ISSN: 0971-1260
Vol-22-Issue-16-August-2019

A Review Paper on Types, Applications , and Issues of Wireless Adhoc Networks

Gurpreet Singh
CSE
Lovely Professional University
gurpreet.17671@lpu.co.in

Ravinder Singh
CSE
Lovely Professional University
ravinder.17750@lpu.co.in

Amritpal Singh
CSE
Lovely Professional University
amritpal.17673@lpu.co.in

Abstract:

The Wireless Networks was invented in1970 under the supervision of Defence Advanced Research Projects Agency (DARPA) in United State of America. The first Wireless network is called as"Packet Radio Network" which was designed, built and performed by Bolt, Bernanke and Newman Technologies (BBN) and SRI International. This Packet Radio Network system anticipated the Internet and has played a measure role in motivating for the Internet Protocol suite. In1980's Survivable Radio Network (SURAN) project was successfully executed by DARPA. Packet Radio networks system did not progress much further until the wireless ad-hoc networks are innovated due to slower data rate, and it was inefficient in maintaining its links in high mobility condition and was bulky elements. Later in mid of 1990's the inexpensive802.11 radio card came for the use of personal computers. The roots of wireless technology are found in Military advancement. These days ad-hoc network are essentially produced for military utility.

I.Introduction:

Wireless communication are very useful to share information between devices without using any wired framework. By utilizing electromagnetic waves, mobile device can communicate through transmitting and receiving information over the wireless medium. Wireless communication expands from homes network to satellites communication, from Mobile communication to walkie-talkies communication. The wireless communication are becoming more popular because of its mobility, flexibility, simplicity and cost saving installation benefits, specifically from past few decades the mobility requirements of client are rising exponentially and growth in the usage of laptops, personal computer and personal digital appliance are itself the major cause for the acceptance of wire free network. The characterstics of Mobile adhoc networks are:

a) **Mobility: -** The most noticeable advantage of the wireless networks that users are able to roam

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

in the range and remain connected to the wireless network which means now while moving client can join to the current network also enjoy the freedom.

b) **Simplicity: -** All are able to convert simplicity into fast growth. It is straightforward to set up a Wire free network, in comparison to a network connected through wires.

c) **Flexibility: -** Wire free communicating network covers a large amount of range which can reach wherever wired infrastructure can't be deployed. This network is extremely helpful to those places where wired links are not practical like traditional block of buildings.

II.Types of Networks

Wireless network allows user to share information with each other, use application and access information in a wireless environment. It provide an ability to deliver the service of application to user through wireless medium. According to transmission range, three types of wireless network has been identified.

- Personal Area Network (PAN),
- Local Area Network (LAN),
- Wide Area Network (WAN).
- Wireless Local Area Network(WLAN)

a) Personal Area Network (PAN)

Personal Area Network are an interconnection of computing devices which are interested in transmitting information to another computing device (consisting laptop, personal digital appliance, extra.) near to each other in range. Usually Personal Area Networks are connected by the Bluetooth, Sensor node network and ZigBees.

It is a different kind of network, in which appliances will be interconnected to all appliances in network range which could be office or college. Wireless Local Area Network (WLAN) is a replacements to the traditional LAN linked through wires. Wired medium interconnected device have to communicate through physical medium like metals wire. Whereas in a Wireless Local Area Network nodes utilise air for transmission as a medium. WLANs have been authorized by IEEE.

b) Wide Area Network (WAN)

Wide Area Network comparatively covers a large amount of geographical area than above mention network type. For example between neighbouring city or neighbouring town. This type of networks could be applied to interconnect branches of offices of business or as public Internet access service system for public. The wireless

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

interconnections are established between access points by using microwave parabolic dish on 2.4 GHz band frequency not through Omni directional antennas usually used for smaller networks. Normally a Wide Area Network consist group of one or more LAN. 2nd Generation and 3rd Generation Cellular ad hoc Network, Paging Networks also Satellite Systems are some few examples of Wireless WANs (WWANs). Figure 1 illustrate interconnection of networks through wireless medium. One can access it personal computer in mobile or any equivalent device through wireless technology. Indeed Figure 1 shows the way wireless technology serve mobility, simplicity and flexibility

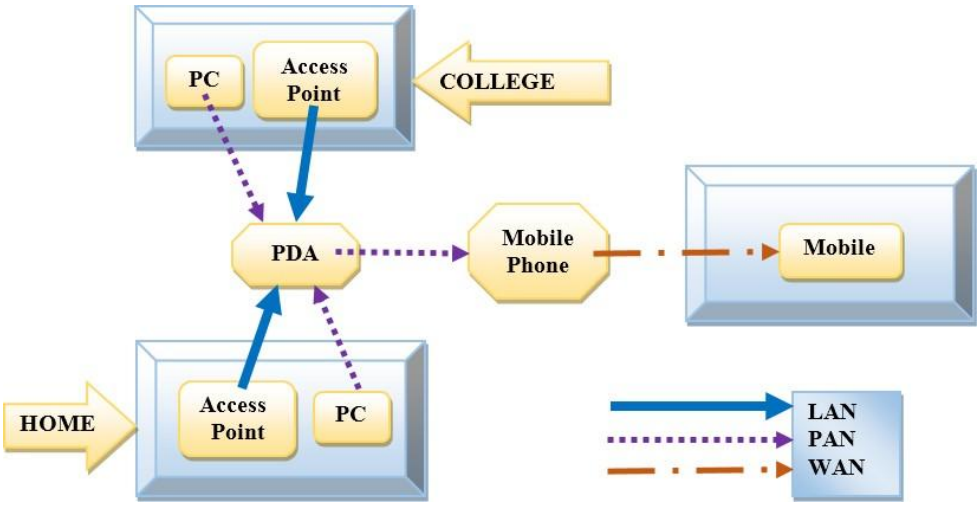

Figure 1: Wireless technology interconnection in diverse environments

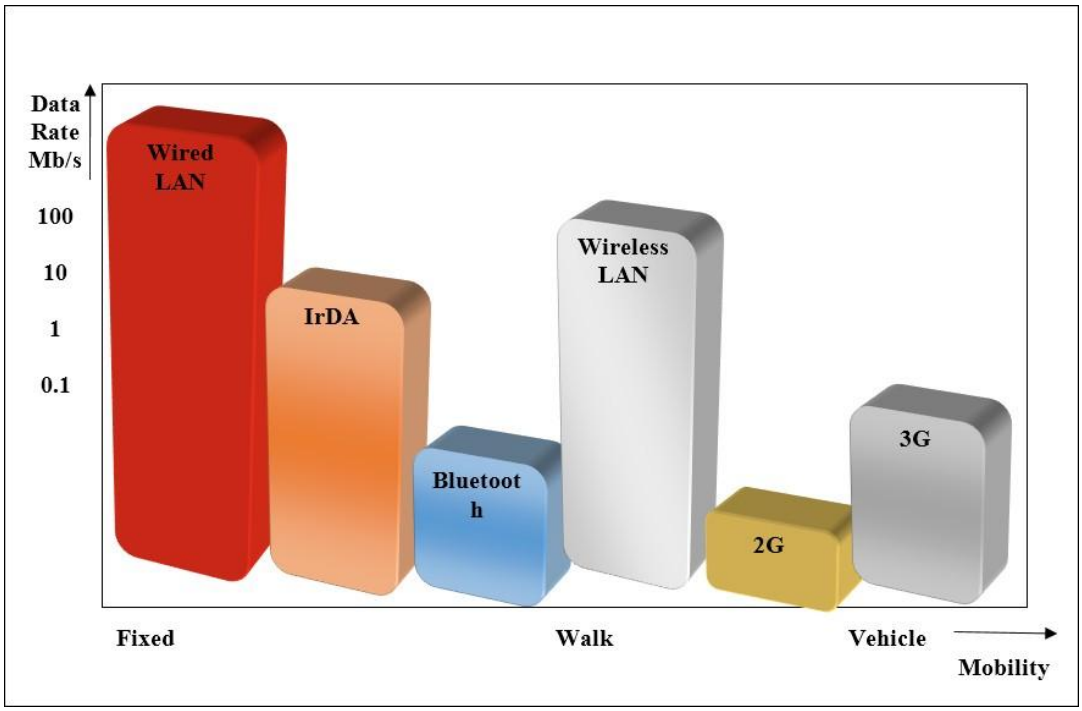

Figure 2: Graph of Data with rates and mobility for different wireless technology.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Figure 2 illustrate different kind of wireless technology communicating together and graph between data rates and mobility.

c) Wireless Local Area Network (WLAN)

Wireless Local Area Network is another possible option to traditional LAN which joins devices with wired nature of network. Wireless Local Area Network communicate message through air as a medium not through wired medium. A Wireless LAN is a shared medium transmission channel which propagate data packet via air as a medium for reach to every devices of network (e.g. personal digital appliance). WLAN is normally utilise interlinking the device to the Internet. Wire free internet access points (AP) are termed as "hot spots" and are in advance are utilise in teahouse and other public location of city for example aviation, railway and in many restaurant. Due to so many advantages, WLAN had acquire considerable recognition between moving clients to retrieve current information. In reality WLAN put into action in mobile devices for example laptops, personal digital appliance etc. for transmitting information among each other without any use of wire Ethernet IEEE 802.3. In a WLAN utilise wireless Ethernet protocol, IEEE 802.11 is utilize rather than wired Ethernet protocol, IEEE 802.3.

III.IEEE 802.11 Standards, Specifications and Technologies

IEEE . 802.11 specifications is associated with the family of IEEE 802 protocol that explains the specifications of fully functional Local Area Network (LAN) technologies. IEEE 802 specifications mainly concentrate on two lowest layers of the OSI model, the Medium Access Control (MAC) also known as Data Link and the physical (PHY) module which combine each other. In the IEEE standard of 802 series, the specifications of individuals are regulated after the point. 802.3, for example design of Carrier Sense Multiple Access network with Collision Detection (CSMA/CD) and Token-Ring specification is determined by 802.5.

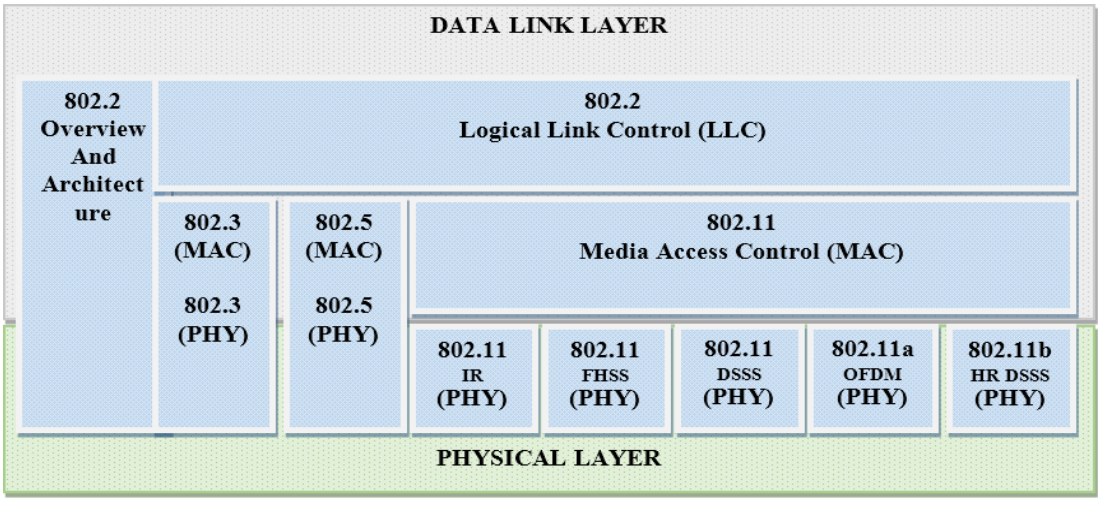

Figure 3: IEEE 802 family

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Figure 3 defines different types of component related to 802 family and relationships with the ISO models.

Figure 4: - Wi-Fi certified logos with SII

IEEE 802.11 technologies / specifications / standards is defined as Wireless Fidelity Wi-Fi. The Wi-Fi alliance had it as a trademark, WECA (Wireless Ethernet Compatibility Alliance) formed it as a non-profit organization. In 1999, Wi-Fi certification program was published by WECA. The products of any vendor of 802.11 using Wi-Fi certification can test for interoperability. Products which pass test are rewarded by Wi-Fi Certified logo with colour SII (standard Indicator Icon). Figure 4 represents the Wi-Fi certified logo with SII.

Dictionary of 802.11 Wireless Term

Station (STA): any wireless network Ethernet card enabled computing device is an 802.11 compliant device termed as Station.

Access Point (AP): The device which act as link between station and wired network while transmission of information also known as bridging function device is AP. **Wireless Distribution System (WDS***):* It is strong base of the device utilize for transmitting frames linked to access point.

Basic Service Set (BSS): It led foundation for 802.11 network, in this basically collection of stations shares information among one other.

Basic Service Area (BSA): It is a fuzzy space which can be determine through communication feature of wireless environment.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

IV.Wireless Local Area Network Modes

Let say only two station are present in a Basic Service Area and communicate within themself, these are elements of the Basic Service Set. The standard 802.11 has two Basic Service Set mode. These are define in Figure 5 and Figure 6 .

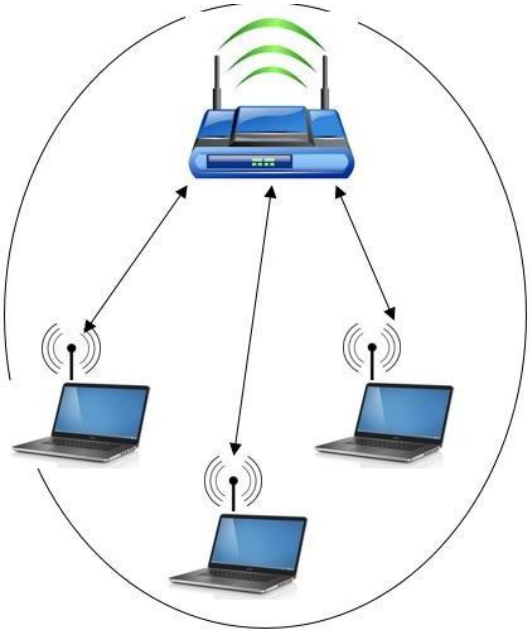

Figure 5: - Infrastructure Network

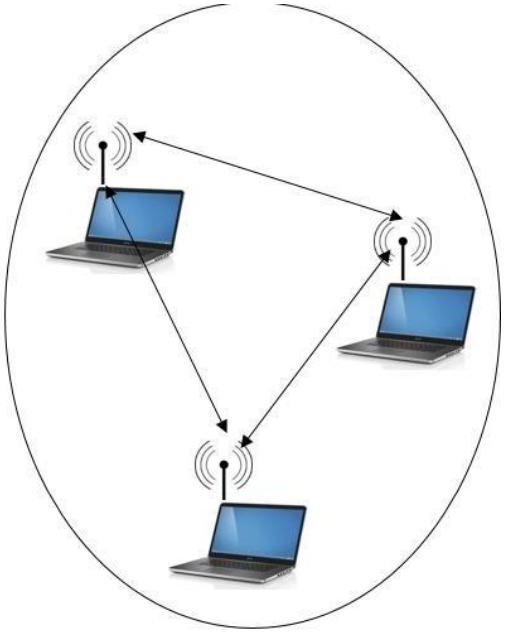

Figure 6: - Ad-hoc Network

These network is referred as Infrastructure Basic Service Set (Basic Service Set (BSS) is never called as Infrastructure Basic Service Set (IBSS)). It is a collection of access point, laptops, PDA and extra. It is more familiar arrangement highlighting that the WLAN doesn't change the wired LAN but increase the operation of wireless devices. A single access point is able to handle 15 to 200 user according to the configuration and technology. Stations during the same Basic Service Area (BSA) share information among one other through access point. Therefore, a station transfer information to another node at the two hops count.

First, frames of information packet are sent to the access point, then after reaching access point it process packet and then forwards the information packet to the destination station. The Basic Service Set (BSS), stations have to link themselves with the access point. Association operation of the infrastructure networks is exactly similar to connecting the cable to the wired network. Basic Service Sets (BSSs) normally covers minimum amount of space, for example offices and home. Figure 7 shows an Extended Service Set (ESS) which is made up of three Basic Service Sets (BSSs).

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

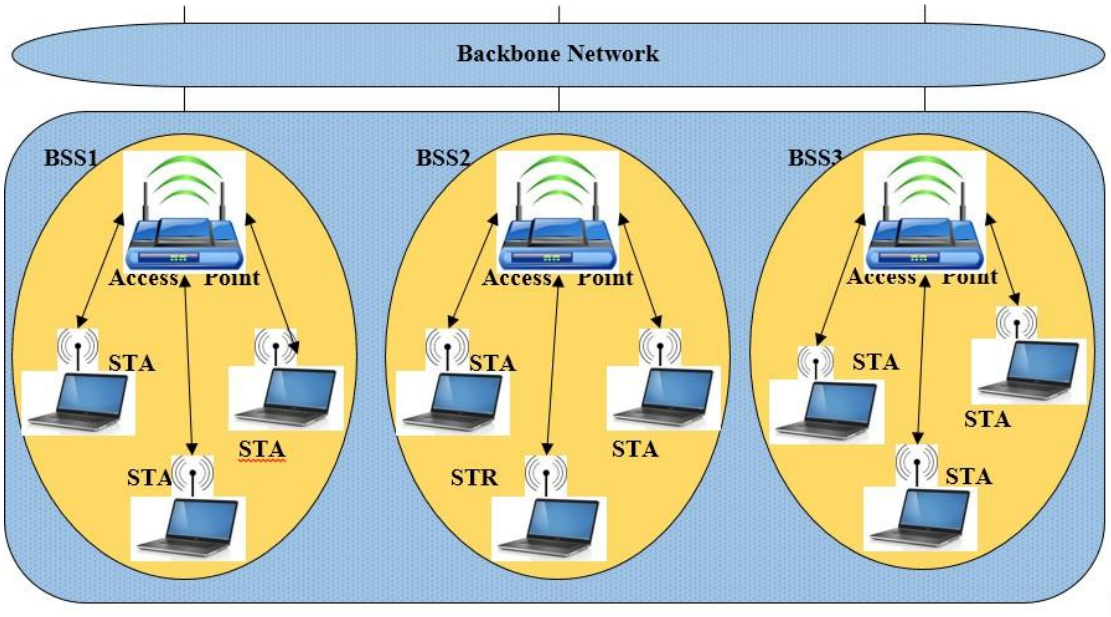

Figure 7: - Demonstration of Extended Service Set (ESS)

The major advantage of the 802.11 standards is the mobility of nodes.

Figure 8 represents the composition of these two operation in a Wireless Distribution System.

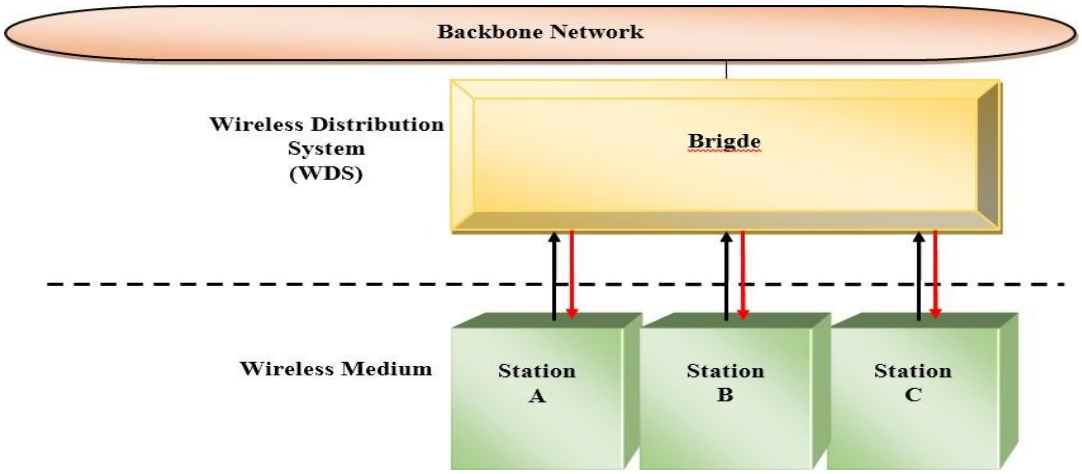

Figure 8: - Wireless Distribution System

V. Mobile Ad-Hoc Networks

The Wireless Local Area Networks (WLANs) allow to communicate over wireless channel, one device can send and receive data, like one can send voice and video to another device which is connected to same network. A precise class of standard which has controlled the market is Institute of Electrical and Electronics Engineers (*IEEE)*

802.11 wireless LAN, also called as Wireless-Fidelity (Wi-Fi). Wireless LAN networks can be in

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

action two modes:-

- Ad-Hoc mode in which the device itself act as routers and can create self- configuring networks by interconnecting wireless links, it also known as MobileAd-Hoc networks (MANET)
- Infrastructure mode in which the device are connected using wireless access point.

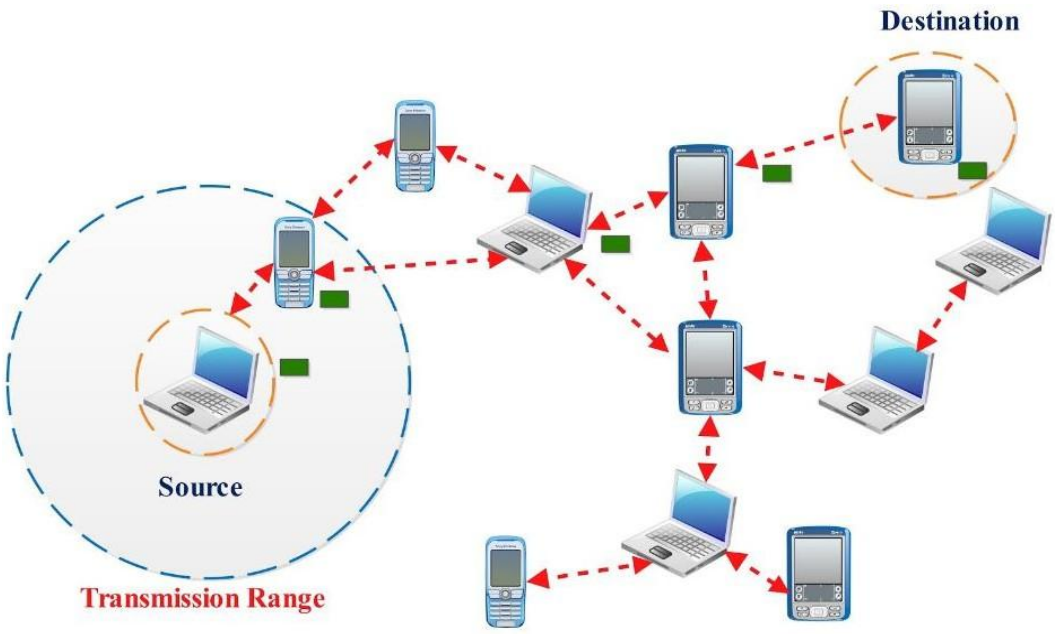

Figure 9: - Mobile Ad-Hoc Networks [21].

[MANET as illustrated by the Internet Engineering Task Force (IETF) MANET Working Group is a permanent or temporary self-governing network in which the nodes can freely move in any direction intending to establish to communication over wireless connection in absence of network infrastructure. [9]

The main function of MANETs is to facilitate wireless and mobile communication service without expensive service provider network and without network infrastructure set up. In this case the network is decentralised and the mobile Nodes should take care of network activities (network discovery) and should deliver the messages with each other by acting as router. In MANET nodes are capable of sensing the presence of other nodes present in the same network, establish connecting links among them and share or communicate information.

MANETs is a set of self-configured communicating node that can act as of data source, router and destination. The information can be directly communicated between source node to a destination node if the both nodes are in the range of each other. The range can vary according to the type of technology used for communication for example Bluetooth, Zigbee and Wi-Fi.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

VI.MANET Application

Followings are the major categorise of MANET application:

a) **Wireless Mesh Networks**: In these networks the broadband wireless connectivity is provided indoor as well as outdoor in rural, suburban and urban environments without any wired network infrastructure.

- **Public Safety System:** Wireless mesh networks can be used for addressing the requirements of law enforcing department and government such that catastrophe can be handle.

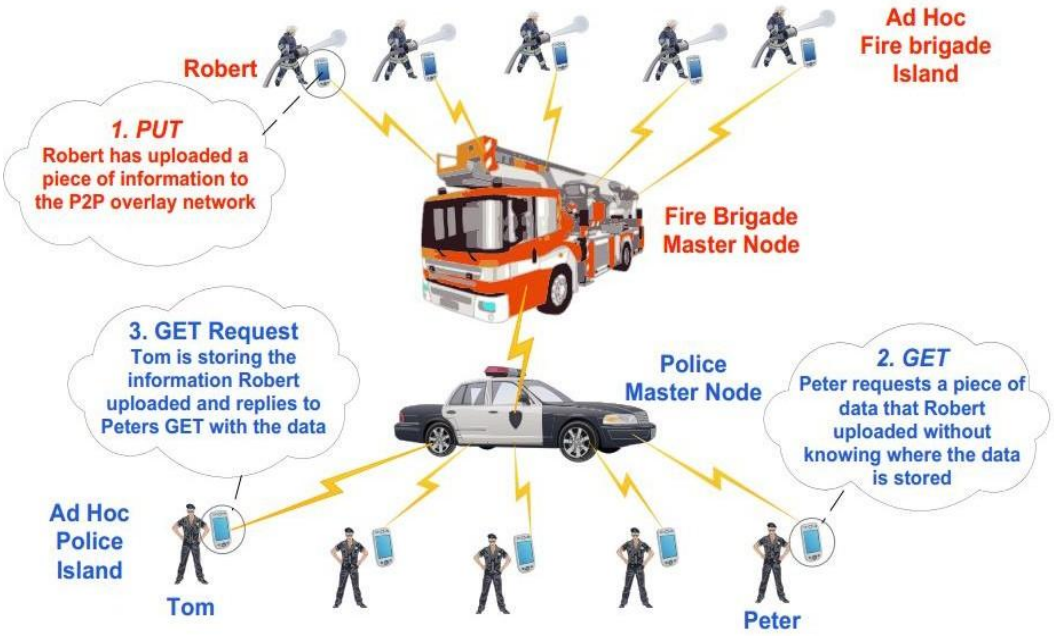

Figure 10: - Public Safety System data sharing [22].

- **Intelligent Transport System**: Wireless mesh networks helps in management of transport service, traffic can be easily manage, as it act as information delivery system.
- **Public Internet Access Networks:** Wireless mess networks are very helpful for providing broadband service in a town.
- **Health Monitoring**: Wireless sensors could be very useful as a part of health monitoring system connected with patient so that doctor and patient can communicate over wireless networks in order to check health status or send notification in case of emergency health condition.

b) **Wireless Sensor Networks:** In these networks nodes are battery powered with computing and communication abilities. Examples wireless sensor networks which communicate information between sensor nodes or to central entity are as follow:

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

- **Environmental monitoring:** Wireless sensors can be very useful in keeping up to date about environmental condition for handling it before getting uncontrollable such as forest fire detection, flood detection.
- **Smart homes**: In today's world the modern homes are having wireless sensor which can communicate with surrounding and people, providing smart home service, like smart lighting.
- **Tracking Application:** Wireless sensor service can be used to locate the location of person or object in specific area.

c) Vehicular Ad-Hoc Networks: these networks communicate take place between nodes and roadside device to assist safe driving, to avoid accident and to avoid traffic jams. In case of any accident it can propagate alert message to life saving service and also to divert traffic.

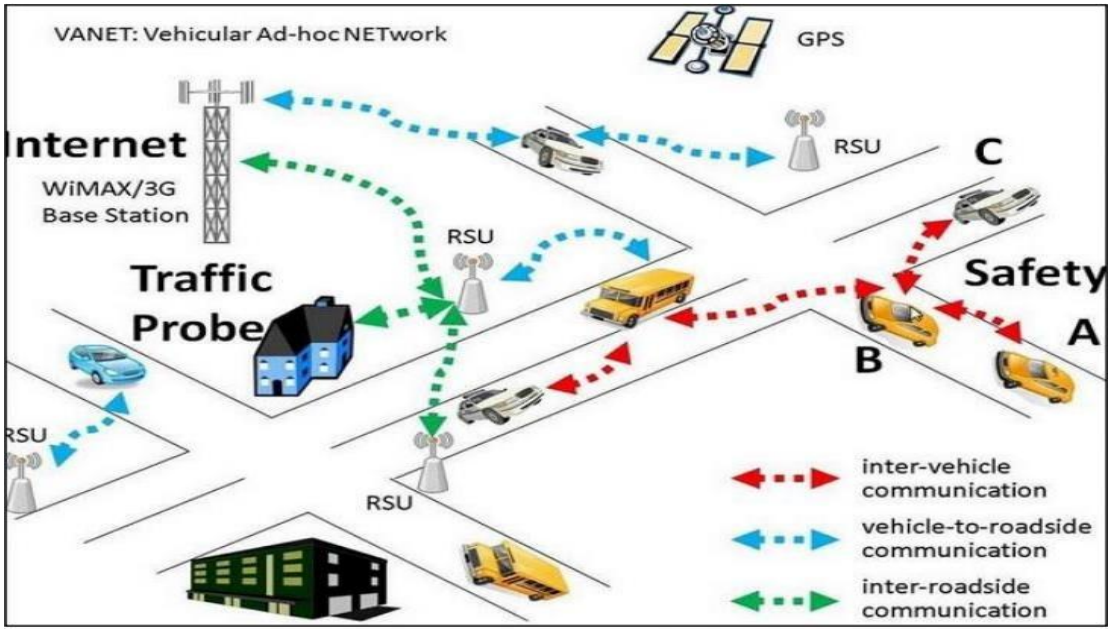

Figure 11: - Vehicular Ad-Hoc Networks [23].

d) Military Mobile Communication Networks: Battlefields does not consist infrastructure oriented networks due to its difficult terrain geography. In such condition wireless ad-hoc networks plays a major role for coordination among the military personnel and are easy to deploy in difficult terrain.[18]

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

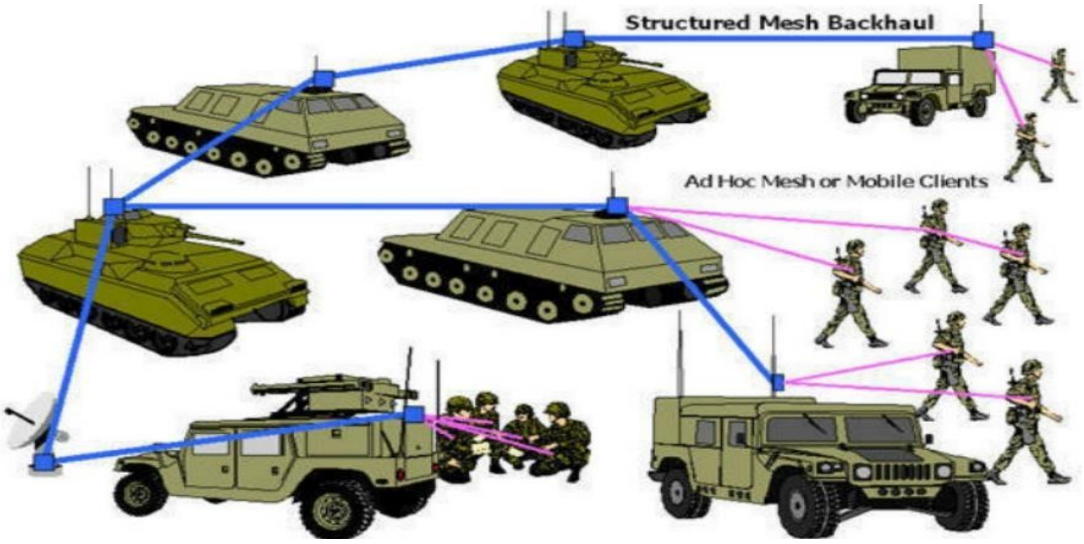

Figure12: - Military Mobile Communication Networks

VII. Issues in Mobile Ad-Hoc Networks

Mobile Ad-Hoc networks are not suitable to integrate with the present global internet. They are more vulnerable due its self-organizing nature of communication. Following are addressing some problems.

a) **Quality of Service:** Maintaining Quality of Service in wireless Ad-Hoc network is a difficult task due to its constantly changing topologies, the network condition in hostile environment are very complicated to maintain quality of service due to the limitation of mobile ad-hoc networks.

b) **Security:** Mobile ad-hoc network is generally more vulnerable than any other wired networks. The designer have designed without keeping security in their mind, they have assumed all nodes in the network will behave in a friendly manner and there will be not any threat to nodes and data packets.

c) **Routing:** In mobile ad-hoc network have one major problem that is routing to have seamless connectivity to other nodes in its surrounding environment. Each node have to behave like a router to forward the data packets to allow information sharing among the moving nodes.

VIII. Conclusion

MANETs are capable of offering efficient and effective communication system in those area which are not in the range of permanent network infrastructure. Due to integral design faults, it affects the security mechanism of routing protocol of the network. There are wide applications of Mobile adhoc networks like smart homes , environmental use , intelligent transport system and so on. But there are various issues that need to take care in adhoc networks. Quality of Service Metrics are the basic parameters of quality for a network. Quality of Service parameter consist security, bandwidth, jitter, availability

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

network availability, delay, packet loss and battery life. Similarlarly confidentiality ensures that the content of message will never be disclose to MANETs entities that are not permitted to interpret it. Due to MANET wireless mode of communication the links are vulnerable to eavesdropping, confidentiality are very critical for protecting the transmitting private information.

IX. References

[1] Salwa othmen, Faouzi, Aymen Belghith, lotfi kamoun, "Energy , Load and QoS-aware Routing protocol for Ad-Hoc NetworkS", IEEE, 978-1-5090-0304- 4, 2016.

[2] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, "A Novel encounter based trust evalution for AODV routing in MANET", IEEE, 978-1-4799-1848-5, 2016.

[3] Siddharth Dhama, Sandeep Sharma, Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", IEEE, 978-9-3805-4421-2, 2016.

[4] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Attacks against AODV routing protocol in MANET",IEEE, 978-15090-0811- 7, 2016.

[5] Sagar R. Deshmukh, Dr. P. N. Chatur, "Secure Routing to Avoid Black Hole Affected Routes in MANET", IEEE, 978-1-5095-0669-4, 2016.

[6] Zne-jung lee, So-Tsung Chou,Chou-Yuan lee, "AODV with intelligent priority flow scheme for multi-hop ad-hoc netnork" , Springer, 40595-016-0072-2, 2016.

[7] Sweta Dixit, Priya Pathak, Sandeep Gupta, " A Nonel Approch for Gray hole And Black hole Detection And Prevention ", IEEE, 978-1-5095-0669-4, 2016.

[8] Apurva Jain, Urmila Prajapati, Piyush Chouhan, "Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario", IEEE, 978-1-5090-0669-4, 2016.

[9] Dhiraj Nitnaware, Anita Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET", IEEE, 978-1-4673-9197-9, 2016.

[10] Sushama Singh, Atish Mishra, Upendra Singh, " Detecting and Avoiding Of collaborative Black hole attack on MANET using Trusted AODV Routing ", 2016, IEEE, 978-1-5090-0669-4, 2016.

[11] N.Venkatadri, K.Ramesh Reddy, "Secure TORA: Removal of Black Hole Attack using Twofish Algorithm", IEEE, 978-1-8286-1, 2016.

[12] Priya Sethuraman, N. Kannan, "Refined trust energy ad-hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET", Springer, 2016.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[13] S.H. Jayachandra, R. Manjunatha, "Analysis of Black hole attack using AODV", Springer, 2016.

[14] Balram swami, Ravindra Singh," Simulation Based compression Between MOWL, AODV and DSDV using NS2", Springer, 978-3-319-30927-9, 2016.

[15] Sathish M, Harikrishnan V S, Arumugam K, S.Neelavathy Pari, "Detection of Single and Collaborative Black Hole Attack in MANET ", IEEE, 978-1-4673- 9338-6, 2016.

[16] R.Priyanka, P.Ramkumar, "Trust based detection algorithm to mitigate the attacker nodes in MANET" , IEEE, 978-1-5090-0669-3, 2016.

[17] Bikramjeet Singh, Dasari Srikanth , C.R. Suthikshn Kumar "Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective" ,IEEE, 978-1-4673-9916-6, 2016.

[18] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack" , IEEE, 978-1-4673-7689-1, 2016.

[19] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Ad-hoc Networks: A Survey", Springer, 95616, 2016.

[20] Lathies Bhasker T," A Scope for MANET Routing and Security threats", ICTACT ISSN: 2229-6948, 2013.

[21] Chaitali Biswas Dutta & Utpal Biswas. An energy aware blackhole attack for multipath AODV. In Business and Information Management (ICBIM), 2014 2nd International Conference. IEEE (2014)

[22] Emmanouil A. Panaousis, "Security for Mobile Ad-hoc Networks", book 2012.

[23] Chaitali Biswas Dutta & Utpal Biswas. A novel blackhole attack for multipath AODV and its mitigation. In Recent Advances and Innovations in Engineering (ICRAIE-2014), International Conference. IEEE (2014)