International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

New trends in Mobile Ad hoc Network

Gaikwad Ranjitkumar Sharnappa
Bheemanna Khandre Institute of Technology, Bhalki
Department of Electronics and Communication Engineering
ranjitkumargs@gmail.com

Abstract **- Mobile ad hoc networks (MANETs) concept is not a new one, it is deployed in 1990's. In the past few years, we have seen a rapid expansion in the field of mobile computing due to inexpensive and widely availability of wireless devices. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET. This paper will address the overview of mobile ad hoc network, potential applications of ad hoc networks, discusses technological challenges, protocols and also presents the security goals defined in the mobile ad hoc network.**

Keywords: **Mobile Ad hoc Network, applications, technological challenges, Protocols, Security**

1. INTRODUCTION

Wireless communications are a very popular application domain. Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. Ad hoc wireless communication between devices might be loosely defined as a scheme, often referred to as ad hoc networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure [1]. Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program [2]. In ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply.

The field of wireless and mobile communications has experienced an unprecedented growth during the past decade from 2G to 4G with high speed, enabling worldwide mobile connectivity. Mobile users can use their cellular phone to check their email and browse the Internet. Recently, an increasing number of wireless local area network hot spots are emerging, allowing travelers with portable computers to surf the Internet from all public places.

A key feature of wireless networks is the ability to operate without fixed, wired communications infrastructure, supports emergency requirements, short term needs and coverage areas. The applications of this wireless network are to public, disaster recovery, law enforcement and battlefield.

In an ad hoc network, mobile nodes cooperate to forward packets for each other, allowing nodes to communicate beyond their direct wireless transmission range. Many proposed routing protocols for ad hoc networks operate in an on-demand fashion, as on-demand routing protocols have been shown to often have lower overhead and faster reaction time than other types of routing based on periodic mechanisms. Significant attention recently has been devoted to developing secure routing protocols for ad hoc networks, including a number of secure on demand routing protocols that defend against a variety of possible attacks on network routing.

2. MOBILE AD HOC NETWORKS

2.1 What Is Mobile Ad Hoc Network

Ad hoc network is used many different ways. Followings are the definitions given by the Internet engineering Task Force, National Institute of Standard and Technology and INTEC. In MANETs, the wireless nodes are free to move and still connected using the multi hop with no infrastructure support. The goal of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Ad hoc networks have fixed routers: all nodes are capable of movement and can be connected dynamically in arbitrary manner. Nodes of these networks function as routers, which discover and maintain routes to other nodes in the network.

2.2 History of MANET

The roots of ad hoc networking can be traced back as far as 1968, when work on the ALOHA network was initiated. The ALOHA protocol itself was a single-hop protocol i.e. it did not inherently support routing. Instead every node had to be within reach of all other participating nodes. Inspired by the ALOHA network and the early development of fixed network packet switching, DARPA began work, in 1973. PRnet provided mechanisms for managing operation centrally as well as on a distributed basis. As an additional benefit, it was realized that multihopping techniques increased network capacity, since the spatial domain could be reused for concurrent but physically separate multihop sessions. In 1980s ad hoc networks was further enhanced and implemented as a part of SURAN (Survivable Adaptive Radio Networks) project that aimed at providing ad hoc networking with small, low cost, low power devices with efficient protocols for improved scalability and survivability. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

In the 1990s, the concept of commercial ad hoc network arrived with notebook computers and other viable communication equipment. The IEEE 802.11 subcommittee had adopted the term "ad hoc networks" and research community had started to look the possibility of deploying applications.

2.3 IEEE 802.11 Networks

In 1997, the IEEE adopted the first wireless local area network standard, named IEEE 802.11, with data rates up to 2 Mbps [4]. In late 1999, two new addenda were released. The 802.11b specification increased the performance to 11 Mbps in the 2.4 GHz range while the 802.11a specification utilized the 5 GHz range and supported up to 54 Mbps. Unfortunately, the two new specifications were incompatible because they used different frequencies. This means that 802.11a network interface cards (NICs) and access points cannot communicate with 802.11b NICs and access points. This incompatibility forced the creation of the new draft standard known as 802.11g. 802.11g supports up to 54 Mbps and is interoperable with 802.11b products on the market today.

802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance. It is also backward compatible with 802.11b and will work with both 11 and 22 Mbps. 802.11g offers the best features of both 802.11a and 802.11b.

Wireless networks are classified into two types Infrastructure based and infrastructure less networks. The infrastructured networks have fixed and wired gateways or fixed base stations through wires as shown in fig1. Example wireless LAN and mobile phones.

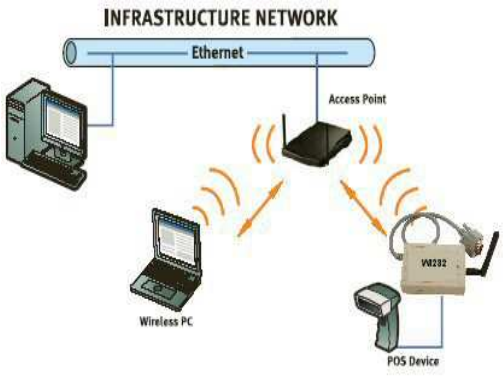

Fig. 1 Infrastructured mode wireless network

The second type infrastuctureless is known as Mobile Ad-hoc networks, these networks have no fixed routers and every node could be router as shown in fig2. The entire network is mobile, and the individual terminals are allowed move freely. In this type of network, some pairs of terminals may not able to communicate directly with each other and have to rely on some terminals so that the messages are delivered to destinations. Such networks are referred to as multi-hop or store and forward networks. The nodes of these networks function as routers, which discover and maintain routes to other nodes in the networks.

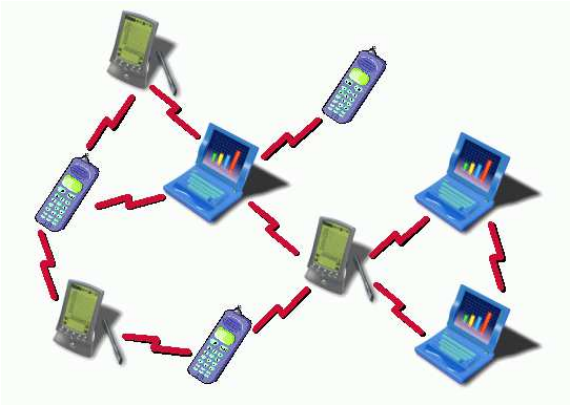

Fig. 2 Infrastructure less mode wireless network

3. APPLICATIONS OF MANET

There are many applications of MANET's in day today life such as emails; file sharing can be considered to be within an ad hoc network. Web services are also possible in case any node in the network can serve as a gateway to the outside world [5]. In this article we summarize following some of the applications.

3.1 Tactical Networks:

Military equipment now contains some sort of computer equipments. Ad hoc networking can be very useful in establishing communication among a group of soldiers and also maintain an information network between the soldiers, vehicles and military information headquarters. These networks also fulfill the requirements of communication mechanism very quickly because they setup without infrastructure which is easy to military troops to communicate.

3.2 Commercial:

The ad hoc network is used in emergency rescue operation. As medical teams requires fast and effective communication when they are in disaster area to treat patients. They cannot afford the time to lie cabling and hardware installation. They can employ laptops and PDAs and communicate via wireless link to remote medical expert team.

3.3 local level:

Ad hoc network can be used to spread and share information among the participants at conferences, meeting or classrooms with the help of notebook or palmtops.

3.4 PAN:

It is the interconnection of devices within the range of 10m. From the traditional mobile network, a Bluetooth-based PAN opens up a new way of extending mobile networks. Someone on a trip who has access to a Bluetooth PAN could use the GPRS/UMTS mobile phone as a gateway to the Internet or to a corporate IP network. In terms of traffic load in the network,

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

the aggregate traffic of the PAN would typically exceed that of the mobile phone. In addition, if Bluetooth PANs could be interconnected with scatter nets, this capacity would be increased. Figure 3 shows a scenario in which four Bluetooth PANs are used. The PANs are interconnected via laptop computers with Bluetooth links. In addition, two of the PANs are connected to an IP backbone network, one via a LAN access point and the other via a single GPRS/UMTS phone. A PAN can also encompass several different access technologies distributed among its member devices which exploit the ad hoc functionality in the PAN. For instance, a notebook computer could have a wireless LAN interface that provides network access when the computer is used indoors. Thus, the PAN would benefit from the total aggregate of all access technologies residing in the PAN devices.

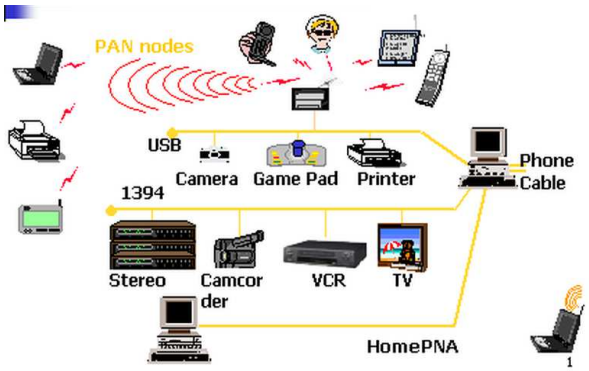

Fig. 3 Personal Area Network

3.5 Other Applications: [3]

Entertainment	• Wireless P2P networking • Outdoor Internet access • Robotic pets • Theme parks • Multi-user games
Sensor networks	• Home applications: smart sensors and actuators embedded in consumer electronics • Body area networks (BAN) • Data tracking of environmental conditions, animal movements, chemical/biological detection
Context aware services	• Follow-on services: call-forwarding, mobile workspace • Information services: location specific services, time dependent services • Infotainment: touristic information
Coverage extension	• Extending cellular network access • Linking up with the Internet, intranets, etc.

4. TECHNOLOGICAL CHALLENGES

Following are the challenges are faced by the MANETs. Which are broadly classified are as follows. These challenges are posed by broad range of environments such as cellular data services [6].

4.1 Spectrum Allocation and Purchase

Regulations regarding the use of radio spectrum are under control of the Federal Communications Commission. Most experimental ad hoc networks are based on the ISM band. To prevent interference, ad hoc networks must operate over some form of allowed or specified spectrum range. Most microwave ovens operate in the 2.4GHz band, which can therefore interfere with wireless LAN systems.

4.2 Media Access

Unlike cellular networks, there is a lack of centralized control and global synchronization in ad hoc wireless networks. Hence, TDMA and FDMA schemes are not suitable. In addition, many MAC (Media Access Control) protocols do not deal with host mobility. As such, the scheduling of frames for timely transmission to support QoS is difficult.

In ad hoc wireless networks, since the same media are shared by multiple mobile ad hoc nodes, access to the common channel must be made in a distributed fashion, through the presence of a MAC protocol. Given the fact that there are no static nodes, nodes cannot rely on a centralized coordinator. The MAC protocol must contend for access to the channel while at the same time avoiding possible collisions with neighboring nodes. The presence of mobility, hidden terminals, and exposed nodes problems must be accounted for when it comes to designing MAC protocols for ad hoc wireless networks.

4.3 Routing

The presence of mobility implies that links make and break often and in an in deterministic fashion. Note that the classical distributed Bellman-Ford routing algorithm is used to maintain and update routing information in a packet radio network. While distance-vector-based routing is not designed for wireless networks, it is still applicable to packet radio networks since the rate of mobility is not high. The bulky and heavy construction of these radios makes them less mobile once deployed. However, advances in microelectronics technology have enabled the construction of small, portable, and highly integrated mobile devices. Hence, ad hoc mobile networks are different from packet radio networks since nodes can move more freely, resulting in a dynamically changing topology. Existing distance-vector and link-state-based routing protocols are unable to catch up with such frequent link changes in ad hoc wireless networks, resulting in poor route convergence and very low communication throughput. Hence, new routing protocols are needed.

4.4 Multicasting

The explosion in the number of Internet users is partly attributed to the presence of video and audio conference tools.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Such multiparty communications are enabled through the presence of multicast routing protocols. The multicast backbone comprises an interconnection of multicast routers that are capable of tunneling multicast packets through non-multicast routers. Some multicast protocols use a broadcast-and-prune approach to build a multicast tree rooted at the source. Others use core nodes where the multicast tree originates. All such methods rely on the fact that routers are static, and once the multicast tree is formed, tree nodes will not move. However, this is not the case in ad hoc wireless networks.

4.5 Energy Efficiency

Most existing network protocols do not consider power consumption an issue since they assume the presence of static hosts and routers, which are powered by mains. However, mobile devices today are mostly operated by batteries. Battery technology is still lagging behind microprocessor technology. The lifetime of a Li-ion battery today is only 2-3 hours. Such a limitation in the operating hours of a device implies the need for power conservation. In particular, for ad hoc mobile networks, mobile devices must perform both the role of an end system and that of an intermediate system (packet forwarding). Hence, forwarding packets on the behalf of others will consume power, and this can be quite significant for nodes in an ad hoc wireless network.

4.6 TCP Performance

TCP is an end-to-end protocol designed to provide flow and congestion control in a network. TCP is a connection-oriented protocol; hence, there is a connection establishment phase prior to data transmission. The connection is removed when data transmission is completed. In the current Internet, the network protocol (Internet Protocol or IP) is essentially connectionless; therefore, having a connection-oriented, reliable transport protocol over an unreliable network protocol is desirable. However, TCP (Transmission Control Protocol) assumes that nodes in the route are static, and only performs flow and congestion activities at the SRC and DEST nodes.

TCP relies on measuring the round-trip time (RTT) and packet loss to conclude if congestion has occurred in the network. Unfortunately, TCP is unable to distinguish the presence of mobility and network congestion. Mobility by nodes in a connection can result in packet loss and long RTT. Hence, some enhancements or changes are needed to ensure that the transport protocol performs properly without affecting the end-to-end communication throughput.

4.7 Service Location, Provision, and Access

While protocols are important for the proper operation of an ad hoc wireless network, service location, provision, and access are equally important. Should we continue to assume that the traditional client/server RPC (remote procedure call) paradigm is appropriate for ad hoc networks? Ad hoc networks comprise heterogeneous devices and machines and not everyone is capable of being a server. The concept of a client initiating task requests to a server for execution and awaiting results to be returned may not be attractive due to limitations in bandwidth and power. Perhaps the concept of remote programming as used in mobile agents is more applicable since this can reduce the interactions exchanged between the client and server over the wireless media. Also, how can a mobile device access a remote service in an ad hoc network? How can a device that is well-equipped advertise its desire to provide services to the rest of the members in the network? All these issues demand research.

4.8 Security & Privacy

Ad hoc networks are intranets and they remain as intranets unless there is connectivity to the Internet. Such confined communications have already isolated attackers who are not local in the area. Note that this is not the case for wired and wireless-last hop users. Through neighbor identity authentication, a user can know if neighboring users are friendly or hostile. Information sent in an ad hoc route can be protected in some way but since multiple nodes are involved, the relaying of packets has to be authenticated by recognizing the originator of the packet and the flow ID or label.

5. ROUTING PROTOCOLS USED BY MANETS

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. The protocols were carefully implemented according to their specifications published as of April 1998 and based on clarifications of some issues from the designers of each protocol and on our own experimentation with them [7].

There are different types of protocols each of them are applied according their need. In this section, we review some of the important protocols used by ad hoc networks. Following are the classifications of routing protocols.

5.1 Proactive Routing Protocols

Proactive routing protocols are also called as table driven routing protocols. In this every node maintain routing table which contains information about the network topology even without requiring it. This feature although useful for datagram traffic, incurs substantial signaling traffic and power consumption. The routing tables are updated periodically whenever the network topology changes. Proactive protocols are not suitable for large networks as they need to maintain node entries for each and every node in the routing table of every node. These protocols maintain different number of routing tables varying from protocol to protocol. Following are various well known proactive routing protocols

i. Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV) is developed on the basis of Bellman–Ford routing [8] algorithm with some modifications. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So the routing information updates might either be periodic or event driven. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors. The advertisement is done either by broadcasting or by multicasting. By the advertisements, the neighboring nodes can know about any change that has occurred in the network due to the movements of nodes. The routing updates could be sent in two ways: one is called a "full dump" and another is "incremental." In case of full dump, the entire routing table is sent to the neighbors, where as in case of incremental update, only the entries that require changes are sent.

ii) Wireless Routing Protocol (WRP)

WRP described as table based protocol with the goal of maintain routing information among all nodes in network [5]. It belongs to the general class of path-finding algorithms, defined as the set of distributed shortest path algorithms that calculate the paths using information regarding the length and second-to-last hop of the shortest path to each destination. WRP reduces the number of cases in which a temporary routing loop can occur. For the purpose of routing, each node maintains four things: 1. A distance table 2. A routing table 3.A link-cost table 4. A message retransmission list (MRL). WRP uses periodic update message transmissions to the neighbors of a node. The nodes in the response list of update should send acknowledgments. If there is no change from the last update, the nodes in the response list should send an idle Hello message to ensure connectivity. A node can decide whether to update its routing table after receiving an update message from a neighbor and always it looks for a better path using the new information. If a node gets a better path, it relays back that information to the original nodes so that they can update their tables. After receiving the acknowledgment, the original node updates its MRL. Thus, each time the consistency of the routing information is checked by each node in this protocol, which helps to eliminate routing loops and always tries to find out the best solution for routing in the network.

iii) Cluster Gateway Switch Routing Protocol (CGSR)

CGSR [4] considers a clustered mobile wireless network instead of a flat network. For structuring the network into separate but interrelated groups, cluster heads are elected using a cluster head selection algorithm. By forming several clusters, this protocol achieves a distributed processing mechanism in the network. However, one drawback of this protocol is that, frequent change or selection of cluster heads might be resource hungry and it might affect the routing performance. CGSR uses DSDV protocol as the underlying routing scheme and, hence, it has the same overhead as DSDV. However, it modifies DSDV by using a hierarchical cluster-head-to-gateway routing approach to route traffic from source to destination.

5.2 Reactive Routing Protocols.

Reactive routing protocol is also known as on demand routing protocol. These protocols depart from the legacy Internet approach. To reduce the overhead, the route between two nodes is discovered only when it is needed [4]. Representative reactive routing protocols include:

a. *Dynamic Source Routing (DSR) protocol*: is based on the link state algorithm in which source initiates route discovery on demand basis. The sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet.

b. *Ad Hoc On-Demand Distance Vector Routing (AODV)* is basically an improvement of DSDV. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. The reply is sent using the reverse path. For route maintenance, when a source node moves, it can reinitiate a route discovery process. If any intermediate node moves within a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. This process continues until the failure notification reaches the source node. Based on the received information, the source might decide to re-initiate the route discovery phase.

c. Associativity-Based Routing (ABR): protocol defines a new type of routing metric "degree of association stability" for mobile ad hoc networks. In this routing protocol, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased. A high value of associativity tick for any particular beaconing node means that the node is relatively static. Associativity tick is reset when any neighboring node moves out of the neighborhood of any other node.

d. Signal Stability–Based Adaptive Routing Protocol (SSA) SSA protocol focuses on obtaining the most stable routes through an ad hoc network. The protocol performs on demand route discovery based on signal strength and location stability. Based on the signal strength, SSA detects weak and strong channels in the network. SSA can be divided into two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

e. Temporarily Ordered Routing Algorithm (TORA) TORA is a reactive routing protocol with some proactive enhancements where a link between nodes is established creating a Directed Acyclic Graph (DAG) of the route from the source node to the destination. This protocol uses a link reversal model in route discovery. A route discovery query is broadcasted and propagated throughout the network until it reaches the destination or a node that has information about how to reach the destination.

5.3 Hybrid Routing Protocol [5]

There is a trade-off between proactive and reactive protocols. Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So a Hybrid protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols. Hybrid routing protocol is combination of both proactive and reactive routing protocol. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Hybrid protocol is suitable for large networks where large numbers of nodes are present. Following are popular HRP.

a. Zone Routing Protocol (ZRP) ZRP is suitable for wide variety of MANETs, especially for the networks with large span and diverse mobility patterns. In this protocol, each node proactively maintains routes within a local region, which is termed as routing zone. Route creation is done using a query-reply mechanism. For creating different zones in the network, a node first has to know who its neighbors are. A neighbor is defined as a node with whom direct communication can be established, and that is; within one hop transmission range of a node. Neighbor discovery information is used as a basis for Intra-zone Routing Protocol (IARP). Rather than blind broadcasting, ZRP uses a query control mechanism to reduce route query traffic by directing query messages outward from the query source and away from covered routing zones. A covered node is a node which belongs to the routing zone of a node that has received a route query. During the forwarding of the query packet, a node identifies whether it is coming from its neighbor or not. If yes, then it marks all of its known neighboring nodes in its same zone as covered. The query is thus relayed till it reaches the destination. The destination in turn sends back a reply message via the reverse path and creates the route.

b. Sharp Hybrid Adaptive Routing Protocol (SHARP) SHARP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. This protocol defines the proactive zones around some nodes. The number of nodes in a particular proactive zone is determined by the node-specific zone radius. All nodes within the zone radius of a particular node become the member of that particular proactive zone for that node. If for a given destination a node is not present within a particular proactive zone, reactive routing mechanism (query-reply) is used to establish the route to that node. Proactive routing mechanism is used within the proactive zone. Nodes within the proactive zone maintain routes proactively only with respect to the central node. In this protocol, proactive zones are created automatically if some destinations are frequently addressed or sought within the network. The proactive zones act as collectors of packets, which forward the packets efficiently to the destination, once the packets reach any node at the zone vicinity

6. SECURITY ISSUES

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. Here, system constraints include low-power, small memory and bandwidth, and low battery power.

6.1.1 Types of Attacks

Attacks against ad hoc networks can be divided into two groups: Passive attacks typically involve only eavesdropping of data. Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. External attacks are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer.

6.1.2 Denial of Service

The denial of service threat either produced by an unintentional failure or malicious action forms a severe security risk in any distributed system.

6.1.3 Impersonation

Impersonation attacks form a serious security risk in all levels of ad hoc networking. If proper authentication of parties is not supported, compromised nodes may in network layer be able to e.g. join the network undetectably or send false routing information masqueraded as some other, trusted node. Within network management the attacker could gain access to the configuration system as a super user. In service level, a malicious party could have its public key certified even without proper credentials

6.1.4 Disclosure

Any communication must be protected from eavesdropping, whenever confidential information is exchanged. Also critical data the nodes store must be protected from unauthorized access. In ad hoc networks such

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

information can include almost anything e.g. specific status details of a node, the location of nodes, private or secret keys, passwords and -phrases and so on. Sometimes the control data is more critical information in respect of the security than the actual exchanged data. For instance the routing directives in packet headers such as the identity or location of the nodes can sometimes be more valuable than the application-level messages.

6.2 Security goals

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation [9].

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

7. FUTURE VIEW

It is sometimes useful to try to predict the future to get new ideas and see the present day in a more appropriate context on larger scale. Future is unknown, but it is, after all, the result of the actions we take now. Future airs of mobile ad hoc network anytime anywhere communication. As the research goes on the nodes in MANET will be smaller, cheaper and capable. They are likely to play larger roles in the future, with 4G network. Future mobile networks will use mobile routers to provide internet connectivity to ad-hoc users.

8. CONCLUSION

In this article we have clarified that what is ad hoc networks. It's intrinsic flexibility, lack of infrastructure, ease of deployment, auto-configuration, low cost and potential applications make it an essential part of future pervasive computing environments. The mobile ad hoc network will become widely used in military contexts in near future; the corporate world has to continue the daunting search for profitable commercial applications and possibilities of the technology. The research in this field will continue being very active and imaginative. Therefore we may conclude that futures network is mobile ad hoc network.

ACKNOWLEDGEMENT

I would like to thank Principal Dr. B. B. Lal, BKIT bhalki. I would like to also thank HOD of ECE dept. Dr. C. M. Tawade, Prof. C. Kalpana, all other staffs for motivating, all collogues and not but the least Mr. Dandvate Ajayji, Prof. Bachewar B. G. for inspiring me and Prof. Awale S. for their valuable guidance.

REFERENCES

[1] Magnus Frodigh, Per Johansson and Peter Larsson, "Wireless ad hoc networking - The art of networking without a network," Ericsson Review No. 4, 2000.

[2] Lu Han, "Wireless Ad-hoc Networks", October 8, 2004.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges".

[4] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", 2003

[5] Carlos de Morais Cordeiro and Dharma P. Agrawal, "Mobile Ad Hoc Networking", OBR Research center for distributed and mobile computing, ECECS.

[6] Vikran Patalbansi, Sonali Mote, Vijayalaxmi Kondal, "Mobile Ad Hoc Networks: Opportunities and Future"

[7] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Jorjeta Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols".

[8] Mueen Uddin, Azizah Abdul Rahman, Abdulrahman Alarifi, Muhammad Talha, Asadullah Shah, Mohsin Iftikhar, and Albert Zomaya, "Improving Performance Of Mobile Ad Hoc Networks Using Efficient Tactical On Demand Distance Vector (Taodv) Routing Algorithm" International Journal of Innovative Computing, Information and Control Volume 8, Number 6, June 2012

[9] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", Cornell University, Ithaca, NY 14853