Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Mobile Ad hoc Networks (MANETs): Challenges, Applications & Security Goals with Minute Introduction of Routing Protocols

Esha Sehgal[1],
Research Scholar,
Venkteshwara University- Gajraula,
Amroha (U.P.), India

Sohan Garg[2]
Professor,
IIMT Management College-Meerut
Merut, India

Abstract: ***Mobile ad hoc network is a temporal wireless network dynamically formed by a group of mobile hosts. These hosts have capabilities of dynamical discovery, orientation and recovery link automatically. They can do the basic network functions of routing, forwarding and service discovery under the non-infrastructure environment Mobile ad hoc networks have many advantages over traditional networks, such as scalability, mobility and robust city. The network can be formed easily. It is gained more and more attention in recent years for the using in urgent and abrupt occasion, for example communication in military battlefield, salvage, temporary assembly and open country construction etc. Mobile ad hoc networks have many characteristics: constrained transmission bandwidth, limited host power and limited processing ability. Therefore, the routing protocols for ad hoc networks should be efficiency, low energy, consumption and lightweight computing. The ad hoc networks have different scale and characteristics in different applications. The change frequency of network topology and the intensity of traffic are difference in different environments, which will be the important parameters effecting on the performance of the routing protocols. Therefore in different network environments, the protocol parameters should been configured dynamically. Thus dynamical configuration can adapt to the changing of the network topology and improve the protocol performance.***

In this paper, we analyze the characteristics and applications of MANETs and will describe the open issues in development of routing techniques in MANETs.

Keywords:

1. Introduction:

The recent developments in various fields such as Medicine, Computer science and Information technology. In no other field has these developments been more evident than in field of wireless technology. There are two basic types of wireless networks that are of interest; the cellular concept and the Ad hoc concept. The cellular concept is basically the same as is used in cellular phone technology (GSM), and is a highly researched area. Though wireless systems have existed since the 1980's it is only in recent times that wireless systems have started to make inroads into all aspects of human life. Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless links. Each node operates as an end system and a router for all other nodes in the network. A mobile Ad hoc Network is a self configuring network of mobile routers connected by wireless links –the union of which forms an arbitrary topology. An Ad hoc network is often defined as an "infrastructure less" network means that a network without the usual routing infrastructure, link fixed routers and routing backbones. A MANET is a distributed network that does not require centralized control, and every host works not only as a source and a sink but also as a router. This type of dynamic network is especially useful for military communications or emergency search and rescue operations, where an infrastructure cannot be supported. The nodes that make up a network at any given time communicate with and through each other. In this way every node can establish a connection to every other node that is included in the MANET. Examples of nodes can be personal devices like, our mobile phones, Laptops, Personal Data Assistants (PDA's), etc. Smaller and simpler devices also use wireless ad-hoc networking, like wireless headsets, hands free, etc. In figure 1 we have shown the ad hoc network.

Thus the maturity of wireless transmissions and popularity of portable computing devices have made the dream [1] of **"communication any time and any where"** possible. An ad hoc wireless network is a good choice for fulfilling this dream. An ad hoc wireless network consists of a set of mobile hosts operating without the aid of an established infrastructure of centralized administration. Communication is done through wireless links among mobile hosts using their antennas.

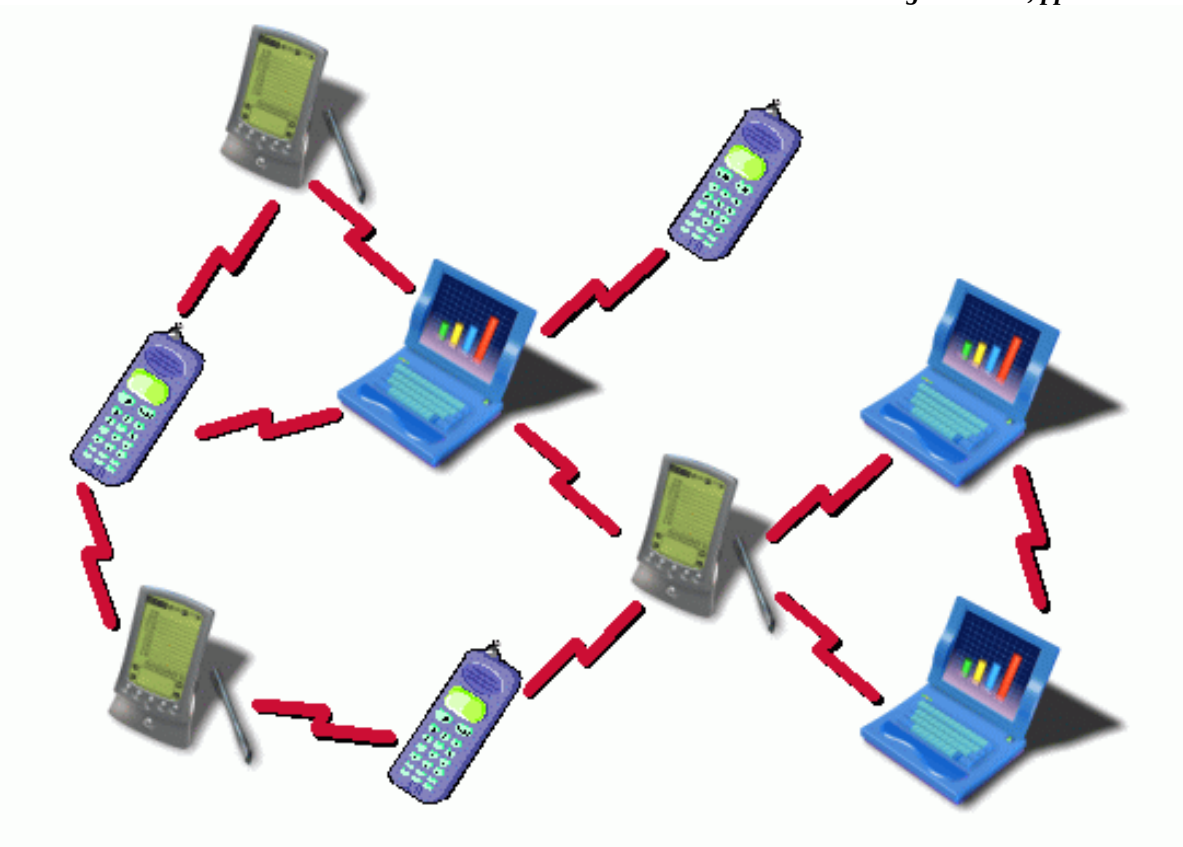

Figure 1. Ad hoc Network

So ad hoc wireless networks consist of a collection of geographically distributed nodes that communicate over a wireless medium but have no fixed infrastructure available and have no predetermined network topology [2, 3]**.** Such networks are also called infrastructure less networks because physical setup needs to be in place to form the network. The nodes in such a network can move around and might leave or enter the network as and when they please; this is because the network rearranges itself when nodes enter and leave it. Further, as nodes move about, they might go out of range of their previous neighbors. In this case, too, the network will have to realign itself.

A simple graph G=G(V,E) represents an ad hoc network, where the vertex set V is the collection of mobile stations within the wireless network. An edge between two stations u and v denoted by $u \leftrightarrow v$ means that both of them are within each other's transmission range. It is assumed that this graph G is finite and connected. We have an example in figure 2 of wireless network. There are five stations A, B, C, D, and E in an ad hoc network. The circle around each one represents its transmission range. Two vertices are connected if and only if they are within each other's transmission range.

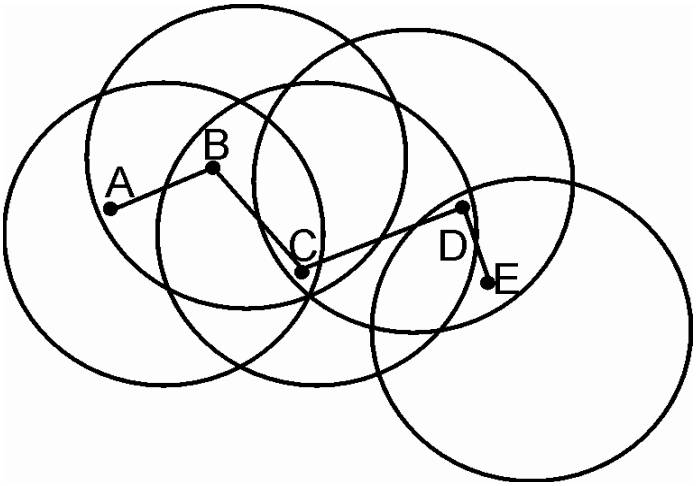

Figure 1.. The Graph Representing an Ad hoc Wireless Network

2. MINUTE REVIEW OF ROUTING PROTOCOLS FOR MANETs:

Routing is the most fundamental research issue in MANET [2] and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as: (1) pro-active (table-driven), (2) re-active (source-initiated on-demand driven) and (3) hybrid. Popular proactive routing protocols are Destination-Sequenced Distance Vector (DSDV) [3] and Wireless Routing Protocol (WRP) [4].They attempt to maintain consistent, up-to-date routing information of the whole network. These keep track of routes for all destinations and enjoy having the advantage of experiencing minimal initial delay in communications with arbitrary destinations. When the application starts, a route can be immediately selected from the routing table. Such protocols are called proactive because they store route information even before it is needed. Re-active routing protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. In contrast to pro-active routing protocols which maintain all up-to-date at every node, routes are created only when desired by the source node in re-active protocols. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Some reactive protocols are Cluster Based Routing Protocol (CBRP) [5], Ad Hoc On-Demand Distance Vector (AODV) [6] and Dynamic Source Routing (DSR) [7]. Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used.

Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) [8] and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network.

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highlydirectional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANETs have several salient characteristics:

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2) Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3) Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixedcable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches. In addition, some envisioned networks (e.g. mobile military networks or highway networks) may be relatively large (e.g. tens or hundreds of nodes per routing area). The need for scalability is not unique to MANETS.

However, in light of the preceding characteristics, the mechanisms required to achieve scalability likely are. These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

3. MANET CHALLENGES:

The major challenges faced by the internet architecture can be broadly classified as:

a) In incorporating emerging wireless network elements such as MDs, ad-hoc routers and embedded sensors in the existing protocol framework &

b) To provide end-to-end service abstractions that facilitates application development.

These challenges are posed by a broad range of environments such as cellular data services, WiFi hot-spots, Info stations, mobile peer-to-peer, Ad-hoc mesh networks for broadband access, vehicular networks, sensor networks and pervasive systems. These wireless application scenarios lead to a diverse set of service requirements for the future Internet as summarized below:

1. Naming and addressing flexibility.
2. Mobility support for dynamic migration of end-users and network devices.
3. Location services that provide information on geographic position.
4. Self-organization and discovery for distributed control of network topology.
5. Security and privacy considerations for mobile nodes and open wireless channels.
6. Decentralized management for remote monitoring and control.
7. Cross-layer support for optimization of protocol performance.
8. Sensor network features such as aggregation, content routing and in-network Processing.
9. Cognitive radio support for networks with physical layer adaptation.
10. Economic incentives to encourage efficient sharing of resources.

Taken together, the above MANET requirements represent a spectrum of network challenges. During the last few years, almost every aspect of MANET has been explored to some level of detail. Yet, more questions have arisen than been answered [2]. The major open problems are listed as:

A. *Autonomous*: No centralized administration entity is available to manage the operation of the different mobile nodes.

B. *Dynamic Topology*: Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

C. *Device Discovery*: Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

D. *Bandwidth Optimization*: Wireless links have significantly lower capacity than the wired links.

E. *Limited resources:* Mobile nodes rely on battery power, which is a scarce resource. Also storage capacity and power are severely limited.

F. *Scalability:* Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

G. *Limited physical security:* Mobility implies higher security risks such as peer-to- peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

H. *Infrastructure less and self operated:* Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

I. *Poor Transmission Quality*: This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

J. *Ad hoc addressing:* Challenges in standard addressing scheme to be implemented.

K. *Network configuration*: The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

L. *Topology maintenance:* Updating information of dynamic links among nodes in MANETs is a major challenge.

4. SOME EMINENT APPLICATIONS OF MANETs:

The application of this wireless network is limited due to the mobile and ad hoc nature. Similarly, the lack of a centralized operation prevents the use of firewall in MANETs. It also faces a multitude of security threats just like wired networks. It includes spoofing, passive eavesdropping, denial of service and many others. The attacks are usually classified on the basis of employed techniques and the consequences.

Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange. In addition, mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks [1]--many of these networks consist of highly-dynamic autonomous topology segments. Also, the developing technologies of "wearable"

computing and communications may provide applications for MANET technology. When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications with survivable, efficient dynamic networking. There are likely other applications for MANET technology which are not presently realized or envisioned by the authors. It is, simply put, improved IP-based networking technology for dynamic,
autonomous wireless networks. Some important applications of MANETs are as follows:

4.1 Tactical Networks :

- Military communication and operations
- Automated battlefields

4.2 Emergency Services:

- Search and rescue operations
- Disaster recovery
- Replacement of fixed infrastructure in case of environmentaldisasters
- Policing and fire fighting
- Supporting doctors and nurses in hospitals

4.3 Commercial & Civilian:

- E-commerce: electronic payments anytime and anywhere environments
- Business: dynamic database access, mobile offices
- Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks
- Sports stadiums, trade fairs, shopping malls
- Networks of visitors at airports

4.4 Home & Eenterprise:

- Home/office wireless networking
networking • Conferences, meeting rooms
- Personal area networks (PAN), Personal networks (PN)
- Networks at construction sites

4.5 Education :

- Universities and campus settings
- Virtual classrooms
- Ad hoc communications during meetings or lectures

4.6 Entertainment :

- Multi-user games
- Wireless P2P networking
- Outdoor Internet access
- Robotic pets
- Theme parks

4.7 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

4.8. Context Aware Services :

- Follow-on services: call-forwarding, mobile workspace
- Information services: location specific services, time dependent services
- Infotainment: touristic information

4.9 Coverage Extension:

- Extending cellular network access
- Linking up with the Internet

5. Security Goals of MANETs

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

5.1 Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

5.2 Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

5.3 Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

5.4 Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

5.5 Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

5.6 Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

5.7 Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

6. ROUTING PROTOCOLS:

Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as:

6.1 Proactive (Table-Driven): The pro-active routing protocols [11,14] are the same as current Internet routing protocols such as the RIP(Routing Information Protocol), DV(distance-vector), OSPF (Open Shortest Path First) and link-state . They attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Some of the existing pro-active ad hoc routing protocols are: DSDV (Destination Sequenced Distance-Vector, 1994), WRP (Wireless Routing Protocol, 1996), CGSR (Cluster head Gateway Switch Routing, 1997), GSR (Global State Routing, 1998), FSR (Fisheye State Routing, 1999), HSR (Hierarchical State Routing, 1999), ZHLS (Zone based Hierarchical Link State,1999),STAR (Source Tree Adaptive Routing, 2000).

6.2 Reactive (Source-Initiated On-Demand Driven): These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Some of the existing re-active routing protocols are [12,14].DSR (Dynamic Source Routing, 1996), ABR (Associativity Based Routing, 1996), TORA (Temporally-Ordered Routing Algorithm, 1997), SSR (Signal Stability Routing, 1997), PAR (Power-Aware Routing,1998), LAR (Location Aided Routing, 1998), CBR (Cluster Based Routing, 1999), AODV (ad hoc On-Demand Distance Vector Routing, 1999). In pro-active routing protocols, routes are always available (regardless of need), with the consumption of signaling traffic and power. On the other hand, being more efficient at signaling and power consumption, re-active protocols suffer longer delay while route discovery. Both categories of routing protocols have been improving g to be more scalable, secure, and to support higher quality of service**.**

6.3 Hybrid Protocols: Hybrid routing protocols [11, 12] aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network. At network layer, routing protocols are used to find route for transmission of packets. The merit of a routing protocol can be analyzed through metrics-both qualitative and quantitative with which to measure its suitability and performance. These metrics should be independent of any given routing protocol. Desirable qualitative properties of MANET are Distributed operation, Loop-freedom, Demand-based operation, Proactive operation, Security, Sleep period operation and unidirectional link support. Some quantitative metrics that can be used to assess the performance of any routing protocol are End-to-end delay, throughput, Route Acquisition Time, Percentage Out-of-Order Delivery and Efficiency. Essential parameters that should be varied include:

Network size, Network connectivity, Topological rate of change, Link capacity, Fraction of unidirectional links, Traffic patterns, Mobility, Fraction and frequency of sleeping nodes [1,9,10].

7. CONCLUSION AND FUTURE SCOPE:

The future of ad- hoc networks is really appealing, giving the vision of ―anytime, anywhere‖ and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend in MANET is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad- hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms. In all, although the widespread deployment of ad- hoc networks is still year away, the research in this field will continue being very active and imaginative.

References:

[1] IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.

[2] A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of Ad Hoc Wireless Networks (chapter 30), CRC press LLC, 2003.

[3] Jie Wu , Fei Dai, ―Broadcasting in Ad Hoc Networks: Based on Self-Pruning‖, Twenty Second Annual Joint Conferences of IEEE Computer and Communication Societies, IEEE INFOCOM 2003

[4] P. Papadimitrates and Z.J. Hass, secure Routing for mobile Ad Hoc Networks in proceeding of SCS Communication Networks and Distributed system modelling and simulation Conference (CNDS), San Antonio, TX, Jan. 2002.

[5] Y.Hu, A Perrig and D. Johnson, Ariadne: A secure On-demand Routing Protocol for Ad Hoc Networks, in Proceeding of ACM MOBICOM'02, 2002.

[6] K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02,2002.

[7] Y. Hu, D. Johnson and A Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wire

[8] D. Johnson and D. Maltz, ―Dynamic Source Routing in Ad Hoc Wireless Networks,‖ Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[9] Broch,J., A.M David and B. David,1998. A Performance comparison of multi-hop wireless ad hoc network routing protocols. Proc.IEEE/ACM MOBICOM'98, pp: 85-97.

[10] C.E.Perkins and P. Bhagwat, ―Highly dynamic destination-sequenced distance vector routing for mobile computers‖, Comp, Comm. Rev., Oct.1994, pp 234-44

[11] Belding-Royer,E.M. and C.K. Toh, 1999. A review of current routing protocols for ad-hoc mobile wireless networks.IEEE Personal Communication magazine pp:46-55.

[12] M. Frodigh, P. Johansson, and P. Larsson.―Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.

[13] Magnus Frodigh, Per Johansson and Peter Larsson. Wireless ad hoc networking— The art of networking without a network.

[14] E. M. Royer and C-K Toh , ―A review of Current routing protocols for Ad Hoc Mobile Wireless.

[15] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6.

[16] HaoYang, Haiyun & Fan Ye ― Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.

[17]. Luis Bernardo, Rodolfo Oliveira, Sérgio Gaspar, David Paulino and Paulo Pinto A Telephony Application for Manets: Voice over a MANET-Extended JXTA Virtual Overlay Network .

