc Networks with Reference to MANET, VANET, FANET

Bodhy Krishna. S
Research Scholar, Department of Computer Science, Farook College, Calicut, Kerala, India

DOI: 10.23956/ijarcsse/V7I7/0159

Abstract: A wireless ad hoc network is a decentralized type of wireless network. It is a type of temporary computer-to-computer connection. It is a spontaneous network which includes mobile ad-hoc networks (MANET), vehicular ad-hoc networks (VANET) and Flying ad-hoc networks (FANET). A MANET is a network that has many free or autonomous nodes often composed of mobile devices that can operate without strict top-down network administration [1]. A VANET is a sub form of MANET. It is a technology that uses vehicles as nodes in a network to create a mobile network. FANET is an ad-hoc network of flying nodes. They can fly independently or can be operated distantly. This paper discusses the characteristics of these three ad-hoc networks.

Keywords: Ad hoc, MANET, VANET, FANET, Comparison

I. INTRODUCTION

A wireless ad hoc network is a collection of wireless nodes without any centralized administration. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. That is, in ad hoc mode, you can set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router.

Ad hoc networks are useful when you need to share files or other data directly with another computer but don't have access to a Wi-Fi network. In this, more than one laptop can be connected to the ad hoc network, as long as all of the adapter cards are configured for ad hoc mode and connect to the same SSID (service state identifier). The computers need to be within 100 meters of each other.

Also, if you were the person who set up the ad hoc network, when you disconnect from the network, all of the other users will also be disconnected. An ad hoc network will also be deleted once everyone on it disconnects. It is truly a spontaneous network. Ad hoc networks have no fixed topology because of the high degree of node mobility. The nodes in an ad hoc network sometimes act as routers to forward packets to each other. These nodes generally have a limited transmission range, so each node seeks the assistance of its neighboring nodes in forwarding packets. Thus data is sent between nodes by hopping through the intermediate nodes. The characteristics of ad-hoc networks are discussed below.

- **Mobility**: The fact that nodes can be rapidly repositioned and/or move is a main characteristic of ad hoc networks. Rapid deployment in areas with no infrastructure often implies that the users must explore an area and perhaps form teams that in turn coordinate among themselves to create a mission.

- **Multihopping**: A multihop network is a network where the path from source to destination traverses several other nodes. Ad hoc networks often exhibit multiple hops for obstacle negotiation, spectrum reuse, and energy conservation.

- **Self-organization**: The ad hoc network must autonomously determine its own configuration parameters including addressing, routing, clustering, position identification, power control etc. In some cases, special nodes (e.g., mobile backbone nodes) can coordinate their motion and dynamically distribute in the geographic area to provide coverage of disconnected islands.

- **Energy conservation**: Most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply and no capability to generate their own power. Energy efficient protocol design is critical for longevity of the mission.

- **Scalability**: In some applications (e.g., large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc.) the ad hoc network can grow to several thousand nodes. For wireless “infrastructure” networks scalability is simply handled by a hierarchical construction. The limited mobility of infrastructure networks can also be easily handled using Mobile IP or local handoff techniques. In contrast, because of the more extensive mobility and the lack of fixed references, pure ad hoc networks do not tolerate mobile IP or a fixed hierarchy structure. Thus, mobility, jointly with large scale is one of the most critical challenges in ad hoc design.

- **Security**: The challenges of wireless security are well known - ability of the intruders to eavesdrop and jam/spoof the channel. A lot of the work done in general wireless infrastructure networks extends to the ad hoc domain. The ad hoc networks, however, are even more vulnerable to attacks than the infrastructure counterparts. Both active and passive attacks are possible. An active attacker tends to disrupt operations. Due to the complexity of the ad hoc network protocols these active attacks are by far more difficult to detect/fold in ad hoc than infrastructure networks. Passive attacks are unique of ad hoc networks, and can be even more insidious.
than the active ones. The active attacker is eventually discovered and physically disabled or eliminated. The passive attacker is never discovered by the network. Like a “bug”, it is placed in a sensor field or at a street corner. It monitors data and control traffic patterns and thus infers the motion of rescue teams in an urban environment, the redeployment of troops in the field or the evolution of a particular mission. This information is relayed back to the enemy headquarters via special communications channels (eg. satellites or UAVs) with low energy and low probability of detection. Defense from passive attacks require powerful novel encryption techniques coupled with careful network protocol designs.

- **Connection to the Internet**: as earlier discussed, there is merit in extending the infrastructure wireless networks opportunistically with ad hoc appendices. For instance, the reach of a domestic wireless LAN can be extended as needed (to the garage, the car parked in the street, the neighbor’s home, etc.) with portable routers. These opportunistic extensions are becoming increasingly important and in fact are the most promising evolution pathway to commercial applications. The integration of ad hoc protocols with infrastructure standards is thus becoming a hot issue.

Node mobility may cause the routes change. Some form of routing protocol is necessary in ad hoc networks, because two hosts that may wish to exchange packets might not be able to communicate directly. Hence efficient and reliable routing is one of the key challenges in ad hoc networks. Many routing algorithms have been devised and developed for attaining this task. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology.

Several routing protocols exist for wired networks, which can be classified as using either the distance vector or the link-state algorithm. These algorithms were designed for use in wired networks where topology changes are infrequent. They are also computation intensive, making them difficult to use with limited resources. Due to these problems, new routing algorithms are designed keeping in mind the characteristics of ad hoc networks. An ad-hoc routing protocol must be able to decide the best path between the nodes having unidirectional links, minimize the routing overhead to enable proper routing, minimize the time required to converge after the topology changes and maximize the bandwidth utilization. Therefore, developing support for routing is one of the key research areas in ad hoc networks.

Wireless ad hoc networks include mobile ad-hoc networks (MANET), vehicular ad-hoc networks (VANET) and Flying ad-hoc networks (FANET). MANET & VANET are many popular parts of ad-hoc networks. MANET is an ad-hoc network of mobile nodes while VANET is an ad-hoc network of Vehicular nodes. In 2012, Ilker Bekmezci introduced the concept of FANET, an ad-hoc network of flying nodes. Details of these networks are discussed in this paper. The main objective of this paper is to explain the members of ad hoc family - MANET, VANET, FANET and to introduce applications, advantages and unique challenges in them.

### II. MOBILE AD-HOC NETWORKS (MANET)

Mobile Ad Hoc Network (MANET) is a temporary network that can be dynamically formed to exchange information by wireless nodes or routers which may be mobile. Network nodes may be laptop, Personal Digital Assistant (PDA), mobile phones, MP3 players, digital cameras and so on. MANET does not use any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves. So, the wireless topology of the network may change frequently and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. A MANET may be defined as a network that has many free or autonomous nodes often composed of mobile devices or other mobile pieces that can arrange themselves in various ways and operate without strict top-down network administration.

The advantages of MANET are that it can have more flexibility, it is better in mobility, it can be turn up and turn down in a very short time, it can be more economical and it is considered a robust network because of its non-hierarchical distributed control and management mechanism. There are several applications for MANET. Some of them are that a group of people with laptops can exchange files without having an access point; they can exchange information when the network infrastructure is destroyed, it is suitable for military communications in battlefield where there is no network infrastructure, they can be used during search and rescue operations in disastrous situations like earthquakes, students can use laptops to participate in an interactive lecture, business associates can share information during a conference etc.

Due to mobility and the decentralized nature, MANETs have a lot of challenges and issues. They are limited wireless range i.e. wireless range may be limited, some terminals may be hidden which causes hidden terminal problem, packets may be lost as the connections are not as reliable as wired networks, there may be changes in routes due to dynamic topology, the devices involved in the ad hoc network can be heterogeneous, nodes in ad hoc networks are equipped with limited battery life, there may be huge number of nodes in some cases which causes scalability problem etc. As wireless networks are less reliable than wired networks, quality of the network can also be affected by environmental factors and may result in low quality communication.

### III. VEHICULAR AD-HOC NETWORKS (VANET)

A Vehicular Ad hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET. It is a technology that uses vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing the vehicles to connect and in turn, create a network within a wide range. It is a special kind of mobile ad hoc network where wireless equipped element called on-board unit (OBU) in vehicles form a network with the Roadside unit (RSU) without any additional infrastructure. It provides communication between vehicles.
and between vehicles and road-side base stations with an aim of providing efficient and safe transportation. VANET introduces more challenging aspects as compared to MANET because of high mobility of nodes and fast topology changes in VANET. VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency and convenience as well as comfort to both drivers and passengers. VANET can achieve effective communication between moving nodes by using different ad-hoc networking tools such as Wi-fi IEEE 802.11 b/g, WiMax IEEE 802.10, Bluetooth, IRA [2].

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow. Vehicular Ad Hoc Networks (VANETs) is technology that integrates the capabilities of new generation wireless networks to vehicles. VANET builds a robust Ad-Hoc network between mobile vehicles and roadside units.

VANET is mainly aimed at providing safety related information and traffic management. As the vehicles are growing, the possibility of accidents has also increased. It is required to make our vehicles a bit intelligent so that we can reduce the possibilities of accidents. A vehicular ad-hoc network (VANET) adds this ability in the vehicles. Simplicity and security of VANET mechanism ensures greater efficiency which leads to efficient emergency communications. For example, in the case of accidents, an alerting message transmitted among vehicles can be faster and, thus, well-timed, rather than communications sent through an infrastructure network (such as cellular systems).

VANETs can be utilized for a broad range of safety and non-safety applications, allowing for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet. VANET inculcate sufficient potential in vehicles to transmit warnings about environmental hazards, traffic and road conditions and regional information to other vehicles.

A. Architecture of VANET

In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. The VANET architecture consists of the following components i.e. Application unit (AU), On Board Unit (OBU) and Road Side Unit (RSU).

i) On Board Unit (OBU)

A device which is commonly known as On Board Unit (OBU), usually mounted on-board a vehicle is used for exchanging information with RSUs or with other OBUs. The OBU comprises of a resource command processor (RCP), and the resources contain a read/write memory used to store up and recover information, a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication. It also comprises of another network device for non-safety applications. The OBU connects to the RSU or to other OBUs all the way through a wireless link, and is responsible for the communications with other OBUs or with RSUs. It can also provide communication services to the AU and forwards data on behalf of other OBUs on the network. The main functions of the OBU in VANET are wireless radio access, ad-hoc and geographical routing, network congestion control, reliable message transfer and data security.

ii) Application Unit (AU)

The Application Unit (AU) is the device within the vehicle which uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be connected to the OBU through a wired or wireless connection and can reside with the OBU in a single physical unit. The dissimilarity between the AU and the OBU is logical. The AU communicates with the network only by the use of the OBU which takes task for all mobility and networking functions.

Road Side Unit (RSU) The Road Side Unit (RSU) is a wave device normally fixed along the road side or in dedicated locations such as at the junctions or near parking spaces. The RSU is equipped with one network device for a Dedicated Short Range Communication and is able to be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network.

For communication to occur between vehicles and RoadSide Units (RSUs) vehicles must be equipped with radio interface or OnBoard Unit (OBU) that enables short-range wireless ad hoc networks to be formed. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Usually, the RSU hosts an application that provides services and the OBU is a peer device. In the Vehicular communication systems the communication among vehicles and RSU is achieved by using a wireless medium which is popularly known as WAVE. This scheme of communication provides a broad range of information to drivers and travellers and intelligence to safety applications to improve road safety and it also provide a secure driving. The application possibly will reside in the RSU or in the OBU. The device to facilitate hosts application is called the provider and the device using the application is known as the user. Each vehicle is equipped with an OBU and a set of sensors to accumulate and process the information. And then send it as a message to other vehicles or RSUs by the wireless medium. It also carries a single or multiple AU that use the applications provided by the provider using OBU connection capabilities. The RSU is capable of connecting to the internet or to another server so as to allow AU’s from multiple vehicles to join in the direction of the Internet.
Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units is dependent on the communication protocol to be used. For example, some protocols require roadside units to be distributed evenly throughout the whole road network; some require roadside units only at intersections, while others require roadside units only at region borders.

IV. FLYING AD-HOC NETWORKS (FANET)

FANET is a group of Unmanned Air Vehicle (UAVs) communicating with each other with no need to access point, but at least one of them must be connected to a ground base or satellite [3]. UAVs work without human help, like autopilot. UAVs can fly independently or can be operated distantly. Earlier, UAVs were simple remotely piloted aircrafts and mostly used for military operations / applications. However, in recent years, UAVs are being used in increasing number of civil applications, such as policing and fire-fighting, non-military security work, etc. The use of single-UAV system is very common, but using a group of small UAVs has become advantageous. Nonetheless, multi-UAV systems have some exclusive challenges and one of the most important design issues is the communication.

There are many advantages of multi-UAV systems. It is economical as the installation and maintenance cost of small UAVs are much less than that of a large UAV [4]. Its coverage rate is low as single UAV have limited coverage area [5]. However, multi-UAV systems can adapt to the situation easily making it more flexible. If the UAV operation (operated by one UAV) fails in a mission, it cannot proceed. However, if a UAV goes off in a multi-UAV system, the operation can be survived through other UAVs. So it has continuity. It has been shown that the missions can be completed faster with a higher number of UAVs [6]. Instead of one large radar cross-section, multi-UAV systems produce very small radar cross-sections which are more accurate and crucial for military applications [7]. Multi UAVs are more sustainable than single UAV system. Multi-UAVs sometime can be solved recursively, which is much easier than single UAV system. So, it is easy to solve.

Although there is much single UAV application but using multiple UAV systems co-operating with each other can be helpful in many ways. But different issues and challenges are needed to be addressed in the case of the multi-UAV system. Co-operation between UAV’s is essential in a multi-UAV system and complex hardware in order to communicate with a ground base station or a satellite. Reliability of the communication is the second issue. Another problem is the range restriction among the UAVs and the ground base station. If a UAV is outside the coverage area of the ground station, it becomes disconnected. To resolve all the above mentioned issues, an alternative solution for multi-UAV systems is required to create an ad-hoc network among the UAVs, which is called FANET.

In FANET, only a subset of UAVs can interconnect with the ground station or the satellite and all UAVs constitute an ad-hoc network. In this way, the UAVs can communicate with one another in addition to the ground station. FANET is basically a special form of MANET/VANET. There are also certain differences between FANET and the traditional ad-hoc networks. Mobility degree of FANET nodes is much higher than that of MANET or VANET nodes. While typical MANET and VANET nodes are walking human beings or vehicles, respectively, FANET nodes fly in the sky. Due to high mobility of FANET nodes, the topology changes more frequently than the network topology of a typical MANET or even VANET. FANET needs peer-to-peer connections for synchronization and relationship of UAVs. It is required to collect data from the environment and to transmit to the command & control center, as in wireless sensor networks [8]. Hence, FANET must support both peer-to-peer communication and converge cast traffic at the equivalent time. The distances among FANET nodes are much higher than in MANETs or VANETs [9]; so higher range of communication is needed. Multi-UAV systems may include different types of sensors, and each sensor may require different data distribution approaches. However, FANET term instantly prompts that it is a specialized form of MANET and VANET. This is why it is called Flying Ad-Hoc Network, FANET.

V. COMPARISON OF MANET, VANET AND FANET

Wireless ad hoc networks are categorized permitting to their application, positioning, communication and assignment intentions. By characterization, FANET is a form of MANET, and there are many mutual design thoughts for MANET and FANET. FANET can also be classified as a subset of VANET, which is also a subgroup of MANET. FANET shares common characteristics with these networks, and it also has some unique design challenges. In the following subsections, the differences among FANET and the existing wireless ad hoc networks are explained in details.

Node mobility issues are the most significant difference between FANET and the other ad hoc networks. MANET node movement is comparatively slow when it is compared to VANET. In FANET, the nodes mobility degree is much higher than in the VANET and MANET. This results in several challenging communication design problems [10]. MANET nodes move on a definite territory, VANET nodes move on the highways, and FANET nodes fly in the sky. In multi-UAV systems, the flight plan is not fixed, if a multi-UAV system uses predefined flight plans it may not be successful, because of the environmental deviations or operation updates, the flight plan may need to be recalculated.

Node density is defined as the average number of nodes in a unit area. FANET nodes are normally spread in the sky, and the distance between UAVs can be several kilometers even for small multi-UAV systems. As a result of this, FANET node density is much lower than in the MANET and VANET. Due to higher mobility degree, FANET topology changes more regularly than MANET and VANET topology. When a UAV fails, the links that the UAV has been involved in also failed and it results in a topology update. Another factor that affects the FANET topology is the link outages. Because of the UAV schedules and variations of FANET node distances, link quality changes very quickly, and it also causes link outages and topology changes [11].
FANET and the other ad hoc network operating environments affect the radio propagation characteristics. MANET and VANET nodes are very close to the ground, and in many cases, there is no line of-sight between the sender and the receiver. Radio signals are mostly affected by the geographic structure. Again, FANET nodes those are away from the ground can be driven remotely and in maximum case; there is a line-of-sight between UAVs [12]. Developing energy efficient communication protocols is a major part to increase the network lifetime. Particularly, while the battery-powered computing devices in MANETs; system developers have to pay extra attention to the energy efficient communication protocols. However, FANET communication hardware is powered by the energy source of the UAV. This means FANET communication hardware has no power resource problem as like in MANET.

MANET nodes are battery powered small computers such as laptops, PDAs and smart phones. Because of the size and energy constraints, the nodes have only limited computational power. On the other hand VANETs and FANETs support devices with high computational power. In MANET, GPS is generally used to receive the coordinates of a mobile communication terminal, and maximum time, GPS is enough to regulate the location of the nodes. In VANET, for a navigation-grade GPS receiver, there is about 10–15 m accuracy, which can be satisfactory for route guidance. Because of the high velocity and dissimilar mobility models of multi UAV systems, FANET needs highly accurate localization data with smaller time intervals. GPS provides position information at one second interval, and it may not be adequate for certain FANET protocols.

VI. CONCLUSION

The wireless connection can be used to extend the network to different places as it removes the need to establish a point to point wired links. Ad-hoc network does not have a central coordination or fixed topology which increases complexity in sending or receiving packets between nodes. This paper explains the members of ad hoc family - MANET, VANET, FANET and introduces applications, advantages and unique challenges in them. Study shows that mobility degree of FANET nodes is much higher than that of MANET or VANET nodes as FANET nodes fly in the sky. Due to high mobility of FANET nodes, the topology changes more frequently than the network topology of a typical MANET or even VANET. So there are more challenges in FANET than in MANET or VANET.

REFERENCES