Chapter 8
A Relative Study About Mobile Ad-Hoc Network (MANET):
Applications, Standard, Protocols, Architecture, and Recent Trends

Preety Khatri
Institute of Management Studies, Noida, India

Priti Rani Rajvanshi
Institute of Management Studies, Noida, India

ABSTRACT

This chapter includes a relative study of mobile ad-hoc networks (MANET), vehicular ad hoc networks (VANET), and Flying ad-hoc networks (FANET). The approaches and protocol applicable to MANET are equally applicable to VANET or FANET. Authors discuss several emerging application and the future trends of MANET, VANET, and FANET. The common attacks on ad hoc networks are also introduced. The chapter enhances the overall concepts relative to MANET, VANET, and FANET. Authors compare mobile ad-hoc networks (MANET), vehicular ad hoc networks (VANET), and flying ad-hoc networks (FANET) in all aspects with the help of several examples. The chapter includes a relative and detailed study of mobile ad-hoc networks (MANET), vehicular ad hoc networks (VANET), and Flying ad-hoc networks (FANET).

INTRODUCTION

Several Nodes in Wireless Environment managed with distributed authority to form a wireless ad-hoc network. Categorization of this network is depending upon the position permission, assignment intentions, user and connections. The wireless connection can be set up directly between computers it means it is a temporary network having computer -to -computer connection. There is no requirement to connect to a Wi-Fi router between them. The specifications to define network ad-hoc is non dependency of fixed or planned framework of network like access points works for infrastructure wireless networking, routers in

DOI: 10.4018/978-1-7998-2570-8.ch008

connected or predefined networks. The extemporaneous way of connecting nodes is a form of connected networks consist of Flying ad-hoc networks (FANET), Mobile ad-hoc networks (MANET) (Abusalah, Khokhar & Guizani, 2008) and vehicular ad hoc networks (VANET). In last few years, there has been growth in the field of MANET, FANET & VANET and these ad-hoc networks are growing day by day in the field of research and development.

Through the medium of wireless routers or nodes and interim network can be setup spontaneously to transfer the data between nodes . This ad hoc network can be operated without strict top-down network administration, For example, the network nodes like mobile phones, digital cameras, laptop and so on. MANET is the new developing and evolving techniques that allows everyone to transfer their information over infrastructure-less environment irrespective of their geographical location and this is the reason sometimes MANET is also known as “infrastructure less network”. MANET attracts a large number of real world application areas and these are the areas where networks topology changes very fast (Govindaswamy, Blackstone & Balasekaran, 2011). But since last few years, lots of researchers are working on and trying to remove the main problems occurred in MANET or example computational power, limited bandwidth, security, battery power and so on. MANET become more exposed to the threads if we follow the same security solutions that are used to protect present wired network. geographical location, that’s why it is sometimes referred to as an infrastructure less network.

As we know that VANET is subgroup of MANET. To create a mobile network technology, VANET works with automobile industry products like car and so on. The function of VANET is to allow automobiles to connect with the help of wide range of network. It converts every two wheeler or four wheeler automobile product. Main aim is to provide communication between vehicles and also established and maintains an efficient and safe transportation. As the vehicles are increasing, day- by- day so the chances of accidents has also increased. So to reduce the chances or possibilities of accidents, there is requirement to make our vehicles intelligent and this is the reason of adding the feature in vehicle by VANET. Vehicular ad-hoc network (VANET) originate several challenging standpoint as compared to MANET because of fast topology changes and high movability of nodes in VANET.

FANET is an ad-hoc network which is also related to air floating nodes and these nodes can be operated distantly and can fly independently (Murthy & Manoj, 2004). FANET is a separate type of MANET with various common infrastructural design convictions. FANET is a class of Unmanned Air Vehicle (UAVs) and these UAV’s interact without any requirement of access point (Muller, 2012). But in between the classes of Unmanned Air Vehicle (UAVs), and these have to be linked in satellite. UAVs can be operated distantly and also can fly independently. Similarly like an autopilot, the UAVs work without human help. Earlier, UAVs were mostly used for military applications or operations because these were simple remotely piloted aircraft (Kumar, Basavaraju & Puttamadappa, 2008). However, in recent years, the UAVs operate without any pilot and the use cases for civil applications are increasing day by day e.g., non-military security work, policing and firefighting and so on. According to the earlier technology single-UAV system is commonly used, however according to new challenges that are by using a class of small UAVs has been added some leverage to the ad hoc networks (Sahingoz, 2014). However, the multi-UAV systems (Govindaswamy et. al, 2011) have one of the most important design issues is the communication and have some limited challenges also. FANETs are used very often in systems as the systems are more capable and can be applied and solve various problems. So, we can say that these networks have some additional advantages as compared to their traditional ad hoc networks as the unmanned systems are used to communicate in different zones (Zhang Jacob, 2003).

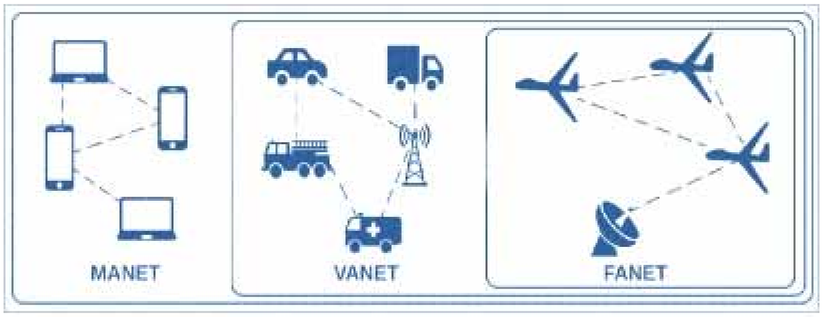
In This chapter we will discuss about detailed study of MANET, VANET, and FANET (Abusalah et. al, 2008) . This chapter also discuss about what are the protocols as well as approaches which are applicable to MANET is equally applicable to VANET or FANET. We will also discuss about several upcoming use cases with the latest agendas of MANET, VANET and FANET. The common attacks on ad hoc networks also introduced. Mainly this chapter enhances the overall concepts relative to MANET, VANET and FANET (Sahingoz, 2014). We will also discuss the comparison between MANET, VANET, and FANET in all aspects with the help of several examples. We will also study about the earlier technologies which were used in ad hoc networks and now days, since few past years, how ad hoc networks are growing day by day. All the above-mentioned networks are the best in their areas according to their features, but out of them (in MANET, VANET and FANET) which one is the best and what are the failures of these ad hoc networks, architecture design, vulnerabilities etc. These types of issues will be discussed in this chapter. In last of this chapter, we will discuss about the future scope of ad hoc networks. So, we can say that in this chapter we will discuss about the relative and detailed study of MANET, VANET, and FANET.

MANET is a temporary network consists of grounded mobile nodes and these are working self-organized wireless network and communication. In case of any tragic condition in which the conventional ways of communication are not available or not in condition to provide services. In that situation MANET (Mobile Ad hoc Network) play a very vital part to develop and maintain communication. Sensors, camera and several other devices are the sources to collect information for grounded mobile nodes to help MANET.

These mobile nodes in MANET connect together wireless network and communication with all other mobile nodes and did not use any pre-established infrastructure (Abusalah et. al, 2008) . These mobile nodes collect all the data and then multi hop way is used to transmit this data to base station. MANET establishes a very economical and can be made very fast whenever and whenever it is required because of no dependency on pre-established infrastructure of communication. There are several issues with the working of MANET as:

- No fixed topology
- Limited or low bandwidth
- No centralized control
- Unstable communication channel
- Security threats to the nodes
- Limited processing power and memory
- Lack of association between grounded mobile nodes
- Limited availability of resources
- Vulnerable
- Shared channel of communication on radio waves

Figure 1. Relationship between MANET, VANET and FANET



A MANET can serve lots of requirements and these requirements are not served by traditional physical infrastructure-dependent networks. Like: cellular network offloading provided by MANETs. But the network offloading may be critical for example: if these are large number of customers which are using the network and at a point the network capacity has been exceeds, causing interruptions or lags in service. Temporarily diverting traffic from traditional network infrastructure is also done by MANET to reproduce service. This ad-hoc network also added some features like information dissemination and communication capabilities which are applied in the areas that permanently or temporarily do not have well-organized communication infrastructure. For example: rural areas, areas having very less economic resources, post-natural disasters areas etc. The main advantage of MANET is Proximity-based applications (Lee, Gahng-Seop, Zhang & Campbell, 2000). The various applications of MANETs employ the co-location of nodes which is used to find opportunities and provide services like parking availability, which results for social and environmental benefits.

APPLICATIONS OF MANET

With the progress in wireless communication ad-hoc networking achieving some importance as well as it also extends the portable devices and also having a large number of applications for example: commercial sector, military and private sectors etc. These networks have some features like where the customers can exchange information irrespective of the geographical position. These networks allow to easily add or remove devices from the network or to maintain connections to the network. MANET doesn't require fixed infrastructure whereas mobile network does. So we can say that the area of MANET applications is very vast and dynamic (Kumar et. al, 2008).

Sensor Networks

Sensor network is a collection of small sensors and these networks has been used to discover a large number of areas like: pollution, pressure, temperature, toxins etc. Every sensor has a very limited capability, so to forward data to a central computer, each have to rely on others. These sensors are prone to loss or failure. So we can say that sensor networks has very vast area which is used to measure environmental conditions like sound, pollution levels, temperature, wind speed, humidity, direction, pressure etc.

Personal Area Network (PAN)

Personal Area Network also an important application area of MANET (Luo, Lu, Bharghavan, Cheng & Zhong, 2004). The interconnection between different mobile devices like cellular phone, laptop etc. is done with the help of Personal Area Network. It can extend its capability to networks like GPRS, WLAN etc. PAN is the wide area of MANET for the future perspective in mobile computing.

For Military Operations

Ad-hoc networks have vast area in the field of military purpose (Murthy et. al, 2004). With the help of networks, it provides short term as well as fast establishment of military deployments and communications in the unknown environments. Ad-hoc network technology is used for military purpose like to provide networks in between vehicles, soldiers etc.

Rescue Operations During Emergency:

MANET also has overcome the area of security as well as safety of people during emergency. It provides networks for communication in areas having no wireless support.

Disaster Management Support

MANET also provides support during disaster management by providing the communication networks.

Law Enforcement

During law enforcement operations, ad-hoc networks provide fast and secure communication.

Commercial Use

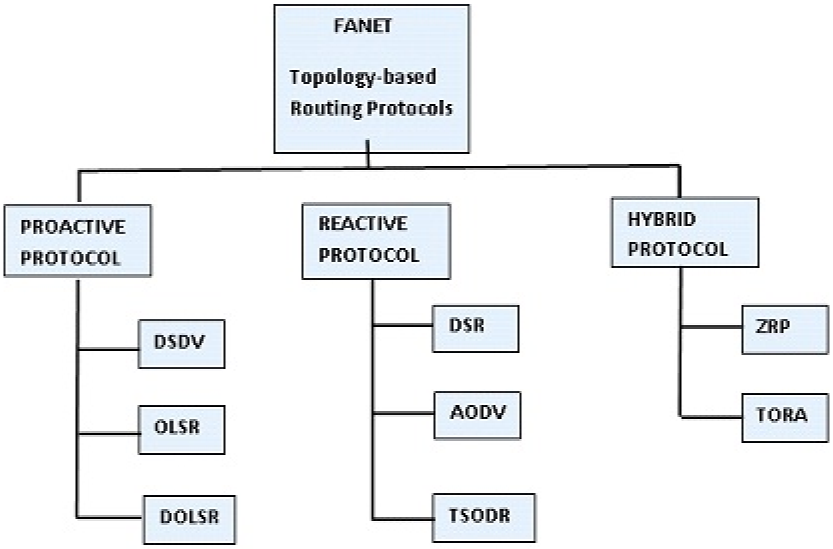
There are various applications related to MANET. Commercial use also the main application area of ad-hoc network and these are used for enabling communications like in business areas, seminars, conferences, exhibitions etc.

ROUTING PROTOCOLS

In ad-hoc networks there are variety of routing protocols has been used in ad-hoc networks. It is the most essential part of research issue in MANET, FANET as well as in VANET (Belding-Royer & Toh, 1999). But during fundamental research it must deal with some disadvantages like power failure, high error rates, low bandwidth, and problem during movement of nodes etc.

By using routing protocol, it reduces the signalling overhead and also provides end-to-end data delivery. As we know that FANET networks are very complex so it has a vast impact on the optimal routing protocol but it is the area of research till now (Bekmezci, Sahingoz & Temel, 2013). These optimal routing protocols like swarm-based routing protocols, topology-based routing protocols, position-based routing protocols etc. In the case of topology-based routing protocol, IP addresses are used to forward data packets (on optimal path) with the help of existing link information. The topology-based routing also establishes the optimal route between all types of communicating nodes. This type of topology has been further classified as reactive routing hybrid routing and proactive routing as shown in Figure 2. To improve FANET performance, these routing protocols has been used. the performance has been increased in terms of minimize delay, increase throughput, consumption of resources etc (Belding-Royer et. al, 1999).

Figure 2. Different types of routing protocols



Proactive Routing Protocols (PRPs)

The PRPs are also known as active or table-driven routing protocols and in these types of protocols, routing table which is moderated on continual basis and these tables placed and stored on each UAV. So this storage shows the whole topology of the network. Thus, for transmitting data packets, the routing paths can be available when required (Muller, 2012). These protocols consist of the most updated information about the routes. So to maintain proper information regarding network, they introduces additional signalling overhead and due to these additional signalling, the controlled messages are transmitted without any need. The disadvantage of these protocols is that these are not suitable for large network.

Destination-Sequenced (DSDV)

DSDV's routing protocol is based on the Bellman–Ford–Moore algorithm. In this type of protocol, each UAV must be aware everything about all of the other UAVs and these UAVs must be connected to the network, so that it receives updated routing information (Lee, Roye & Perkins, 2003). In these types of protocols, routing tables are updated periodically, which results in routing loops. For maintaining the updated routing tables, these protocols also add sequence numbers with the help of data packets. These protocols are simple to apply and use as compared to other protocols, which benefits the data transmission among all the UAVs is loop-free. But the main disadvantage of these protocols is that extra signalling overhead issue in case of data transmission.

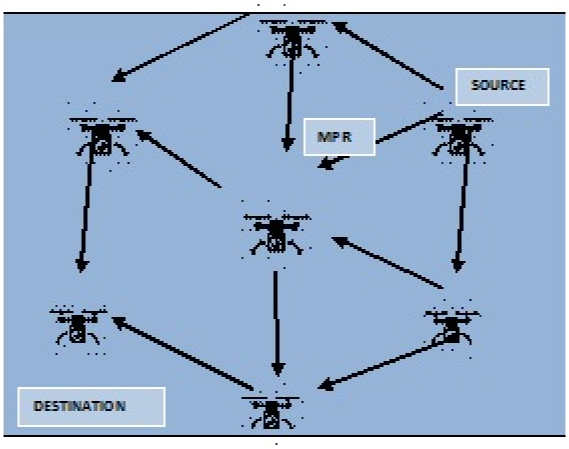
Optimized Link State Routing (OLSR)

OLSR's protocol (Singh & Verma, 2014). is the most routing protocols for FANET system (Muller, 2012). In this protocol system the routing paths are continuously updated in the routing table. So for data transmission path, when it is required, the protocol finds the path to all the possible destination UAVs. This protocol consists of a packet having collection of messages which are used to maintain communication UAVs. This unique packet consists of various type of messages:

1. A message to control topology (to maintain topological information)
2. A message HELLO, to find neighbouring UAVs
3. The message related to multiple interface declaration on UAVs.

As shown in Figure 3 it displays the multipoint relay (MPR) mechanism in OLSR and this represents the MPR selection with the help of UAV and these MPR have the impact on no. of MPRs. The signalling overhead will reduce, in case if the number of MPRs shrinks. If the distance is greater, then DOLSR is selected for data transmission.

Figure 3. Multipoint relay (MPR) mechanism in OLSR



Reactive Routing Protocols (RRP)

RRP's also known as passive routing or on-demand protocols (Gerla, Lee & Su, 2000). *RRP's* used to maintain and discover the routing path in the network. For this, it maintains routing table, which updates the information regarding data to be send. The updating will be reflected in the routing table if and only if in case of the availability of data. During routing through these protocols, these are two types of messages are generated:

1. **RouteRequest:** This message generated from the source node and extends uotp all UAV's which are adjacent to the source.. This RouteRequest message uses the flooding process which is used to find out the optimal route.
2. **RouteReply Messages**: This message generated when reply message is received by UAV's.

Dynamic Source Routing (DSR)

DSR's protocol is very reactive in nature, it means this protocol is suitable for wireless mesh network. As like in reactive routing protocols, the source establishes the connection with target for routing path, similarly, DSR also establishes the same connection during routing path, but when required. Basically, this is based on the two factors:

1. **Route Discovery:** As the name suggests, this message represents to find out the route. The UAV's which are initiated through the source, have to find out the best route until the destination has been reached.
2. **Route Maintenance:** Maintenance between route has to be required only when there is some problem occurs between links.

Ad-Hoc On-Demand Distance Vector (AODV)

AODV's routing (Royer & Perkins, 1999) is very reactive in nature. Similar features like DSR, it maintains paths which are from source to destination. To avoid network congestion, AODV protocol allocates the time slots to packet transmissions (Lee et. al, 2003). There are three phases in routing protocol:

1. **Route Discovery:** This represents to find out route. In case if a source UAV sends the packet, so that message has been required.
2. **Packet Transmitting:** Without routing loops, it does the packet transmission and forward packet over a determined path,
3. **Route Maintaining:** This is the phase which represent maintenance between route to be required if some problem has been occurred between routes. This works same like in DSR protocol. It is required only when link failure occurs.

Time-Slotted On-Demand Routing (TSODR)

TSODR's protocol is mostly used for FANETs. It works in similar way (in case of time-slotted) like AODV (Royer et. al, 1999). TSODR sends packets in allocated time slot (Gerla et. al, 2000) This protocol provides better bandwidth and routing protocol in allocated time silce. It also avoids collisions among packets and data transmission.

Hybrid Routing Protocols (HRP)

HRP's (Wang, Chuang, Hsu & hung, 2003) *consist* of proactive as well as reactive routing protocol methods.

Reactive Routing Protocol: These protocols have been used to find out optimal route, which is very effective. This protocol also has advantage that it overcomes end-to-end delay. It has also some feature that shows that inner-zone routing is also possible and executed with the help of this protocol.

Proactive Routing Protocol: To control a large amount of messages the proactive routing protocol has been used. The large problem overhead has been overcome in this routing protocol.

Zone Routing Protocol (ZRP)

ZRP's based on the routing of "zones" which has been used for different types of mobility patterns of UAVs (Zhang et. al, 2003). These protocols have two types of routing:

Intrazone Routing: Intrazone routing is carried through proactive routing. The data packet routing is done with intrazone routing.

Interzone Routing: The interzone routing has been carried through reactive routing. The optimal path finding is done with interzone routing.

Temporarily Ordered Routing Algorithm (TORA)

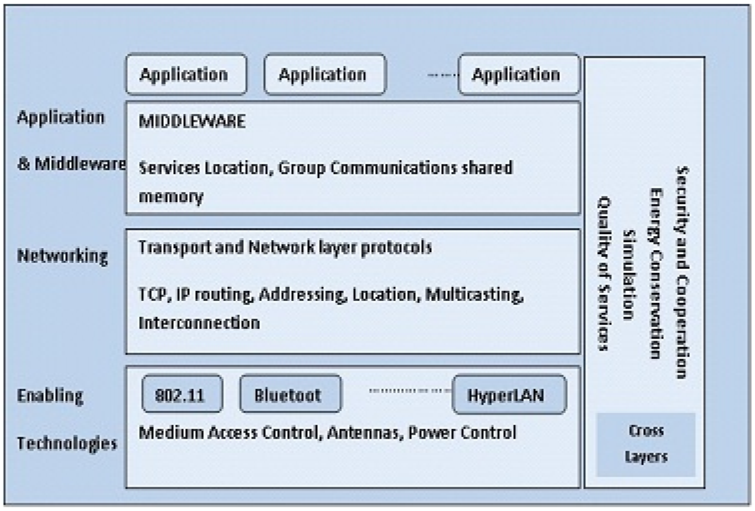
TORA has been used for multi-hop networks as well as for proactive routing. These protocols maintain the acyclic graph (directed) from source to destination. Based on the directed acyclic graph, the multiple paths have been created from source to destination and these paths have been used to transmit the packets. For data packet transmission, this routing protocol used the top-down approach. It means the data packets have been transmitted from top UAVs to lower UAVs.

As shown in below table, this displays about the comparative study of topology-based routing protocols.

Table 1. Comparative study of topology-based routing protocols

Routing Protocol	Protocol Type	Topology Size	Communication Latency	Route Updates	Bandwidth Utilization	Signaling Overhead
DSDV	Proactive	Small	Low	Periodic	Minimum	Large
OLSR	Proactive	Small	Low	Periodic	Minimum	Large
DOLSR	Proactive	Small	Low	Periodic	Minimum	Large
DSR	Reactive	Large	High	On Need	Maximum	Small
AODV	Reactive	Large	High	On Need	Maximum	Small
TSODR	Reactive	Large	High	On Need	Maximum	Small
ZRP	Hybrid	Both	Low	Hybrid	Medium	Average
TORA	Hybrid	Both	Low	Hybrid	Medium	Average

Figure 4. MANET architecture


Application
Application
Application
Application
& Middleware
MIDDLEWARE
Services Location, Group Communications shared memory
Networking
Transport and Network layer protocols
TCP, IP routing, Addressing, Location, Multicasting, Interconnection
Enabling
Technologies
802.11
Bluetoot
HyperLAN
Medium Access Control, Antennas, Power Control
Security and Cooperation
Energy Conservation
Simulation
Quality of Services
Cross
Layers

MANET ARCHITECTURE

As shown in the above figure 4, this displays about the MANET architecture (Swarnapriyaa, Vinodhini, Anthoniraj & Anand, 2011). It is divided into three layers:

- **Application & Middleware:** it is the first layer of MANET architecture. In this layer, the application and middleware which provide service location, group communications shared memory.
- **Networking:** This is the second layer of MANET architecture (Xiang, Wang & Yang, 2011). In this layer, the transport and network layer protocols which are used for IP routing, addressing, multicasting, interconnection etc. The main aim of network protocols is to develop to end-to-end reliable services and this transmission between sender and receiver.
- **Enabling Technologies:** This is the below most layer in the architecture. It consist of antennas, medium access control, power control etc. Based on the coverage area, these technologies are further classified as:
  - **PAN (Personal Area Network):** This network runs around an individual person and also connects mobile services through the network. The PAN network having the communication range is up to 10 meters.
  - **BAN (Body Area Network):** This network works on the pattern same like PAN, but as in case of PAN, it runs around an individual person whereas Ban runs around wearable devices. The normal range is 1-2 meters. This network is used to connect the devices wearable also.
  - **HiperLAN:** this network is used to provide an infrastructure or ad-hoc wireless with small radius and low mobility. There are different components of HiperLAN are: physical layer, link adaption, data ink control layer, convergence layer. This network supports isochronous traffic with low latency.
- **Cross Layers:** MANET architecture consists of various layers which are used to manage the architecture. These layers also provide some responsibilities for example to conserve the energy, to provide better quality service etc.

- **Middleware and applications:** There are various middleware and applications like WIFI, Bluetooth, IEEE 802.11, WIMAX etc. Which enhance the ad hoc networking applications and ad hoc technologies in various fields e.g. disaster recovery, environment monitoring, emergency services etc.

ATTACKS IN MANET

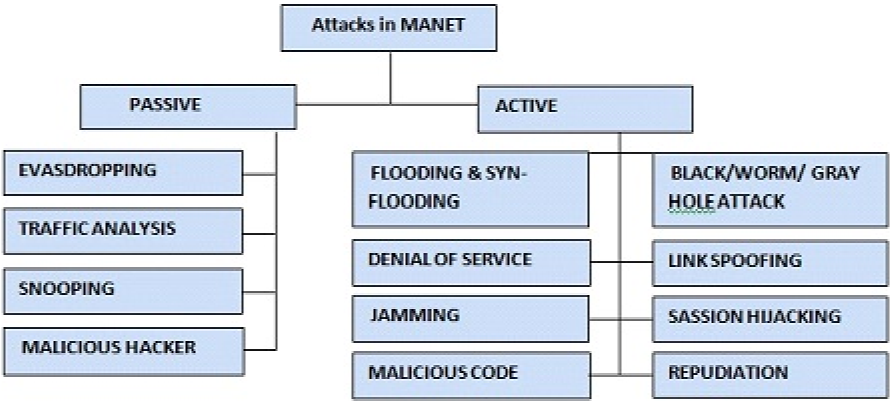
MANET systems are more open to attacks because of decentralized and wireless medium then wired network several attacks are there to impact MANET (Swarnapriyaa et. al, 2011). Classification of these attacks shown in below table 2. The foremost and important challenge is the security of Wireless as-hoc networks. The first step to provide a good solution for any challenge related to security is to find out and understands the major possible types of attacks. The important point for secured transfer of any data or information in MANET is that the communication should be highly secured. The MANET will become more vulnerable to any kind of cyber/digital attacks than any wired network if there is no mechanism of shared wireless communication medium and non availability of central coordinator. MANET can be affected by several kinds and numbers of attacks. Some attacks categorized in the table as below:

Table 2. Different attacks in MANET

Different security Layer of MANET	Attacks in MANET
Application Layer	Unsuspected, unreliable code
Transport Layer	To hijack the session, flooding
Network Layer	Spoofing problem, grey, worm and black hole
Data Link Layer	To analyze and monitor the traffic

In MANET, the layout of these attacks are divided as active and passive attacks as described in below figure-

Figure 5. Different types of attacks in MANET



- **Passive Attack:** To access information of traffic not by insulating any wrong information however the intrusion will be performed by various types of continuous monitoring on specific networks. To perform an impactful attack, it will assist the attacker to provide the path of the network which is going to be attacked and to access all the information. Some passive attacks are categorized as eavesdropping, traffic analysis and snooping, malicious hacker.
    - **Eavesdropping:** Here, the attacker is also called eavesdropper. The secret information is being watched by the nodes continuously. Confidential information can be like password, public key, location, private key and so on. Then malicious nodes follow the footsteps of this node and the information will be accessed by the attacker.
    - **Traffic Analysis:** In traffic analysis attack is the major key areas for attackers are pattern of traffic and the data packets. This attack can also be in the category of active attack because of destroying the nodes.
    - **Snooping:** This type of passive attack is very similar to eavesdropping but with a difference as it is not only get access during the transmission but snooping also involve the basic observation of e-mails on any other user's system or even snooping what anyone is typing on their system. To access anyone else's information illegally is called Snooping.
    - **Malicious Hackers:** This type of passive attack adapt snooping as a technique to check continuously about the login information, interpret e-mail communication, key strokes, view passwords, any private communication and transmission of any confidential information. Snooping has both aspects positive and negative it depends upon its use by its user.
- **Active Attack:** The active attack can be performed by two ways either by modifying transmitted data or unethical access to network resources. Active attacks can be of further two types internal or external. In external attack the attack is caused by the node of external network whereas internal attack is caused by the internal node of the same network. Types of active attacks are explained below-
    - **Flooding and SYN-Flooding Attack:** These types of attacks have focus is to degrade the performance of the transmission network either by overuse the resources of nodes, like battery backup, disturb the routing operations or by wasting the resources of network like bandwidth, it will flood the network and result will be wastage of battery power and bandwidth and lead to denial-of-service (Lee & Gerla, 2000). SYN-Flooding attack is also having same technique as in flooding to attack on networks. In these types of active attack the invader generates several TCP connections which are half opened to the node on which the attack is going to be happened. These connections never complete the communication and that also lead to denial-of-service.
    - **Denial of Service Attack:** This type of active attacks follows the technique to destroy the complete information of route from the routing table and then focus on destroying all the operations of MANET.
    - **Jamming:** In this type of active attack there are two extremes one is positive as it helps to protect the authorized packets of information to be received by any other nonauthorized node. Jammer is the main resource in this attack which works on the transmission signals along with the threats to the security. It is also one of the types of DOS attack which starts after sensing the rate of communication between two nodes.

- **Malicious Code Attacks:** In this attack the victim node can be user application and operating system as both the parties are involved in the communication and transmission. This attack involves viruses, spywares, Trojan horses, worms, intruders and so on. These malicious and unwanted pieces of codes affect the working of network and make it allow the abrupt operations in all the cases.
- **Black/ Worm/ Gray hole Attack:** These three attacks majorly focus on the routing in the MANET. In case of black hole attack if invader found any request then a suspicious node mislead the traffic and drop it in the temporary area in the network by just showing that it has the fresh and shortest path, which even does not exist in reality. In the case of wormhole attack, it will work as a tunnel in between two attacks which are collaborative. This tunnel interrupts the routing via routing control messages. Invader once senses a packet at a location in the network send them to another location via tunnel. Wormhole attack is perilous as it can lead to damage without the information of the network. In case of gray hole attack, one is by showing itself a verified route from source to target place and another is by misleading packets to reach the wrong destination with some possibility.
- **Link Spoofing Attack:** Link spoofing attack on MANET the invader or unwanted node spread a forged hyperlink with other receipts other than neighbourhood to interrupt the operations in routing of network. The invader then modifies the information or traffic data of routing and performing any other types of denial-of-service attack.
- **Session Hijacking:** Session Hijacking attack of MANET it start searching for the sessions which are newly established and not so protected then destroy those sessions. This attack is also called address attack. The invader intrude into IP address of node which is going to be attacked, extract sequence number belongs to that node which is going to be hijacked and execute many denial-of-service attacks. It starts intruding into the confidential data starting from public key, private key, login information, passwords till all other information of nodes and networks.
- **Repudiation Attacks:** Repudiation attack of MANET the major concern on the participation in the communication partially or fully (Yap, Liu, Tan & Goi, 2015). This attack creates denial participation on behalf of the victim nodes. Because of which packet security is not so sufficient via encryption and decryption and firewalls that are used at different layers of communication network.

COMPARATIVE STUDY

As from the above discussion, there are various FANET protocols (Bekmezci, 2013). Below given in table 3, which represents the comparison among basic routing protocols in FANET based on some major criteria.

- **Main Idea:** The routing information is static means whereas, in case of Proactive protocol the main idea is based on table driven protocol. On demand protocol (Lee et. al, 2003). comes under reactive protocol.

Table 3. A comparative study of FANET protocols based on some major criteria

TYPES OF PROTOCOLS				
Criteria	**Static Protocols**	**Proactive Protocols**	**Reactive protocols**	**Hybrid Protocols**
Main Idea	Static table	Table driven protocol	On demand protocol	Combination of proactive and reactive protocol
Operation	Fixed mission	Dynamic mission	Dynamic mission	Dynamic mission
Route	Static	Dynamic	Dynamic	Dynamic
Complexity	Less	Moderate	Average	Average
Popularity	Least	Medium	Medium	Best
Bandwidth Utilization	Best possible	Least possible	Best possible	Moderate
Failure Rate	High	Low	Low	Very Low
Convergence Time	Quicker	Slower	Mostly fast	Medium
Fault Tolerance	Missing	Missing	Missing	Mostly Present
Memory Size	Extensive	Extensive	Least memory	Medium memory
Topology Size	Small	Small	Large	Small & Large
Communication Latency	Less	Less	High	High
Signaling Overhead	Missing	Existing	Existing	Existing

- **Operation:** Operation in static protocol is fixed whereas in other protocols the operation is dynamic. Most protocols were used as a part of military operations. These protocols can be used for military as well as in civilian operations.
- **Route:** Routes are static for static protocols whereas these are dynamic for other protocols (Lee et. al, 2003).
- **Complexity:** In static protocol, complexity is comparatively low, whereas in reactive and hybrid protocols, complexity is average.
- **Popularity:** Static protocols are easy to understand but these are least popular as compared as compared to other protocols. The hybrid protocol is most popular as compared to other protocols.
- **Bandwidth Utilization:** Transmission capacity in static and reactive protocols is best as compared to other protocols. Transmission capacity for reactive protocol is source driven, so their bandwidth utilization capacity is very less.
- **Convergence Time:** The hybrid protocols required average time to converge the network whereas static protocols provide very fast convergence time for the network. The reason is that static protocol finds the route in the best possible way and very fast.
- **Fault Tolerant:** Fault tolerance is missing in static, proactive and reactive protocols. Whereas it is present in hybrid protocols. There are some routing methods which have fault tolerance mechanism which is used to find best optimum routes.
- **Memory Size:** There is less memory space in reactive protocols whereas large memory space is there in case of hybrid protocols. Large memory space is required in proactive protocols.
- **Topology Size:** It is the best use of static as well as proactive protocols for small network. But there is requirement of large network then reactive and hybrid protocol is best.

- **Communication Latency:** The Reactive and hybrid protocols have higher latency as compare to static and proactive protocol because reactive and hybrid protocols required time for route discovery.
- **Signalling Overhead:** Signalling overhead is present in proactive, reactive and hybrid protocols whereas it is absent in the static protocol. For example to request a route, reply messages, these are present in these protocols. But this is absent in static protocol.

To measure the performance between MANET protocols some of the measuring criteria has been followed:

- **Throughput:** Throughput defines that at specific period of time, how many data packets has been received.
- **Packet Delivery Fraction:** It defines that ratio of packets received by destination with packet sent by source.
- **Routing Load:** It defines the ratio of no. of routing packets transmitted with no. of packets received.
- **End-to-End Delay:** It defines what is the time taken to transmit packets from source to the destination.

Below given some of the comparison between some of these protocols based on these parameters:

Figure 6. Comparison between Routing protocols in terms of speed

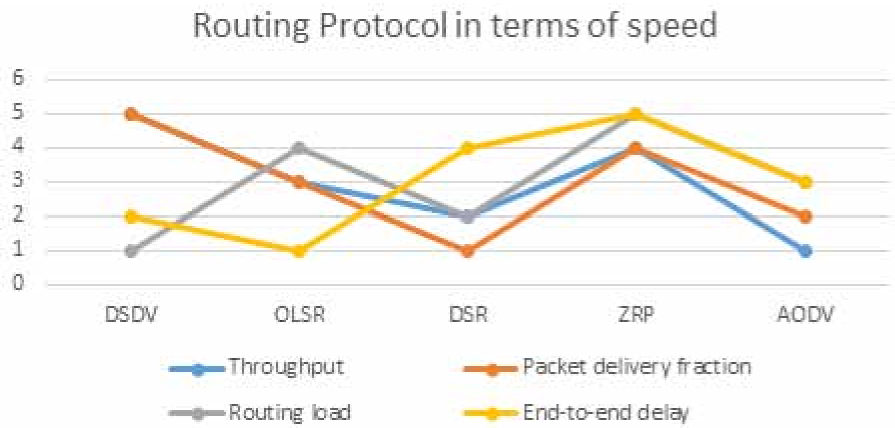


Figure 7. Comparison between Routing protocols in terms of network density

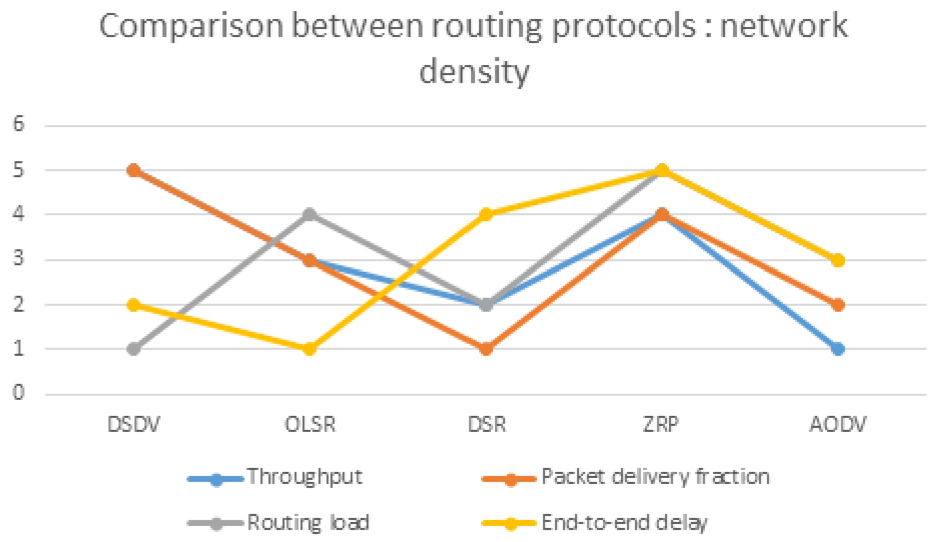
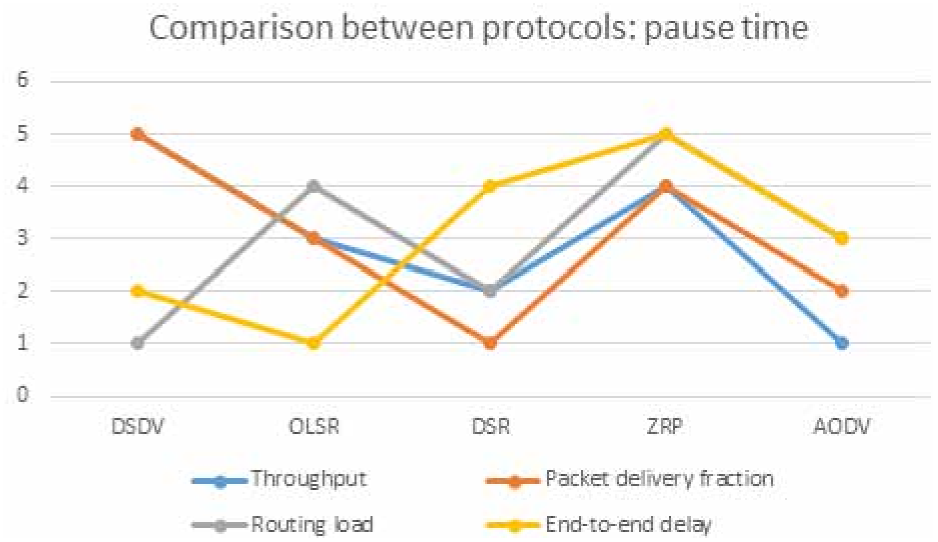


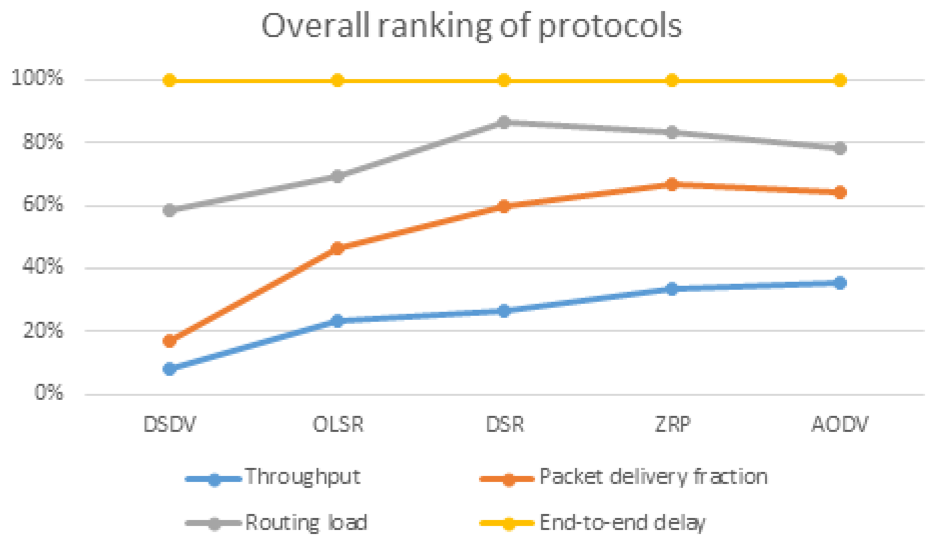
Figure 8. Comparison between Routing protocols in terms of pause time



CONCLUSION AND FUTURE SCOPE

The future of ad- hoc networks provides the vision like: anywhere, anytime available network and it's having cheap communication. In today's scenario, the general aim in MANET is about larger scalability and protocols. There is requirement of higher frequency, which needs improvement in bandwidth and capacity of the network. Another challenging issue in future will be large scale ad hoc networks because ad hoc networks have smaller, cheaper and are more capable forms.

Figure 9. Comparison between Routing protocols: overall ranking



In the field of mobile computing, a large evolution has been driving towards mobile communication, where mobile devices form self-organising, self-creating wireless network which is known as MANET. MANET are more susceptible to physical security threats as compared to hardwired or fixed networks. MANETs, VANETs and FANETs which helps the researchers to the maximum. This chapter emphasis on several protocols, emerging application and the future trends of ad hoc networks. The nodes in ad-hoc networks will be cheaper and also available in various forms (Murthy et. al, 2004). So overall, the use of ad hoc networks is still years away, so we can say that in this field, there is large amount of research and implementation will continue being imaginative and very active.

REFERENCES

Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols (pp. 78–93). IEEE Communication: Surveys & Tutorials, IEEE.

Bekmezci, S. O., Sahingoz, O. K., & Temel, Ş. (2013). Flying ad-hoc networks: A survey. *Ad Hoc Networks*, *11*(3), 1254–1270. doi:10.1016/j.adhoc.2012.12.004

Belding-Royer, E., & Toh, C. (1999). *A review of current routing protocols for ad-hoc mobile wireless networks*(pp. 46-55). IEEE Personal Communication magazine.

Gerla, M., Lee, S., & Su, W. (2000). *On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks*. Retrieved from draft-ietfmanet-odmrp-02.txt.

Govindaswamy, V., Blackstone, W., & Balasekaran, G. (2011). Survey of Recent Position Based Routing Mobile Ad-hoc Network Protocols (pp. 467-471). *Proceedings of 2011, UKSim, 13th International Conference on Modelling and Simulation*. 10.1109/UKSIM.2011.95

Kumar, S., Basavaraju, T., & Puttamadappa, C. (2008). *Ad-hoc Mobile Wireless Networks Principles, Protocols, and Applications*. New York: Auerbach Publications.

Lee, J., & Gerla, M. (2000). AODV-BR: Backup routing in Ad Hoc networks. *Proceedings of IEEE, WCNC*. 10.1109/WCNC.2000.904822

Lee, S., Gahng-Seop,, A., Zhang,, X.,, & Campbell,, A. (2000). INSIGNIA: An IP-based Quality of Service Framework for Mobile Ad-hoc Networks (pp. 374-406). Journal of Parallel and Distributed Computing8. Scalability study of the ad hoc on-demand distance vector routing protocol (pp. 97-114). *International Journal of Network Management*, *13*.

Luo, H., Lu, S., Bharghavan, V., Cheng, I., & Zhong, G. (2004). *A Packet Scheduling Approach to QoS Support in Multi-hop Wireless Networks* (pp. 193-206). International Journal of Mobile Networks and Applications.

Muller, M. (2012). Flying Adhoc Network. In *Proceedings of the 4th Seminar on Research Trends in Media Informatics*. Institute of Media Informatics, Ulm University.

Murthy, C., & Manoj, B. (2004). *Ad-hoc Wireless Networks Architectures and Protocols* (p. 07458). Upper Saddle River, NJ: Prentice Hall.

Royer, E., & Perkins, C. (1999). Multicast Operation of the Ad Hoc On Demand Distance Vector Routing Protocol (pp. 207-218). *Proc. ACM/IEEE MobiCom*.

Sahingoz, O. (2014*)*. Networking models in flying Ad-hoc networks (FANETs): Concepts and challenges (pp. 513-527). *Journal of Intelligent & Robotic Systems*.

Singh, K., & Verma, A. (2014). Applying OLSR routing in FANETs. In *Proceedings International Conference on Advanced Communication Control and Computing Technologies* (pp. 1212-1215). IEEE. 10.1109/ICACCCT.2014.7019290

Swarnapriyaa, U., Vinodhini, A. S., & Anand, R. (2011). Auto Configuration in Mobile Ad Hoc Networks (pp. 61-66). In *Proceedings of the National Conference on Innovations in Emerging Technology*.

Wang, Y., Chuang, C., & Hsu, C., & Hung, C. (2003). Ad hoc on-demand routing protocol setup with backup routes (pp. 137-141). In *Proceedings of ITRE, International Conference on Information Technology, Research, and Education*.

Xiang, X., Wang, X., & Yang, Y. (2011). Supporting Efficient and Scalable Multicasting over Mobile [IEEE Transactions on mobile computing.]. *Ad Hoc Networks*, 544–550.

Yap, W., Liu, J., Tan, S., & Goi, B. (2015). On the security of a lightweight authentication and encryption scheme for mobile ad hoc network. *International Journal of Security and Communication Networks*.

Zhang, X., & Jacob, L. (2003). *Multicast Zone Routing Protocol in Mobile Ad Hoc Wireless Networks*. Proc. Local Computer Networks.