Study and Implementation of Mobile Ad Hoc Networking

Smita Patel
Digital Communication Department
Patel Institute of Engineering and Science,
RGPV Unv.
Bhopal, M.P ,India

Dr. PadamashriKunthe
Proff and Principle E&C Deptt.
Patel Institute of Engineering and Science,
RGPV Unv.
Bhopal, M.P, India

Mrs. SameenaZafar
Asst. Proff& HOD, E&C Deptt,
Patel College of Science and Technology,
RGPV Unv.
Bhopal, M.P, India

Abstract:- **A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, "ad-hoc" network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure.**

Ad hoc networking concept is not a new one, having been around in various forms for over 20 years. Traditionally, tactical networks have been the only communication networking application that followed the adhoc paradigm. 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 attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. Then, it reviews the latest research activities in these areas of MANET_s characteristics, capabilities and applications.

Keywords : Adhoc Network, Bluetooth, 4G, Routing, Security, Performance evaluation

I. INTRODUCTION

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad- hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." 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. An Ad-hoc network is a collection of wireless mobile nodes which dynamically forming a temporary mobile nodes which dynamically forming a temporary network without the aid of any established infrastructure or centralized administration.. The proliferation of mobile computing and communication devices (e.g., cell phones, laptops, handheld digital devices, personal digital assistants, or wearable computers) is driving a revolutionary change in our information society. We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ubiquitous Computing age in which a user utilizes several electronic platforms at a single instance through which he can access all the required information whenever and wherever needed. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations; tourists can use Global Positioning System (GPS) terminals installed inside rental cars to locate driving maps and tourist attractions, researchers can exchange files and other information by connecting portable computers via wireless LANs while attending conferences; at home, users can synchronize data and transfer files between portable devices and desktops. Not only are mobile devices getting smaller, cheaper, more convenient, and more powerful, they also run more applications and network services, commonly fueling the explosive growth of mobile computing equipment market. The exploding number of Internet and laptop users driving this growth further. Projections show that in the next two years the number of mobile connections and the number of shipments of mobile and Internet terminals will grow yet by another 20–50%. With this trend, we can expect the total number of mobile Internet users soon to exceed that of the fixed- line Internet users. Among all the applications and services run by mobile devices, network connections and corresponding data

services are without doubt the most demanded service by the mobile users. According to a study, the number of subscribers to wireless data services will grow rapidly from 2.6 billion worldwide in 2009 to more than 3.3 billion in 2010, and the number of wireless messages sent per month will rise continuously. Currently, most of the connections among these wireless devices are achieved via fixed infrastructure-based service provider, or private networks.

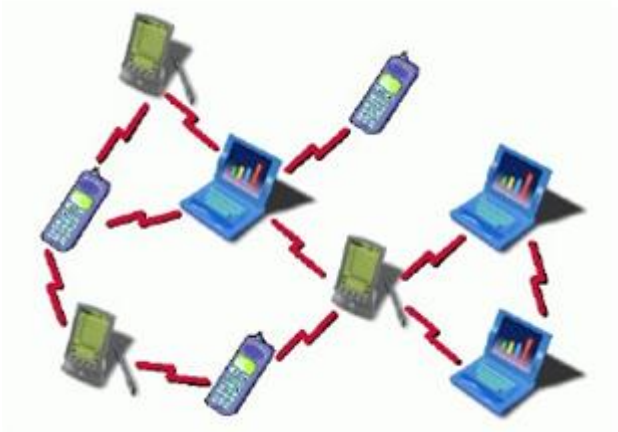

Fig. 1 : Mobile Network

There are, furthermore, situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. More recently, new alternative ways to deliver the services have been emerging. These are focused around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile network that is both flexible and powerful. In this way, not only can mobile nodes communicate with each other, but can also receive Internet services through Internet gateway node, effectively extending Internet services to the non-infrastructure area. As the wireless network continues to evolve, these ad hoc capabilities are expected to become more important, the technology solutions used to support more critical and significant future research and development efforts can be expected in industry and academy. Inside the ad hoc networking field, wireless sensor networks take a special role. A sensor network is composed of a large number of small sensor nodes, which are typically densely (and randomly) deployed inside the area in which a phenomenon is being monitored. Wireless ad hoc networking techniques also constitute the basis for sensor networks. However, the special constraints imposed by the unique characteristics of sensing devices, and by the application requirements, make many of the solutions designed for multi-hop wireless networks (generally) not suitable for sensor networks. This places extensive literature dedicated to sensor networks beyond the scope of this paper; however, the interested reader can find an excellent and comprehensive coverage of sensor networks in a recent survey. This paper demonstrates the impetus behind mobile ad hocnetworks, and presents a representative collection of technology solutions used at the different layers of the network.

II. AD HOC NETWORKING AND 4G

A major goal toward the 4G Wireless evolution is the providing of pervasive computing environments that can seamlessly and ubiquitously support users in complishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device. In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need. The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the nvironment, without requiring any major change in the users_ behavior. This new philosophy is the basis of the Ambient Intelligence concept. The objective of ambient intelligence is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and "natural" interactions, a multitude of services and applications. Ambient intelligence places the user at the center of the information society. This view heavily relies on 4G wireless and mobile communications. 4G is all about an integrated, global network, based on an open systems approach. Integrating different types of wireless networks with wire-line backbone network seamlessly, and convergence of voice, multimedia and data traffic over a single IP-based core network are the main foci of 4G. With the availability of ultra-high bandwidth of up to 100 Mbps, multimedia services can be supported efficiently; ubiquitous computing is enabled with enhanced system mobility and portability support, and location-based services

Fig.2 : 4G Networks

A. Evolution of MANET

- In 1970, Normanl Abramson and his fellow researchers at the University of Hawaii invented ALOHAnet.
- In 1972 DARPA Packet Radio Network (PRNet)
- In 1980 Survivable Radio Networks (SURAN).

- During 1980 emergence of Internet Emerging Task

Force (IETF), termed the mobile ad hoc networking group.

- In 1994 emergence of Bluetooth by Ericsson.

B. Characteristics of MANET

- Network is not depend on any fix infrastructure for its operation.
- Eas of deployment
- Speed of deployment
- Dynamic Chanign g Topology of nodes
- Multi-hop network
- Each node is working as intelligent node
- Not any mediator networking device is required for communicatons
- Each node is work as a DTE (Data Terminal
- Equipment) and DCE (Data Communication Equipment)

III. AD-HOC APPLICATIONS

- Tactical networks : Military Communication automated Battle fields
- Sensor Network : Remote weathers for sensors, earth
  activities
- Emergency Services : Disaster recovery, earthquakes,
  crowd control and commando operations
- Educational Applications : Setup virtual class & conference rooms
- Entertainment : Multi-user games, robotics pets.
- Location Aware Services : Automatic Call forwarding,
  advertise location specific services, Location–dependent travel guide.

In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. To present the huge amount of research activities on ad hoc networks in a systematic/organic way, we will use, as a reference, the simplified architecture shown in as shown in the figure, the research activities will be grouped, according to a layered approach into three main areas:

•Enabling technologies;

•Networking;

• Middleware and applications

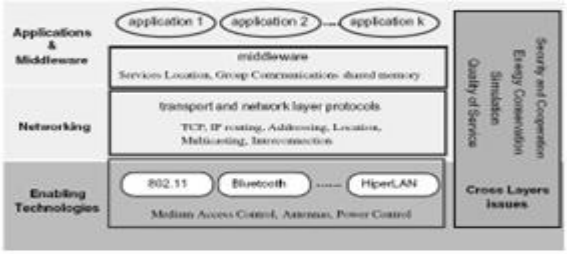

Fig 3. MANET Architecture

In addition, as shown in the figure, several issues (energy management, security and cooperation, quality of service, network simulation) span all areas, and we discuss them separately. Ad hoc networks can be classified, depending on their coverage area, as : Body (BAN), Personal (PAN), Local (LAN), Metropolitan (MAN) and Wide(WAN) area networks. Ad-hoc singlehop BAN, PAN and LAN wireless technologies are already common on the market, these technologies constituting the building blocks for constructing small, multi-hop, ad hoc networks that extend their range over multiple radio hops. For these reasons, BAN, PAN and LAN technologies constitute the Enabling technologies for ad hoc networking.

The success of a network technology is connected to the development of networking products at a competitive price. A major factor in achieving this goal is the availability of appropriate networking standards. Currently, two main standards are emerging for ad hoc wireless networks: the IEEE 802.11 standard for WLANs, and the Bluetooth specifications 3 for short-range wireless communications.

IV. BLUETOOTH

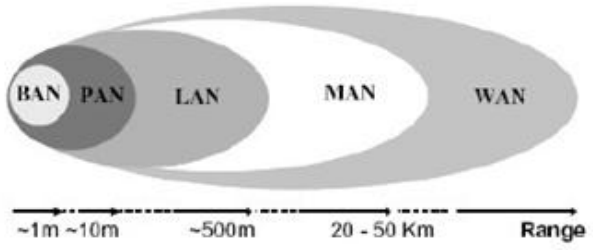

Fig. 4 : Bluetooth range

The Bluetooth technology is a de-facto standard for low-cost, short-range radio links between mobile PCs, mobile phones, and other portable devices. The Bluetooth Special Interest Group (SIG) releases the Bluetooth specifications. Bluetooth specifications were established by the joint effort from over two thousand industry leading companies including 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, Toshiba, etc. under the umbrella of Bluetooth SIG. In addition, the IEEE 802.15 Working Group for Wireless Personal Area Networks approved its first WPAN standard derived from the Bluetooth Specification. The IEEE 802.15.1 standard is based on the lower portions of the Bluetooth specification. A Bluetooth unit, integrated into a microchip, enables wireless ad hoc communications, of voice and data between portable and/or fixed electronic devices like computers, cellular phones, printers, and digital cameras. Due to its low-cost target, Bluetooth microchips may become embedded in virtually all consumer electronic devices in the future.

V. IEEE 802.11 NETWORKS

The IEEE adopted the first wireless local area network

standard, named IEEE 802.11, with data rates up to 2 Mbps. Since then, several task groups (designated by the letters from_a_, _b_, _c_, etc.) have been created to extend the IEEE 802.11standard. Task groups_ 802.11b and 802.11a have completed their work by providing two relevant extensions to the original standard, which are often referred to with the friendly name of Wireless Fidelity (Wi-Fi). The 802.11b task group produced a standard for WLAN operations in 2.4 GHz band, with data rates up to 11 Mbps and backward compatibility. This standard, published in 1999, has become an „„overnight success"", with several IEEE 802.11b products available on the market currently. The 802.11a task group created a standard for WLAN operation in the 5 GHz band, withdata rates up to 54 Mbps. Among the other task groups, it is worth mentioning the task group 802.11e (attempting to enhance the MAC with QoS features to support voice and video over 802.11 networks), and the task group 802.11g (that is working to develop a higher speed extension to the 802.11b). The IEEE 802.11 standard defines two operational modes for WLANs: infrastructure-based and infrastructure-less or ad hoc. Network interface cards can be set to work in either of these modes but not in both simultaneously. Infrastructure mode resembles cellular infrastructure-based networks. It is the mode commonly used to construct the so-called Wi-Fi hotspots, i.e., to provide wireless access to the Internet. In the ad hoc mode, any station that is within the transmission range of any other, after a synchronization phase, can start communicating.

VI. MAC PROTOCOL

Bluetooth and IEEE 802.11 technologies exemplify the two main categories in which multiple access networks can be categorized into: random access (e.g., CSMA, CSMA/CD) and controlled access (e.g., TDMA, token passing schemes, etc.). The lack of an infrastructure, and the peer-to-peer nature of ad hoc networking, make random access protocols the natural choice for medium access control in ad hoc networks. Indeed, most proposals of MAC protocols for ad hoc networks are based on the random access paradigm; in addition, the CSMA/CA scheme was selected (due to the inherent flexibility of this scheme) by the IEEE802.11 committee as the basis for its standards. On the other hand, demand assignment access schemes (even though generally more complex) are more suitable for environments that need guarantees on the Quality of Service (QoS) perceived by its users. Several controlled access schemes exist, e.g., TDMA, CDMA, token-passing, etc. Among these, TDMA is the most commonly used in ad hoc networks. In the TDMA approach, the channel is generally organized in frames, where each frame contains a fixed number of time slots. The mobile hosts phenomena.

VII. NETWORK SECURITY AND COOPERATION

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design.Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers_ control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. Finally, the security of routing protocols in the MANET dynamic environment is an additional challenge. The self-organizing environment introduces new security issues that are not addressed by the basic security services provided for infrastructure based networks. Security mechanisms that solely enforce the correctness or integrity of network operations would thus not be sufficient in MANET. A basic requirement for keeping the network operational is to enforce ad hoc nodes contribution to network operations, despite the conflicting tendency (motivated by the energy scarcity) of each node towards selfishness.

VIII. SECURITY ATTACKS

Securing wireless ad hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context The complexity and diversity of the field (different applications have different security constraints) led to a multitude of proposals that cannot be all surveyed in this article. Detailed analyses of ad hoc networking security issues and solutions can be found in. Below we summarize only the main directions of security in ad hoc networks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network. These attacks can be grouped in: Impersonation, Denial of service, and Disclosure attack.

Secure routing : Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. Recent studies brought up also a new type of attack that goes under the name of wormhole attack mentioned earlier. Cooperation enforcing : A basic requirement for keeping an ad hoc network operational is to enforce ad hoc nodes contribution to basic network functions such as packet forwarding and routing. Unlike networks using dedicated nodes to support basic network functions including packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This difference is at the core of some of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hocothers to forward packets on its behalf. Such a node uses the network but does not cooperate.

IX. SIMULATION AND PERFORMANCE EVALUATION

There are two main approaches in system performance evaluation: the first uses measurements; the second is based on a representation of the system behavior via a model Measurement techniques are applied to real systems, and thus they can be applied only when a real system, or a prototype of it, is available. Currently, only few measurements studies on real ad hoc testbeds can be found in the literature. The Uppsala University APE testbed is one of the largest, having run tests with more than thirty nodes. The results from this testbed are very important as they are pointing out problems that were not detected by preceding simulation studies. An important problem, related to the different transmission ranges for 802.11b control and data frames, is the so-called communication gray zones problem. This problem was revealed by a group of researchers at the Uppsala University, while measuring the performance of their own implementation of the AODV routing protocol in an IEEE 802.11b ad hoc network. Observing an unexpected large amount of packets_ losses, mainly during route changes, it was found that increase in packet loss occurred in some specific geographic areas termed called "communication gray zones". In such zones, the packet loss experienced by a station may be extremely high, up to 100%, thus severely affecting the performance of applications associated with a continuous packet flow (e.g., file transfers and multimedia streaming). It was also found that the reason for this phenomenon is that a station inside a gray zone is considered (using the routing information) reachable by a neighboring station, while actual data communication between the stations is not possible. The same problem was found to affect other routing protocols, such as OLSR. It is important to point out that communication gray zone problem cannot be revealed by commonly used simulation tools (e.g., NS-2, Glomosim), as in these 802.11 models both unicast and broadcast transmissions are performed at 2 Mbps, and hence have the same transmission range. Constructing a real ad hoc network testbed for a given scenario is typically expensive and remains limited in terms of working scenarios, mobility models, etc. Furthermore, measurements are generally non-repeatable. For these reasons, protocols scalability, sensitiveness to users mobility patterns and speeds are difficult to investigate on a real testbed. Using a simulation or analytic model, on the other hand, permits the study of system behavior by varying all its parameters, and considering a large spectrum of network scenarios. Evaluating system performance via a model consists of two steps: (i) defining the system model, and (ii) solving the model using analytical and/or simulative techniques. Analytical methods are often not detailed enough for the ad hoc networks evaluation and in terms of accounting for mobility, in their infancy. On the other hand, simulation modeling is a more standardized, mature, and flexible tool for modeling various protocols and network scenarios, and allows (by running the simulation model) collection and analyses that fully characterize the protocol performance in most cases.

Mobility models: The ability of ad hoc networks protocols to correctly behave in a dynamic environment, where devices position may continuously change, is a key issue

Network simulators : Most MANET simulative studies are based on simulation tools. The main advantage of these tools is that they provide libraries containing predefined models for most communication protocols.

X. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node"s IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. route Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a reply (RREP) packet back to the neighbor from which it first received the RREQ (Fig. 5). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used

within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message (an RREP with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route.

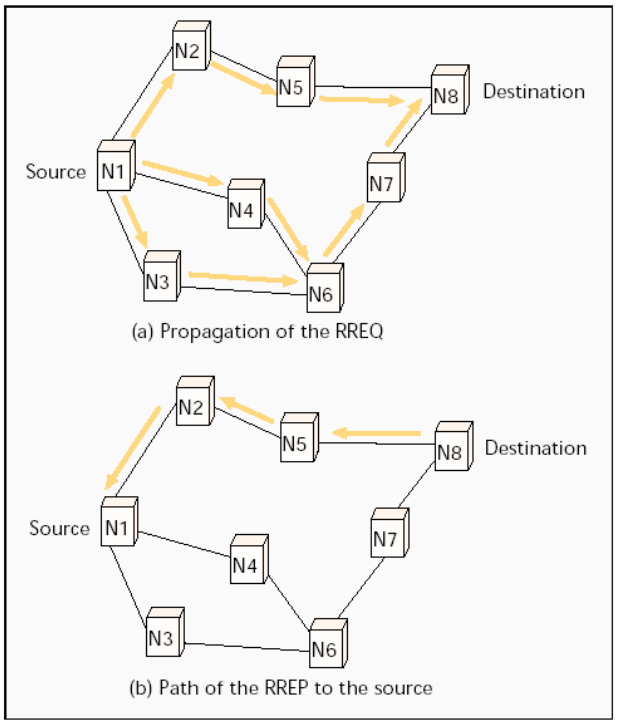

Figure 5. AODV route discoveries

CONCLUSIONS

In coming years, mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable. Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self-administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-hoc Networks. So, it becomes the best solution of different problems of network.

REFERENCES

[1] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.
[2] A. Ahuja et al., Performance of TCP over different routing protocols in mobile ad-hoc networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC 2000), Tokyo, Japan, May 2000.
[3] B.Kalaavathi,et.Al, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1470874 Raj Kamal, Mobile Computing, Oxford University Press, 2009.
[4] Proceedings IT in Academics, Sinhgad Institute of Management, Pune, India, 2009.
[5] G. Anastasi, M. Conti, E. Gregori, A. Passarella, A power saving architecture for web access from mobile computers, in: Proceedings of the Networking 2002, Lecture Notes in Computer Science, vol. 2345, Springer, Berlin, 2002.
[6] S. Basagni, Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks, in: Proceedings of the IEEE Vehicular Technology Conference (VTC) 1999, Amsterdam, The Netherlands, September 19–2004.
[7] C. Bisdikian, An overview of the Bluetooth wireless technology, IEEE Communication Magazine, December2001.
[8] J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, J. Jetcheva, A Performance Comparison of Multi-Hop Wireless Ad Hoc network Routing Protocols, Proc. Of MobiCom˝98, Oct. 1998
[9] P. Sinha, R. Sivakumar, V. Bharghavan, CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm, , IEEE INFOCOM˝99
[10] E. R. Royer, C.-K. Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, , IEEE Personal Communications, Apr. 1999
[11] V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks, , IEEE INFOCOM˝97, 1997
[12] Special Issue on Wireless Ad Hoc Networks, IEEE Journal on Selected Areas in Communications, Aug. 1999