International Journal of Information Technology and Knowledge Management
July-December 2008, Volume 1, No. 2, pp. 245-257

ROADMAP THROUGH COBCOB WEB OF CHALLENGES FOR COMPUTING IN MANET

P. K. Suri & Kavita Taneja

Abstract

To be able to connect to the Internet is as a necessity as air and water to survive while keeping pace with exploding information technology era of today. In view of the increasing demand for wireless information and data services, providing faster and more reliable mobile access is becoming an important concern. A mobile ad hoc network (MANET) is a network formed and functioning without any established infrastructure or centralized administration and consists of Mobile devices (MDs) that use a wireless interface to communicate with each other. These devices serve as both hosts and routers so they can forward packets on behalf of each other. Hence, the MDs are able to communicate beyond their transmission range by supporting multihop communication. In this paper, a roadmap for the MANET is provided covering broadly the origin, types, history, applications and challenges.

Keywords: Mobile ad hoc network (MANET), Mobile device (MD), Global System for Mobile Communication (GSM), Personal Digital Assistants (PDAs), Wireless Local Area Netrwork (WLAN).

1. MANET's Origin: "The Necessity is the Mother of Unvention"

The immense utility of the internet access is limited if one has to find a stationary computer with a modem or a network card to connect to the Internet. Therefore, it is desirable to have access to the Internet from portable devices such as mobile phones, laptops or personal digital assistants (PDAs) which are flooding the computer industry [1]. The widely deployed and successful mobile communication standard *global system for mobile communication* (GSM) has spoiled user by the expectation to reach, and be reached, by everyone at (almost) every place. Laptops with WiFi cards are available; hotspots can be found at airports, hotels and shopping malls; businesses are converting existing local area networks to a wireless network. These kinds of spontaneous, temporary networks are referred to as *mobile ad hoc networks* (MANETs) (sometimes just called *ad hoc networks*) or *multihop wireless networks*, and promise to play an important role in our daily lives in the near future [2].

2. Networks -> Wired -> Wireless -> Ad Hoc-> MANET

The MANET is a collection of wireless mobile hosts dynamically establishing a short lived network without the support of a network infrastructure. In this type of environment, a large number of ad-hoc connections are expected to exist in the same region without any mutual coordination. MANETs are truly coined as *the future of wireless networks*. Basically, MANETs differ from wired networks due to often and unpredictable topology changes resulting from nodes mobility, absence of dedicated routers, dual incarnation of every node as a router and a host and changing channel capacity due to environmental effects [3]. MANETs differ from mobile cellular networks in that due to the absence of central administration. MANETs use multihop approach to deliver data as shown in Fig. 1. *Dotted circle represent the transmission range of the MD placed at the centre of each such circle displayed and the colored circle represent the local ad hoc network formed for transmitting data from MD 1 to MD 5.* There are currently two types of mobile wireless networks. The first is known as *infrastructured* networks, such as networks with fixed and wired gateways. The bridges for these networks are known as base stations. Such wireless mobile networks [2, 3] have traditionally been based on the cellular concept and relied on good infrastructure support, in which MDs communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, WLAN, etc. The second type of wireless network is the MANET that is *infrastructureless*. It is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure [4]. These networks facilitate ad-hoc connectivity based on *peer-to-peer* communication (communication between two nodes which are within one hop), *Remote-to-Remote* (communication between two nodes beyond a single hop but which maintain a stable route between them), *and dynamic traffic* (when nodes are

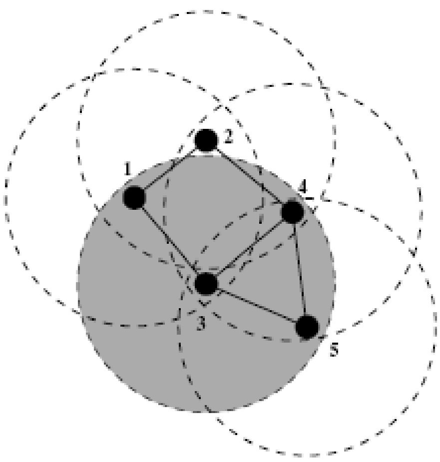

Figure 1: Multihop Data Transfer in MANET

dynamic and moving around, routes must be reconstructed that lead to poor connectivity and network activity in short bursts).

3. History

Wireless devices are getting smaller, cheaper, and more sophisticated. In the array of these ubiquitous devices, organizations are looking for inexpensive ways to keep these MDs connected. The IEEE 802.11 subcommittee had adopted the term "ad-hoc networks" and the research community had started to look into the possibility of deploying ad-hoc networks in other areas of application [7]. MANET comprises a set of wireless devices that can move around freely and cooperate in relaying packets on behalf of one another [6]. Such a network does not require a fixed infrastructure or centralized administration. Because mobile units have limited transmission range, distant nodes communicate through multihop paths. In the **1960s**, Advanced Research Projects Agency (ARPA) became interested in developing a way for computers to communicate with each other and began to fund programs at universities and corporations. A network would both advance American technological development and provide a secure command and control over information during wartime. To this end, in the mid-1960s, ARPA began to support research into building an effective network. It was 1964, the height of the Cold War, when American government find the most pervasive problem to sustain communication among military [5]. A centralized system might easily be destroyed in wartime, and so traditional technologies wouldn't work. This fear impressed a need on the government to do something different — to develop a whole new scheme for post-nuclear communication. 1969 marked the beginning of Advanced Research Projects Agency Network (ARPANet) which connected University of LA, SRI, University of California at Santa Barbara, and the University of Utah [8]. The first generation goes back to **1972** [8]. Instead of performing its own research, ARPA (a branch of the Department of Defense), which became The Defense Advanced Research Projects Agency (DARPA) in 1972, regularly funded research projects related to technological development or military problems.

Table 1
MANET History

Time	*Coined as*	*Application*
1972	The first generation **PRNET** (Packet Radio Networks)	Trial base usage to provide different networking capabilities in a combat environment.
1980	The second generation **SURAN** (Survivable Adaptive Radio Networks)	Implemented as a part of the SURAN to provide packet-switched network to the mobile battlefield.
1990	The third generation **Commercial Ad Hoc** Networks	Notebook computers and viable communications equipments.

At the time, they were called PRNET (Packet Radio Networks). In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment [7]. The second generation of ad-hoc networks emerged in **1980s**, when the ad-hoc network systems were further enhanced and implemented as a part of the Survivable Adaptive Radio Networks (SURAN) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks. After the unveiling, technologies to help develop the network began to sprout. Hence, in the **1990s**, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of MDs was proposed at several research conferences [9].

4. APPLICATIONS

The fame MANET enjoy is due to the increasing interactions between mobile communication and mobile computing, which is changing soul of such ad hoc networks from ***"anytime anywhere"*** into ***"all the time, everywhere"*** information access and processing. MANET or on-the-fly networks are characterized by the lack of infrastructure which is nothing short of a boon as far as ease of deployment is concerned which results in a spectrum of areas where it is justified to apply MANET [10]. Examples include battleground communications, disaster recovery efforts, communication among a group of islands or ships, conferencing without the support of a wired infrastructure, and interactive information sharing. Unlike typical Internet applications, most applications of MANETs involve one-to-many and many-to-many communication patterns [3]. Examples of emergency networks include the disaster relief efforts after terrorist bombing attacks or in the aftermath of a natural disaster where cellular/PCS service may not be available. Today, commercially MANET is used to track seismological phenomena, transmit pressing news bulletins, and send email to mom. This partly signal a shift in priorities from military application to commercial world, more appropriately though, it is an example of a technology with more uses than anybody ever imagined.

5. MANET: CHALLENGES CLOSE-UP

Ad hoc networking allows portable devices to establish communication independent of a central infrastructure [11]. However, the fact that there is no central infrastructure and that the devices can move randomly gives rise to plethora of problems. All the challenges are cob webbed (Fig. 2) as for achieving reliable routing, the reliability and

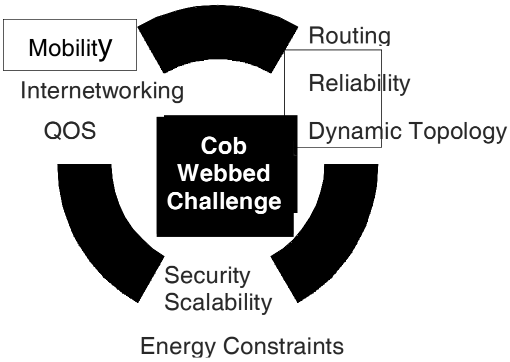

Figure 2: MANET Challenges

routing are in itself two challenges that the MANET faces. Hence, achieving a clean chit, challenge free performance from a MANET is next to impossible for the hostility contained in such open networks. Only a tradeoff between various sets of challenges can be handled and that too, to a satisfactory level depending on the application [12].

5.1. Scalability

Scalability in MANET can be broadly defined as whether the network is able to provide an acceptable level of service to packets even in the presence of a large number of nodes in the network. In proactive networks, scalability is often accomplished by introducing routing and or location hierarchy in the network [14], or by limiting the scope of control updates to locations close to the changes [15, 16].

In reactive ad hoc networks, techniques such as dynamically limiting the scope of route requests and attempting local repairs to broken routes are often used [16].

5.2. Security

Another area which has garnered attention is **SECURITY** and is a major concern for providing protected communication between MDs in an ever demanding environment. Any proposed security policy must provide protection services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should traverse the entire protocol stack, under its double fenced umbrella. Security is critical for many wireless sensor network applications such as battlefield surveillance, medical monitoring, and emergency response. However, many security mechanisms developed for the Internet or ad-hoc networks have to be effectively tailored or enhanced to be applied directly to MANET due to limited resources in computation, memory, communication bandwidth, and energy prevailing in such networks. The insecurity of the wireless links, energy constraints, relatively poor physical protection of MDs in a hostile environment, and the vulnerability of statically configured security schemes have been identified [17, 18] in literature as major challenges embedded in security mechanism for MANETs. The severe resource constraints of MANETs give rise to the need for resource bound security solutions. There are at least two interesting aspects of this concept. First, individual security mechanisms must be efficient in memory, computation, energy and bandwidth. For example, certain cryptographic schemes are inappropriate because ciphertext message expansion results in costly memory, bandwidth and energy use. Second, the resource consumption of all security mechanisms installed together at a MDs in MANET must not exceed the amount of resources allocated for security and they cannot degrade performance to an unacceptable level during normal operation nor when an attack is underway [17, 18]. For the problem of secure data forwarding, two mechanisms that (i) detect *misbehaving MDs* and report such events and (ii) maintain a set of metrics reflecting the past behavior of other MDs [19] have been proposed to alleviate the detrimental effects of packet dropping. Each MD may choose the 'best' route, comprised of relatively well-behaved MDs.

5.3. Internetworking

MANET is formed by wireless nodes that collaborate to route packets inside a multi-hop network. While MANETs are autonomous, it will oftentimes be desirable to interconnect them to the fixed infrastructure. One of the implications of ad hoc connectivity [3] is that networks have become more heterogeneous as users have been employing a diverse set of devices ranging from laptops, PDAs, cellular phones, pagers, and smart badges to stay connected everywhere, everytime. Furthermore, forthcoming applications such as smart environments (homes, offices, buildings, highways, etc.), factory automation, surveillance, environmental and biomedical monitoring will add a whole new set of *different* devices that will need to communicate with one another. Therefore, network heterogeneity will manifest itself in terms of increased diversity in communication medium technology (e.g., as wired, wireless, satellite, and optical links), as well as in the types of devices networks will interconnect. In the near future, internetworks will interconnect not only traditional desktop and laptop computers, but also unconventional devices whose power, processing, and communication capabilities differ widely [10]. 'The prospect of doing so impacts nearly every aspect of network design including addressing, mobility management relative to the fixed network, security, and transport-layer functionality. MDs casually use the concept of communicating between devices across multiple networks, i.e., "Internetworking." Internetworking between MANET and IP based fixed networks is often required in many applications. The coexistence of different protocols in such a hostile environment is a severe challenge as far as mobility management is concerned. *Internetworking* facilitates *Interoperability* among global coalition networks built upon multiple, heterogeneous networks [48]. The technical challenges faced are the hierarchical management of global network of heterogeneous networks, adequacy of emerging Internet security protocols and standards for hostile networks, end-to-end routing and quality-of-service across multiple autonomous systems, connectivity across dynamic nomadic networks reaching to mobile end users. Internetworking main goal is to allow interconnection of heterogeneous devices with varying power, processing, and communication capabilities, ranging from simple sensors to more powerful computing devices such as laptops and desktops. The major thrust areas are in system architecture, security, network and traffic management, mobility, and IPv4/IPv6 internetworking. The future scope is to develop further insights on integration of different IPv6-based network technologies to be worked together effectively in a practical context. Internetworking of the scale and diversity of a global ad hoc network of heterogeneous networks is by its very nature beyond the capabilities of achieving in full.

5.4. Quality of Service

The wireless channel bandwidth is limited making QoS provisioning in MANETs complex and challenging. The problem gets compounded if a best set of protocols or algorithms for MANETs to satisfy different MANET application requirements is expected. Besides, topology shifts in MANETs often render routing paths not viable. Such frequent path failures have detrimental effects on the network ability to support QoS-driven services especially multimedia applications [24]. The spectrum of applications of MANET reflects the density of need for QOS [20]. MANETs are viewed conditionally as sugarcoated option to cellular and WLANs, if MANETs can support QoS that is service based and have minimum latency times, to facilitate seamless roaming of MDs. QoS guarantees are possible only if we can have more robust routes. In the literature, a lot of proposals have been presented to support QoS in mobile ad hoc networks such as QoS MAC protocols, QoS routing protocols and resource reservation protocols. While these protocols are quite sufficient to meet QoS needs, with the given assumptions, an integrated framework for routing and Qos has yet to be explored. QOS can be achieved to acceptable levels by enhancing the existing routing protocols for the MANETs [21, 22, 23]. Hence, QoS support for distributed, non-realtime and realtime traffic in MANETs has emerged as a major research opportunity.

5.5. Routing

Existing wireless ad hoc routing protocols typically find routes with the minimum hop-count. A promising technique for coping with frequent route failures is to enhance the diversity of routes used in MANETs [25]. Traditional routing protocols [26] use a single path between the source and the destination. When that path fails, they need to perform a potentially costly operation to locate an alternate route for the given destination. In the case of reactive protocols, each disruption of *"on demand constructed"* route may lead to excessively long delays at the routing layer on the order of seconds, which in turn prohibit higher-level protocols to take full advantage of the network bandwidth even after the route is restored. On the other hand, proactive protocols pay a higher penalty in order to have alternative routes at hand as *"the routes are to be constructed from scratch"*. Single-path routing algorithms lead to long network latencies and excessive overhead when path failure is encountered. A promising approach is to use a set of redundant paths than a single path, to minimize the lass due to link failures in the network [27].

5.6. Reliability

Reliability is a network's ability to perform a designated set of functions under certain conditions for specified operational times. The degree to which a wireless network is able to provide the required services needs to be quantitatively assessed by defining proper measurable quantities. These measurable quantities are called the *network reliability measures*. The typical network reliability problem is *to calculate the probability that a certain set of nodes can communicate with each other for a given period of time*. Based on the number of communicating nodes, there are three main formulations of the network reliability problem: two-terminal, K-terminal and all-terminal reliabilities [28]. In order to confirm the stability of the whole route from source node to destination node, every link between each adjacent node should be ensured firstly. For reliable performance from the networks made of unreliable interconnections, several routing models [29-32] have been proposed in MANET, and these models have been used in some protocols—DV-MP (Distance Vector with Mobility Prediction), QRMP (Quality Related Market Price), ODMRP (On-Demand Multicast Routing Protocol) and FORP (the Flow Oriented Routing Protocol), etc.

5.7. Mobility Management

Topological changes in MANETs frequently render routing paths unusable and project a downward spiral as far as performance of existing protocol stack is concerned. As the recurrent path failures have detrimental effects on the network ability to support QoS-driven services. The answer is self organization and the essence of auto configuration is that the patterns arise from many interactions spread over space and time. Such patterns studied in light of natural phenomenon are known as emergent properties because they have no meaning for individual components and also mobility for survival is the source of evolution [33]. Three frequently used mobility models are (1) *random walk*, which is a simple mobility model based on random directions and speeds, (2) *random waypoint* [37], which includes pause time between changes in destination and speed, and (3) *random direction mobility*, which forces hosts to travel to the edge of the simulation area before changing direction and speed [34]. Several routing protocols, associativity-based routing (ABR) [35] and signal stability based adaptive routing (SSA) [36], have been proposed that select less stochastic links to construct a more stable route. In [30], GPS information is used to estimate the expiration time of the link between two neighboring nodes. Although work is available on the effect of mobility on routing path [38] but no broadcast protocol uses the notion of stable link to evaluate the stability of neighbor set in order to better decide the forwarding status of each node. More contended answer come from protocols based on probabilistic approach for parameters evaluation [39] but they tradeoff between simple design and delivery ratio. Still to establish a direct connection between forwarding probability and node mobility need rigorous research. In addition to the communication within an ad hoc network, internetworking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such an environment is a challenge for the harmonious mobility management.

5.8. Energy Constraints

The use of a MD is constrained by its energy, making power conservation the most critical issue for MDs and their applications. Hence, for MANETs power conservation is a vital issue while still delivering messages reliably as the life of the network is determined by the power sources. The MANET environment is resource-constrained, in such multihop environment, available bandwidth is very limited and some routers may have severe energy constraints as well (e.g. relying on battery power).Hence, inter-router communication is an *expensive* activity in MANETs in terms of bandwidth, and possibly energy, consumption. MDs operating on a battery supply have strong power constraints and network life depends on the management of this resource. Less power in routing has benefits from conserving power for battery life to radiate with the least amount of power in order to minimize the probability of detection/interception. Therefore, a MANET routing protocol should be *power efficient*. However, none of the proposed protocols consider the power consumption and battery life of each node in the choice of the “best” route from a source to a destination. The shortest path does not necessarily correspond to the most power efficient route, as shown in [40], where a minimum power routing (MPR) algorithm was developed. The most popular of existing work on energy efficient protocols [41-44] for MANET is the IEEE 802.11 Power Saving Mode (PSM) [45]. But it is originally designed for the single hop environment, making it inapplicable to MANET which has primarily a multi-hop connectivity. S-MAC [46] applies message passing to reduce energy consumption when listening to an idle channel. But S-MAC is specially designed for sensor networks; therefore it is not directly applicable to MANET due to the maintenance overhead. SPAN [42] and GAF [47] reduce energy consumption and delay latency conspicuously in densely networks by keeping only selective elements called the coordinator to stay in active mode to maintain the routing backbone connectivity and other nodes may stay in sleep mode until receiving packets.

6. Conclusion and Future Works

Mobile computing faces multi-layer challenge. The physical layer must adapt to stochastic link characteristics of such ad hoc networks. The multiple access control (MAC) layer needs to minimize collisions, allow fair access, and semi-reliably transport data over the shared wireless links in the presence of rapid changes and hidden or exposed terminals. The network layer needs to determine and distribute information used to calculate paths in a way that maintains efficiency when links change often and bandwidth is at a premium. It also needs to integrate smoothly with traditional, non ad hoc internetworks and perform functions such as auto-configuration in this changing environment. The transport layer must be able to handle delay and packet loss statistics that are very different than traditional networks. Finally, applications need to be designed to handle frequent disconnection and auto-reconnection with peer applications as well as widely varying delay and packet loss characteristics. Among several technical challenges of MANETs, the sharing of information among various computing devices can be regarded as one of the basic issues. Information access and sharing is difficult in MANET due to their dynamic nature, scarce resources, and heterogeneous user devices.

References

[1] Leiner and Barry M., "Globalization of the Internet," *Internet System Handbook*.

[2] Internet Engineering Task Force, "Mobile ad hoc Networks Working Group Charter," http://www.ietf.org/html.charters/manet-charter.html.

[3] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc Networking: the Art of Networking without a Network," *Ericsson Review*, **4**, (2000), 248–263.

[4] IETF Working Group: Mobile Adhoc Networks (manet). http://www.ietf.org/html.charters/manet-charter.html.

[5] Scott Ruthfield, "The Internet's History and Development from Wartime Tool to the Fish-Cam," *Crossroads Mag.*, (Sept. 1995).

[6] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," in Proceedings of ACM Mobicom *'94*, Dec. 1994.

[7] Zhisheng Niu, "Broadband Computer Networks," Lecture Notes, Tsinghua University, 2003. cone.informatik.unifreiburg.de/teaching/lecture/manet-7/slides/MANET-10.ppt

[8] Humayun Bakht, "The History of Mobile ad-hoc Networks," *Computing Unplugged Mag.*, Aug. 2005.

[9] A.Penttinen, "Research On Ad Hoc Networking: Current Activity And Future Directions," http://citeseer.nj.nec.com/533517.html

[10] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.

[11] G. H. Forman and J. Zahorjan, "*The Challenges of Mobile Computing*," *IEEE Computer,* **27**, (4), (1994), 38–42.

[12] R. Ramanathan and J. Redi, "A Brief Overview of Ad Hoc Networks: Challenges and Directions," *IEEE Commun. Mag.*, **40**, (5), May 2002.

[13] R. Ramanathan and M. Steenstrup, "Hierarchically-Organized, Multihop Mobile Wireless Networks for QOS Support," *Baltzer Mobile Networks and Applications*, (1998)**.**

[14] C. Santivanez, R. Ramanathan, and I. Stavrakakis, "Making Link-State Routing Scale for Ad Hoc Networks," in *Proceedings of ACM Mobihoc 2001,* Long Beach, CA.

[15] A. Iwata, C. C. Chiang, G. Pei, M. Gerla, and T. W. Chen, "Scalable Routing Strategies for ad hoc Wireless Networks," *CEC JSAC*. **17**, (8), Aug. 1999, 1369–79.

[16] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," *IEEE Network Mag*., **13**, (6), Nov.-Dec. 1999.

[17] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," *Security Protocols, 7th International Workshop*, LNCS, Springer-Verlag, 1999.

[18] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6^{th} MobiCom, BA Massachusetts, (Aug. 2000).

[19] Lo A., Xiao H., Seah W. K. G. and Chua K.C., "A Flexible Quality of Service Model for Mobile AdHoc Networks" *IEEE Vehicular Technology Conference Fall 2000*, 445–449, (May 2000).

[20] Xue Q. and Ganz. A., "Ad hoc QoS on-demand Routing (AQOR) in Mobile ad hoc Networks," *Journal of Parallel and Distributed Computing*, **63**, (2003), 154–165.

[21] Ge Y., Kunz T., Lamont L., "Quality of Service Routing in ad-hoc Networks using OLSR," *The 36th Hawaii International Conference on System Sciences (HICSS-36)*, Hawaii, USA, (Jan. 2003).

[22] Zhu C, Corson M. S., "QoS Routing for Mobile Ad hoc Networks," *INFOCOMM 2002*, **2**, 958–967.

[23] S. Chakrabarti and A. Mishra, "QoS Issues in ad hoc Wireless Networks," *IEEE Commun. Mag*., **39**, (2), (2001), 142–148.

[24] M.R. Pearlman and Z.J. Haas, P. Sholander, S.S.Tabrizi., "On the Impact of Alternate Path Routing for Load Balancing in Mobile ad hoc Networks.," in *Proceedings of First Workshop on Mobile and ad hoc Networking and Computing* (MobiHoc 2000), Boston, MA, (Aug. 2000).

[25] Elizabeth M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Commun. Mag.*, **6**, (2), (Apr. 1999), 46–55.

[26] A. Tsirigos and Z. J. Haas. "Multipath Routing in the Presence of Frequent Topological Changes," *IEEE Commun. Mag*., (Nov. 2001), 132–138.

[27] S. Rai and D. P. Agrawal, "Distributed Computing Network Reliability," *Los Alamitos: IEEE Computer Society Press*, (1990).

[28] Bruce McDonald and Taieb Znati, "A Path Availability Model for Wireless Ad-hoc Networks," in *Proceedings of IEEE Wireless Communications and Networking Conference* 1999 (WCNC2 99), (1999), 21–24.

[29] W. Su, S. J. Lee and M. Gerla, "Mobility Prediction and Routing in ad hoc Wireless Networks," *International Journal of Network Management*, **11**, (1), (Jan.-Feb. 2001), 3–30.

[30] Shah H., Nahrstedt K., "Predictive Location based QoS Routing in Mobile Ad-hoc Networks," in Proceedings of *IEEE International Conference on Communications (ICC2002),* **2**, (2002), 1022–1027.

[31] Shengming Jiang, He D. J., Rao J.Q., "A Prediction Based link Availability Estimation for Mobile Ad-hoc Networks", IEEE INFOCOM 2001, 1745–1752.

[32] Kauffman SA, "The Origins of Order: Self-Organization and Selection in Evolution," Oxford University Press, (1993).

[33] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for ad hoc Network Research," *Wireless Communication & Mobile Computing (WCMC)*: *Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, **2**, (5), (2002), 483–502.

[34] C.K. Toh, "Associativity-based Routing for ad-hoc Mobile Networks," *IEEE Personal Communications*, **4**, (2), (Mar. 1997), 36–45.

[35] R. Dube, C. Rais, K. Wang, and S. Tripathi, "Signal Stability based Adaptive Routing (SSA) for ad hoc Mobile Networks," *IEEE Personal Communications*, **4**, (1), Feb. (1997), 36–45.

[36] C. Bettstetter, "Topology Properties of ad hoc Networks with Random Waypoint Mobility," in *ACM MobiHoc*, (Jun. 2003).

[37] N. Sadagopan, F. Bai, B. Krishnamachari, and A. Helmy, "Paths: Analysis of Path Duration Statistics and their Impact on Reactive MANET Routing Protocols," in *Proceedings of MobiHoc*, (Jun. 2003).

[38] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc Routing," in *Proceedings of IEEE Infocom*, (Jun. 2002).

[39] Madhavi W. Subbarao, "Dynamic Power-Conscious Routing for MANETs: An Initial Approach", IEEE VTC, Amsterdam, The Netherlands, Sept. 1999.

[40] Y. C. Tseng, C. S. Hsu, and T. Y. Hsieh, "Power-Saving Protocols for IEEE 802.11-Based Multi-Hop Ad Hoc Networks," *Computer Networks*, Elsevier Science Pub., **43**, (3), (Oct. 2003), 317–337.

[41] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An Energy-efficient Coordination Algorithm for Topology Maintenance in ad hoc Wireless Networks," in the Proceedings of the 7th *Annual International Conference on Mobile Computing and Networking*, 85–96. ACM, (Jul. 2001).

[42] R. Bhatia and M. Kodialam "On Power Efficient Communication over Multi-hop Wireless Networks: Joint Routing, Scheduling and Power Control," *IEEE INFOCOM 2004*, March, 2004, 7–11.

[43] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *IEEE INFOCOM, 2002*, **3**, 1567–1576.

[44] IEEE, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec, *IEEE* 802.11 standard (1998).

[45] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *IEEE INFOCOM*, **3**, (2002), 1567–1576.

[46] Y. Xu, J. Heidemann, and D. Estrin., "Geographyinformed Energy Conservation for ad hoc Routing," in *Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking*, (Jul., 2001), 70–84

[47] M. Zuniga and B. Krishnamachari, "Integrating Future Large-Scale Wireless Sensor Networks with the Internet," *USC Computer Science Technical Report CS 03-792*, (2003).

P. K. Suri
Professor
Deptt. of Computer Science and Applications
Kurukshetra University
Kurukshetra, Haryana, India
E-mail: pksuritf25@yahoo.com

Kavita Taneja
Asst. Prof.
M.M.I.C.T & B.M.
Maharishi Markendeshwar University
Mullana, Haryana, India
E-mail: kavitatane@gmail.com