Information Technology Journal 3 (2): 168-175, 2004
ISSN 1682-6027

A Survey on Mobile Ad Hoc Wireless Network

Samba Sesay, Zongkai Yang and Jianhua He
Department of Telecommunication and Information Technology,
Huazhong University of Science and Technology Wuhan, 430074, People's Republic of China

Abstract: This paper presents a coherent survey on ad hoc wireless networks, with the intent of serving as a quick reference to the current research issues in ad hoc networking. It starts with a background on the origin and development stages of ad hoc network, then summaries the characteristics, capabilities, applications and design constraints of ad hoc network fully distinguishing it from traditional networks. The paper discuses a broad range of research issues such as Routing, Medium Access, Multicasting, Quality of service, TCP performance, Energy, Security and Bluetooth, outlining the major challenges which have to be solved before widespread deployment of the technology is possible. Through this survey it would be seen that Ad hoc Networking presence an interesting research area inheriting the problems of wireless and mobile communications in their most difficult form.

Key words: Ad hoc network, routing, MAC, multicasting, quality of service, TCP, energy, security, bluetooth

BACKGROUND

Early ad hoc networking applications can be traced back to the DARPA (Defense Advance Research Projects Agency) Packet Radio Network (PRNet) project in 1972[1], which was primarily inspired by the efficiency of the packet switching technology, such as bandwidth sharing and store and-forward routing and its possible application in mobile wireless environment. In PRNet network nodes and devices (repeaters, routers etc.) were all mobile although mobility was limited. These advanced protocol was consider good for the 1970s. With the progress in time, advance in microelectronics technology has made it possible to integrate nodes and network devices into a single unit called Ad hoc node. And the wireless interconnection of such nodes is referred to as Ad hoc Network Active research work on ad hoc networks started in 1995 in a conference session of Internet Engineering Task Force (IETF). Early discussions centered on military tactical networks, satellite networks and wearable computer networks, with specific concerns being raised relative to adaptation of existing routing protocols to support IP networking in a highly dynamic environments. By 1996 this work had evolved into the Mobile Ad-Hoc Network (MANET) and finally to the charter of the MANET working group (WG) of the IETF in 1997. The task of the MANET WG is to specify standard interfaces and protocols for support of IP-based internet working over ad-hoc networks.

More recently, the Ad-Hoc Wireless Networking/Computing Consortium was established, with the goal of coalescing the interests and efforts of industry and academics, in order to apply ad-hoc networking technology to applications ranging from home wireless, to wide area peer-to-remote networking and communications.

INTRODUCTION

Mobile Ad hoc Networks are formed by autonomous system of mobile hosts connected by wireless links with no supporting fixed infrastructure or central administration. Communication is directly between nodes or through intermediate nodes acting as routers. The advantages of such a network are rapid deployment, robustness, flexibility and inherent support for mobility. In some application environments, such as battlefield communications, national crises, disaster recovery (fire, flood, earth quake) etc., the wired network is not available and ad hoc networks provide the only feasible means for communications and information access. Also Ad hoc network is now playing important role in civilian forums such as campus recreations, conferences, electronic classrooms etc.

The vision of ad hoc networks is wireless Internet, where users can move anywhere anytime and still remaining connected with the rest of the world[2,3].

The successful implementation of ad hoc wireless networking technology presents a unique set of

Corresponding Author: Samba Sesay, Department of Telecommunication and Information Technology, Huazhong University of Science and Technology, Wuhan, People's Republic of China
E-mail: sambasey@yahoo.com

challenges that differ from traditional wireless systems and wired networks.

This paper discus the research issues generated by these challenges and as such present a detailed overview of ad hoc networking.

Ad hoc MAC protocols research issues: There are basically two main categories of MAC protocols: Random Access Protocols–wherein nodes compete with one and other to gain full access to the shared medium and Controlled Access Protocols–wherein an infrastructure or Master node decides which node get access to the medium. The lack of an infrastructure and the peer-to peer nature of ad hoc networking, makes Random Access Protocols the natural choice for medium access control in ad hoc networks. Thus most ad hoc MAC protocols are based on the random access paradigm. Example includes MACA (Multiple Access with Collision Avoidance)[4], MACAW (MACA with Acknowledgment), MACA-BI (MACA by Invitation)[5], DBTMA (Dual Busy Tone Multiple Access) and FAMA (Floor Acquisition Multiple Access). Amongst these protocols CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) a variant of MACA was selected by IEEE 802.11 Committee as the basis for its standards due to it inherent flexibility and because it solves hidden and expose terminal problem through RTS-CTS-DATA-ACK handshake[6-9].

MAC Controlled Access Protocols example TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access), CDMA (Code Division Multiple Access) and TSMA (Time Spread Multiple Access) though seldom used in ad hoc networks are preferred in environments that needs Quality of Service (QOS) guarantee as their transmissions are collision free. Their applications are mainly adapted to Bluetooth and cluster-based ad hoc networks where access to the shared medium is control by Master nodes.

Optimization to improve the performance of ad hoc MAC protocols includes algorithms to reduce mobile node energy consumption, like allowing nodes to sleep during idle period and in the incorporation of directional antenna. Typically ad hoc network nodes assume the use of omni-directional antennas. With omni-directional antennas, while two nodes are communicating using a given channel, the MAC protocol (e.g., IEEE 802.11) requires that all other nodes in the vicinity stay silent. But with directional antennas, two pairs of nodes located in each other's vicinity may potentially simultaneously access the channel, depending on the directions of transmission. Directional antennas can adaptively select radio signals of interest in specific directions, while filtering out unwanted interference from other directions. This can increase spatial reuse of the wireless channel, in addition to higher power gain[10].

Ad hoc routing protocols: Ad hoc routing protocols[11-17] are typically subdivided into two main categories: Proactive (Table-Driven) Routing Protocols and Reactive (On-Demand) routing protocols. Proactive routing protocols are derived from legacy Internet distance-vector and link-state protocols. They maintain tables that store routing information. And for any change in network topology, they triggers propagating updates throughout the network in order to maintain a consistent network view. This can cause substantial overhead affecting bandwidth utilization, throughput as well as power usage. The advantage is that routes to any destination are always available without the overhead of a route discovery but such protocols cannot perform properly when the mobility rate in the network is high or when there are a large number of nodes in the network. Protocols in this category differ in the number of tables they contain as well as on the details of how they are updated. For example, nodes in Destination-Sequenced Distance Vector (DSDV) algorithm maintain route information to every other node in the network. As the network status changes full updates are exchange among all nodes. The Wireless Routing Protocol (WRP) localizes the updates to the immediate neighbors. When a new node A moves into range of a node B and a hello message is received from it, A is added to B's routing table and sent a full copy of the table. When a link fails, a node sends updates to its neighbors. The Cluster Gateway Switch Routing (CGSR) protocol reduces the size of the tables and amount of information propagation by having each cluster of nodes elect a cluster head. Network-wide information is only exchanged among the cluster heads. While the amount of information propagation is reduced, this results in inefficient routes. The Fisheye State Routing Protocol has been recently suggested, this differ from others in that the update frequency is inversely related to the distance between any two nodes[18].

On-Demand routing protocols are characterized by a path discovery mechanism that is initiated when a source needs to communicate with a destination that it does not know how to reach. The Route Discovery is usually in the form of query flood. Generally, on-demand routing requires less over-head than table-driven routing; but it incurs a path discovery delay whenever a new path is needed.

The differences between on-demand protocols are in the implementation of the path discovery mechanism and optimizations of it. Dynamic Source Routing (DSR) uses source routing, with every packet carrying the full path

information with it[19,20]. Similarly, Ad hoc On-Demand Distance Vector Routing (AODV[21,22] is an on-demand version of DSDV where the path results in exchange of the portions of the routing table necessary for establishing the route. Other on-demand algorithms include Temporally Ordered Routing Algorithm (TORA)[23] that discovers multiple paths from a source to destination and re-initiates discovery only when all of them have failed.

Associativity-Based Routing (ABR) incorporates route quality by preferring hops that have been static for a long period. Similarly, Signal Stability Routing (SSR) prefers routes with strong received signal power.

In addition to proactive and reactive protocols are hybrid protocols. The Zone-Based Hierarchical Link State Routing Protocol (ZRP) is an example of hybrid protocol that combines both proactive and reactive approaches thus trying to bring together the advantages of the two approaches. ZRP defines around each node a zone that contains the neighbors within a given number of hops from the node. Proactive algorithm is used by a node to maintain route to all other nodes within its zone and reactive algorithms are used by the node to determine routes to nodes outside it zone[24].

Presently, TORA, DSR, AODV and ZRP are the four protocols currently under study by the IETF MANET working group as candidate protocols for evaluation and standardization.

Ad hoc multicasting: Multicasting is the transmission of datagrams to a group of zero or more hosts identified by a single destination address. Multicast service is critical in applications where one-to-many dissemination is necessary. Such as characterized by close collaboration of teams (e.g., rescue patrols, military battalions, scientists, etc.) with requirements for audio and video conferencing and sharing of text and images. Multicast routing strategy optimization resource usage; this is seen to be as an important feature for energy- and bandwidth-constrained networks as mobile ad hoc networks. However multicasting in MANET is much more complex than in wired networks because of host mobility, interference of wireless signals and the broadcast nature of wireless communication.

Several ad hoc multicast routing algorithms have been proposed and evaluated. Although there is the conviction that ad hoc multicast routing technology is a relatively immature technology area and much of ad hoc unicast routing protocols have their multicast variants.

There are three basic categories of Ad hoc multicast algorithms. A first, naive, approach is to simply flood the network. Every node receiving a message floods it to a list of neighbors. Flooding is robust and well suited to network with high mobility. However, bandwidth is severely wasted as a result of unnecessary forwarding of duplicate data. The other two approaches are: source-based and core-based (group-shared). The source-based protocol tries to maintain a per-source multicast tree from each source host to every member in the multicast group. Thus, in an environment with G multicast groups where each group has S multicast nodes, there will be (G*S) multicast trees established and maintained. The advantage is that each multicast packet is forwarded along the most efficient path from the source node to each and every multicast group member. This scheme however suffers from scalability problems because a lot of overhead is incurred in establishing and maintaining several multicast trees as the number of multicast groups and multicast source nodes increases. Frequent topological changes in mobile ad hoc network, becomes another factor in increasing the overall overhead since many source-based trees will be affected and will need to be repaired. An example is DVMRP (Distance Vector Multicast Routing Protocol).

The core-based protocol, on the other hand, uses only one multicast tree rooted at a core host. The tree then spans from the core host to every member of the multicast group. Its advantage is that it is more scalable than source-based with reduced overhead.

A disadvantage of core-based protocol is that traffic is concentrated on the shared links, which results in a high tendency for congestion at the shared links. In addition, the multicast packets tend to be forwarded along less optimal paths since they are forced to transmit along the shared tree. Moreover core node, which is the most critical component in this scheme, becomes the single point of failure. Examples of core-based protocols are Multicast Ad hoc On-Demand Distance Vector (MAODV), Ad hoc Multicast Routing (AMRoute), Ad hoc Multicast Routing Protocol utilizing increasing id numbers (AMRIS).

To adapt to the dynamic nature of ad hoc networks and alternate to tree approach has been proposed known as Multicast Mesh. A mesh is different from a tree since each node in the mesh can have multiple parents. Using a single mesh structure spanning all multicast group members, multiple paths exist and they are immediately available for use when the primary path is broken. Therefore, a multicast mesh provides multiple redundant paths, avoiding frequent mesh configurations. This minimizes the disruption of on-going multicast sessions and reduces protocol overhead. An example protocol is Core-Assisted Mesh Protocol (CAMP) and the On-Demand Multicast Routing Protocol (ODMRP)[1].

Quality of service (QOS): Due to the broadcast and dynamic nature of Mobile Ad hoc Networks (MANET), providing Quality of Service (QOS) other than best effort, is a very challenging task. But QOS is important for the mobile ad hoc network to interconnect with wired networks which support QOS (e.g. ATM, Internet, etc.) and for real time applications.

A lot of work has been done in supporting QOS in the Internet and other network architectures, but unfortunately none of them is directly suitable in MANET environment. To support QOS, the link state information such as delay, bandwidth, cost, loss rate and error rate in the network should be available and manageable. However, getting and managing this link state information is very difficult. Because of resource limitations, mobility and random joining and leaving of network nodes.

Quality of service provisioning in ad hoc network is not dedicated to any specific layer rather it requires coordinated efforts from all layers. Thus QOS support components includes: QOS models, QOS resource reservation signaling, QOS routing and QOS medium access control (MAC)[25].

QOS models: QOS Model specifies the architecture in which some kinds of services could be provided in MANET. It is the system goal to be achieved. All other QOS components, such as QOS signaling, QOS Routing and QOS MAC must cooperate together to achieve this goal. The Flexible QOS Model for MANET (FQMM)[26] is based both on IntServ and Diffserv. Specifically, for applications with high priority, per-flow QOS guarantees of IntServ are provided. On the other hand, applications with lower priorities achieve DiffServ per class differentiation. As FQMM separately applies both IntServ and DiffServ for different priorities, the drawbacks related to IntServ and DiffServ still remain. A more realistic direction for QOS provisioning in ad hoc network is based on an adaptive QOS model: applications must adapt to the time varying resources offered by the network.

QOS resource reservation signaling: QOS Signaling is the process of setting up a connection from the source to the destination that involves reservation of resources in the intermediate nodes. QOS Signaling acts as a control center in QOS support. It reserve and release resources, setup, tear down and renegotiate flows in the networks.

QOS Signaling systems can be divided into in-band signaling and out-of-band signaling. In in-band signaling, control information is piggybacked within data packets while in out-of-band signaling control information are sent as explicit packets.

INSIGNIA[27] is an example of In-Band Signaling system that supports QOS in MANET. It supports fast flow reservation, restoration and adaptation algorithms that are specifically designed to deliver adaptive real-time service in a mobile ad hoc networking environment. To establish an adaptive real-time flow, Signaling information is carried in the IP option of every IP data packet, which is called the INSIGNIA option. When an intermediate node receive packet with the appropriate option field, they reserve the resources if available and forward the packet towards the destination. The destination sends a QOS report message to the source periodically. The QOS report will indicate the state of the network to the source. This report could take a different path to the source. The source takes adaptation decisions based on the QOS report. All the intermediate nodes maintain soft state. The absence of traffic will result in the resource allocated for the flow being recovered.

QOS routing: QOS routing refers to the discovery and maintenance of routes that can satisfy QOS objectives under given resource constraints. A QOS routing protocols should work together with QOS signaling to establish paths through the network that meet end-to-end QOS requirements, such as delay or delay jitter bounds, bandwidth demand, or multi-metric constraints. One main difficulty for QOS routing protocols in MANET is that the traditional meaning that the required QOS should be ensured once a feasible path is established is no longer true. The reserved resource may not be guaranteed because of the mobility-caused path breakage or power depletion of the mobile hosts[28,29].

Ticket-based Probing Algorithm[30] is an example of QOS routing protocol. The basic idea in using tickets is to limit the number of candidate paths searched. When a source wants to find QOS paths to a destination, it issues probe messages with some tickets. The number of the tickets is based on the available state information. One ticket corresponds to one path searching and one probe message should carry at least one ticket. So the number tickets bound the maximum number of searched paths. When an intermediate node receives a probe message with n tickets, based on its local state information, it decides whether to and how to split the n tickets and where to forward the probe(s). When the destination host receives a probe message, a possible path from the source to the destination is found. Other QOS routing protocols include Preemptive Routing[31], Multi-path Routing and Power Aware Routing[32].

QOS medium access control (MAC): QOS MAC Protocol solves the problems of medium contention, hidden and expose terminal problem, supports reliable unicast

communication and provides resource reservation for real-time traffic in a distributed wireless environment. Among numerous MAC protocols and improvements that have been proposed, protocols that can provide QOS guarantees to real time traffic in a distributed wireless environment include GAMA/PR protocol and Black-Burst (BB) contention mechanism.

TCP issues: TCP is an effective connection-oriented transport control protocol that provides the essential flow control and congestion control required to ensure reliable packet delivery. TCP was originally designed to work in fixed networks. Because error rate in wired network is quite low, TCP uses packet loss as an indication for network congestion and deals with this effectively by making corresponding transmission adjustment to its congestion window[33]. In MANET several factors impact on the performance of TCP.

Mobility may cause route failures and hence, packet losses and increased delays. TCP misinterprets these losses as congestion and invokes the congestion control mechanism, potentially leading to unnecessary transmissions and throughput degradation. In addition, the stations_ mobility may exacerbate unfairness between competitive TCP sessions.

In ad hoc networks even when the stations are static, performance will be far from ideal as a station activity is limited by the activity of neighboring stations inside the same TX_Range, IF_Range or PCS_Range and by the interference caused by hidden and exposed stations.

TCP congestion window size may have a significant impact on performance. In[34,35], the authors show that, for a given network topology and traffic patterns, there exists an optimal value of the TCP congestion window size at which channel utilization is maximized. However, TCP does not operate around this optimal point, but typically with a window that is much larger, leading to decreased throughput (10–30% throughput degradation) and increased packet loss. These losses are due to link-layer drops: a station fails to reach its adjacent station due to the contention/interference of other stations. By increasing the congestion window size, the number of packets in the pipe between the sender and the receiver is increased and hence the contention at the link-level increases, as well. Small congestion windows (i.e., 1–3 packets) typically provide the best performance[36].

The interaction of MAC protocol (IEEE 802.11) with the TCP protocol mechanisms may lead to unexpected phenomena in a multi-hop environment. For example, in the case of simultaneous TCP flows, severe unfairness problems and–in extreme cases–capture of the channel by few flows may occur[37]. Furthermore, instantaneous TCP throughput may be very unstable also with a single TCP connection. These phenomena can be reduced/ exacerbated by using small/large TCP congestion window. Such problem does not appear, or appear with less intensity, when the UDP protocol is used[38].

Numerous new mechanisms for TCP optimization have also been proposed with the aim of resolving MANET specific issues, including adaptation of TCP error-detection and recovery strategies to the ad hoc environment. To minimize the impact of mobility and link disconnection on TCP performance[34], proposed to introduce explicit signaling (Route Failure and Route Reestablishment notifications) from intermediate nodes to notify the sender TCP of the disruption of the current route and construction of a new one. In this way, TCP after a link failure does not activates the congestion avoidance mechanisms, but simply freezes its status that will be resumed when a new route is found. Also an Explicit Link Failure Notification (ELFN) mechanism is introduced. The ELFN objective is to provide (through ELFN messages) the TCP at the sender side explicit indications about link and route failures[39,40].

Energy conservation: Mobile devices rely on batteries for energy. Battery power is finite and represents one of the greatest constraints in designing algorithms for mobile devices[41]. Projections on progress in battery technology show that only small improvements in the battery capacity are expected in the near future. Under these conditions, it is vital that power utilization be managed efficiently by identifying ways to use less power, preferably with no impact on the applications. Limitation on battery life and the additional energy requirements for supporting network operations (e.g., routing) inside each node, makes the energy conservation one of the main concern in ad hoc networking. The importance of this problem has produced a great deal of research on energy saving in wireless networks in general, and ad hoc networks in particular[42-44]. Strategies for power saving have been investigated at the various protocol layers. And the techniques include:

- Physical layer
  - Use of directional antenna
  - Controlling the transmission power with knowledge of neighborhood.
- Data-link layer
  - Avoid unnecessary retransmissions.
  - Avoid collisions in channel access whenever possible.
  - Put receiver in standby mode whenever possible.
  - Use/allocate contiguous slots for transmission and reception whenever possible.
  - Turn radio off (sleep) when not transmitting or receiving.

- Network layer
  - Consider route-relaying load.
  - Consider battery life in route selection.
  - Reduce frequency of sending control message.
  - Optimize size of control headers.
  - Efficient route reconfiguration techniques.
- Transport layer
  - Avoid repeated retransmissions.
  - Handle packet loss in a localized manner.
  - Use power-efficient error control schemes[1].

Security issues: Performing communication in free space and the broadcast nature of ad hoc networks expose it to security attacks. Ad hoc wireless links are susceptible to attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Active attacks might allow the adversary to delete messages, inject erroneous, modify messages and impersonate a node, thereby violating availability, integrity, authentication and nonrepudiation.

Security is often considered to be the major "roadblock" in commercial application of ad hoc network technology. In civilian, especially commercial, applications even mere lack of cooperation may be enough to bring the network on its knees[45].

Understanding possible form of attacks is always the first step towards developing good security solutions. Two types of security mechanisms can generally be applied: preventive and detective. Preventive mechanisms are typically based on key-based cryptography. However, designing secure key distribution that allows the creation of unforgeable credentials in ad hoc networks is a challenging problem. Diffie–Hellman key exchange may indeed help to establish some temporary security between particular endpoints. However, they are also vulnerable to the man-in-the-middle attacks

The intrusion detection field studies how to discover that an intruder is attempting to penetrate the network to perform an attack. Most of the intrusion detection techniques developed on fixed wired network is not applicable to ad hoc network environment, as there are no traffic concentration points (switches, routers, etc.) where the intrusion detection system (IDS) can collect audit data for the entire network. The only available audit trace will be limited to communication activities taking place within the radio range and the intrusion detection algorithm must rely on this partial and localized information. A proposal for a new intrusion detection architecture that is both distributed and cooperative is presented in[46]. Here all nodes in the wireless ad hoc network participate in intrusion detection and reaction. Each node is responsible for detecting signs of intrusion locally and independently, but neighbors can collaboratively investigate in a broader range. The Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA)[43] is designed against denial of service attacks. The TIARA mechanisms limit the damage caused by intrusion attacks and allow for continued network operations at an acceptable level during such attacks. The Authenticated Routing for Ad hoc Network (ARAN) protocol is an on-demand, secure, routing protocol that detects and protects against malicious actions carried out by third parties in the ad hoc environment. The Secure Efficient Ad hoc Distance (SEAD) is a proactive secure routing protocol based on DSDV. SEAD deals with attackers that modify a routing table update message. The basic idea is to authenticate the sequence number and the metric field of a routing table update message using one-way hash functions. Hash chains and digital signatures are used by the SAODV mechanism to secure AODV.

Node cooperation enforcing is also an important issue in providing a secure ad hoc network. A node that does not cooperate is called a misbehaving node. Routing–forwarding misbehaviors can be caused by nodes that are malicious or selfish. A malicious node does not cooperate because it wants to intentionally damage network functioning by dropping packets. On the other hand, a selfish node does not intend to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. To cope with these problems, a self-organizing network must be based on an incentive for users to collaborate, thus avoiding selfish behavior[47].

Bluetooth: Bluetooth is an Ad hoc network of small groups or cluster called piconets. A piconet contains a master station and up to seven active (i.e., participating in data exchange) slaves simultaneously. The master decides which slave is the one to have access to the channel thus enabling contention and collision free transmissions. Independent piconets overlapping in the coverage areas to form a scatternet. Bluetooth operates in the 2.4 GHz industrial, scientific and medicine (ISM) band and is the de facto standard for low-cost, short-range (about 10 m), radio links between mobile PCS, mobile phones and other portable devices[48].

Ad hoc-networking is becoming increasingly important in today's world. And its importance is recognized by both the research and industry community, as evidenced by the flood of research activities, as well as the almost exponential growth in the Wireless LANs and Bluetooth technology. From a technical standpoint, despite the large volume of research activities and rapid progress made in the MANET technologies in the past

few years, almost all research areas (from enabling technologies to applications) still harbor many open issues. This paper also discuses a broad range of ad hoc research issues-Routing, Medium Access, Multicasting, Quality of service, TCP performance, Energy, Security and Bluetooth, outlining the major challenges which have to be solved before widespread deployment of the technology is possible.

Most of the research work on ad hoc network is being performed in the framework of the IETF MANET working group that serves as the standardizing body. The ultimate goal of ad hoc networking is wireless Internet.

REFERENCES

1. Toh. C.K., 2002. Ad hoc Mobile Wireless Networks Protocols and Systems. Prentice Hall, Inc.
2. Giordano, S, 2002. Mobile ad-hoc networks. In: I. Stojmenovic (Ed.), Handbook of Wireless Networks and Mobile Computing. Wiley, New York, pp: 325-343, 371-391.
3. Corson, S. and J. Macker, 1999. Mobile ad hoc networking (MANET), IETF RFC 2501, January, 1999.
4. Kam, P., 1990. MACA-A new channel access method for packet radio. In ARRL/CRRL Amateur Radio 9th Computer Networking Conference, pp: 134-140.
5. Talucci, F., M. Gerla, 1997. MACA-BI (MACA By Invitation) A wireless MAC protocol for high speed ad hoc networking. In Proceedings of ICUPC_97, November, 1997.
6. Xu, S.S.T., 2001. Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? IEEE Communication Magazine, pp: 130-137.
7. Xu, S.S.T., 2002. Revealing the problems with 802.11 MAC protocol in multi-hop wireless networks. Computer Networks, 38: 531-548
8. Anastasi, G., M. Conti and E. Gregori, 2003. IEEE 802.11 ad hoc networks: protocols, performance and open issues. IEEE Press and John Wiley and Sons, Inc., New York , USA.
9. Bianchi, G., L. Fratta and M. Oliveri, 1996. Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs. In Proceedings of PIMRC, Taipei, Taiwan, pp: 392-396.
10. Ramanathan, R., 2001. On the performance of ad hoc networks with beamforming antennas. In Proceedings of ACM MobiHoc, 2001.
11. Belding-Royer, E.M. and C.K. Toh, 1999. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications Magazine pp: 46-55.
12. Royer, E. M. and C.E. Perkins 1999. Multicast operation of the ad-hoc on-demand distance vector routing protocol. In Proceedings ACM/IEEE MOBICOM '99, Seattle, WA, Aug. 1999, pp: 207-218.
13. Maltz, D.A., J. Broch, J. Jetcheva and D.B. Johnson, 1999. The Effects of on-demand behavior in Routing protocols for multi-hop wireless Ad hoc networks. IEEE JSAC, 17.
14. Petteri, K., Classi.cation of ad hoc routing protocols, Seminar paper presented to Finnish Defence Forces, Naval Academy, Finland. Available at <http://keskus.hut../opetus/s38030/k02/Papers/12-Petteri.pdf>.
15. 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.
16. Mario, G. and H. Xiaoyan, 2002. Fisheye State Routing Protocol draft-ietf-manet-fsr-03.txt 55th IETF Meeting in Altanta, GA. 2002 .
17. Samir, R., D. Perkins, C.E. Elizabeth and M. Royer, 2000. Performance comparison of two on-demand routing protocols for ad hoc networks. In Proceedings INFOCOM, Tel Aviv, Israel.
18. Maltz, J.B. and D. Johnson, 2001. Lessons from a full-scale multi-hop wireless ad hoc network test bed. IEEE Personal Communications Magazine.
19. Broch, J., D. Johnson, D. Maltz, Y.C. Hu and G. Jetcheva, 2001. The Dynamic Source Routing Protocol for mobile Ad hoc Networks. Internet-Draft, draft-ietf-manet-dsr-05.txt.
20. Johnson, D. and D. Maltz, 1996. Dynamic Source Routing in Ad hoc wireless Networks. T. Imielinski and H. Korth, (Eds). Mobile Computing, Ch. 5, Kluwer.
21. Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. In Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications.
22. Perkins, C.E., E.M. Royer and S.R. Das, 2001. Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org / internet-drafts/draft-ietf-manet-aodv-08-txt,IETF Internet Draft.
23. Park, V. and S. Corson, 2001. Temporally-ordered Routing algorithm (TORA). Internet Draft, draft-ieft-manet-tora-spec-04-txt. July, 2001.
24. Haas, Z.J. and M.R. Pearlman, 1997. The zone routing protocol (ZRP) for ad hoc networks, Internet Draft hdraft-haaszone- routing-protocol-00.txti, pp: 153-181.
25. Kui, Wu. and H. Janelle, 2001. QOS support in mobile ad hoc networks. Crossing Boundaries an Interdisciplinary J., pp: 92-107

26. Xiao, H., W.K.G. Seah, A. Lo and K.C. Chua, 2000. A flexible quality of service model for mobile ad-hoc networks, IEEE VTC2000-spring, Tokyo, Japan, May, 2000.
27. Ahn, G.S., A.T. Campbell, S.B. Lee and X. Zhang, 1999. INSIGNIA. Internet Draft, draft-ietf-manet-insignia-01.txt, October, 1999.
28. Chen, W., T. Tsai and Gerla, 1997. QOS Routing performance in multi-hop, multimedia wireless networks in Proc. IEEE ICUPC, 1997.
29. Leonard, B.A. and S. Takuo, 2003. A Genetic Algorithm (GA) based routing method for Mobile Ad-hoc Networks. J. Interconnection Networks, 4: 257-270.
30. Chen, S. and K. Nahrstedt, 1999. Distributed Quality-of-Service Routing in Ad hoc Networks. IEEE J. Selected Areas in Communication, 17: 1488-1505.
31. Goff, T., N.B. Abu-Ghazaleh, D.S. Phatak and R. Kahveciogw, 2001. Preemptive Routing in Ad hoc Networks. ACM Sigmobile.
32. Toh, C-K., H. Cobb and D.A. Scout, 2001. Performance Evaluation of Battery-life Aware Routing Schemes for Wireless Ad hoc Networks. IEEE, ICC.
33. Stevens, W.R., 1994. TCP/IP Illustrated, Vol. 1. The Protocol, Addison-Wesley, Reading, MA.
34. Zhenghua, F., Z. Petros, X. Kaixin, L. Haiyun, L. Songwu, Z. Lixia and G. Mario, 2003. The impact of multihop wireless channel on tcp throughput and loss. In Proceedings of INFOCOM 2003. San Francisco, April, 2003.
35. Gavin, H. and H.V. Nitin, 2002. Analysis of TCP performance over mobile ad hoc networks. ACM/Kluwer J. Wireless Networks, 8: 275- 288.
36. Tang, K. and M. Gerla, 1999. Fair sharing of MAC under TCP in wireless ad hoc networks. In Proceedings of IEEE MMT_99, Venice (I), October, 1999.
37. Xu, K. and M. Gerla, 1996. TCP over an IEEE 802.11 ad hoc network: unfairness problems and solutions. UCLA Computer Science Department Technical Report--020019, May 2002._96, London, UK., pp: 1411-1416.
38. Ahuja, S., J.P. Singh and R. Shorey, 2000. 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.
39. Ahuja, S., J.P. Singh and R. Shorey, 2000. performance of TCP over different routing protocols in mobile Ad hoc networks. IEEE Personal Communications Magazine.
40. Petrioli, R.R. and J. Redi, 2001. Special Issue on Energy Conserving Protocols. ACM/Kluwer MONET 6, pp: 207-209.
41. Jones, K., P. Sivalingam, Agarwal and J.C. Chen, 2001. A survey of energy efficient network protocols for wireless and mobile networks. ACM/Kluwer Wireless Networks, 7: 343-358.
42. Anastasi, G., M. Conti, E. Gregori and A. Passarella 2003. Balancing energy saving and QOS in the mobile internet: an application-independent approach. In Proceedings of the 36th Hawaii International Conference on System Sciences, pp: 305- 314.
43. Forman, G.H. and J. Zahorjan, 1994. The challenges of mobile computing. IEEE Computer, pp: 38-47.
44. Urpi, M.A. and S.G. Bonuccelli, 2003. Modeling cooperation in mobile ad hoc networks: a formal description of sel.shness. In Proceedings of WiOpt 2003, Sophie-Antipolis.
45. Zhang, Y. and W. Lee, 2000. Intrusion detection in wireless ad-hoc networks. In Proceedings of the Sixth ACM International Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, MA, USA., August 6-11.
46. Ramanujan, A.A., J. Bonney, R. Hagelstrom and K. Thurber, 2000. Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). In Proceedings of MILCOM.
47. Capkun, S., L. Buttyan, J.P. Hubaux, 2003. Self-organized public-key management for mobile ad hoc networks, IEEE Transactions on Mobile Computing 2: 1536-1553.
48. Salonidis, T., P. Bhagwat, L. Tassiulas and R. LaMaire, 2001. Distributed topology construction of Bluetooth personal area networks. In Proceedings of INFOCOM 2001, Anchorage, pp: 1577-1586.