Routing Strategies in Mobile Ad Hoc Networks

Aasim Zafar

Department of Computer Science, Aligarh Muslim University, Aligarh, Email: aasimzafar@gmail.com

Abstract – Due to the inherent limitations and dynamic nature of mobile ad hoc networks, the routing is different from wired network. To meet the challenges of MANET, various routing strategies were proposed. This paper presents a survey of routing strategies employed in MANET and provides a quick reference of researches done in this area. This study gives an opportunity to analyze these strategies with an objective to achieve an efficient algorithm to overcome the challenges still suffered by MANETs and improve the performance.

Keywords: Mobile Ad hoc Networks, Position based Routing, Secure Routing, QoS Routing, Multicast and Unidirectional Routing.

----------♦----------

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) 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 router [1]. Routing in MANETs is quite different from that in a wired network. What makes ad hoc network different from wired networks is that all the usual rules about fixed topologies, fixed and known neighbors, fixed relationships between IP addresses and location, and more are not prevalent in ad hoc networks. Hosts and routers are usually on the same computer and are free to move randomly anywhere in the network. MANET nodes are equipped with wireless transmitters and receivers using antennas, which may be omnidirectional (broadcast), highly directional (point to point), possibly steerable, or some combination thereof [6]. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or ad hoc network exists between the nodes. The topology keeps on changing all the time, so desirability and even validity of paths change spontaneously without warning. Besides dynamic topology and bandwidth constraints, limited battery power and weak physical security makes MANET routing difficult and challenging. There are several well-known protocols in the literature that has been specifically developed to cope with the limitations imposed by ad hoc networking environments. Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, namely the table-driven and the on-demand approaches.

- *Table-driven protocols:* Proactive or table driven protocols follow a similar approach as used in wired routing. They continuously update their routing information in order to maintain the routing information of the dynamic topology. This helps them to efficiently route the packets as the routes are known prior to the arrival of packets. The main drawback of this approach is the amount of bandwidth they consume for continuous updates and maintenance of unused path as the topology changes frequently. Some of the popular routing protocols of this family are Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Cluster head Gateway Switch Routing Protocol (CGSRP) etc.

- *On-Demand Protocols:* Reactive protocols or On-demand protocols on the other hand determine the route only when required and maintain only those routes that are currently in use. This reduces the bandwidth consumption of the network. However this causes a significant delay as the routes are to be discovered before the packet can be transmitted. Moreover, if topology changes frequently, it generates a significant amount of traffic. Some of the well-known on-demand routing protocols are Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA).

In the following sections, a brief account of various routing strategies is being presented.

II. POSITION BASED ROUTING

As stated earlier mobile ad hoc network consists of wireless hosts that are free to move randomly. Unlike wired networks, it operates in the absence of any fixed infrastructure. The position of the hosts keeps on changing. Whenever a node has to transmit any message to other node, position of the destination may not be known in prior. In such case a route discovery process has to be initiated to determine the position of the destination. Dynamic topology is one of the major challenges faced by MANETs. Position based routing is one of the mechanisms introduced by researchers to reduce the efforts in determining the position of the nodes of the network. [2] presents a survey on position based routing in MANETs. Position based routing make forwarding decision based on the geographic position of packet's destination. Other than the destination's position, each node needs to know only its own position and the position of its one-hop neighbors in order to forward the packets. Since it is not necessary to maintain explicit routes, position based routing does scale well even if the network is highly dynamic. This is a major advantage in a mobile ad hoc network where the topology changes frequently. [3] suggests that using location information in routing, improve the performance for routing protocols for mobile ad hoc networks. By using location information, the search area for a route is limited to a smaller zone. This results in a significant reduction in the number of routing messages.

One of the examples of position based routing is Distance Routing Effect Algorithm for Mobility (DREAM). [4] Introduces a routing mechanism where each node maintains a position database that stores position information of other nodes that are part of the network. Like most the tables driven protocols, each node broadcasts control packets to inform all other nodes about their locations. With the location information stored at routing tables, data packets are partially flooded to nodes in the direction of the destination, and then it selects a set of one-hop neighbors that are located in the direction. If such steps are empty the data is flooded to the entire network. Otherwise, the set is enclosed in the data header and transmitted with the data. Only nodes specified in the header are qualified to receive and process the data packet. They repeat the same procedure by selecting their own set of one-hop neighbor updating the data header and sending the packet out. Location-Aided Routing (LAR) [3] uses the concept of '*expected zone*' and '*requested zone*' to reduce the search space for a desired route.

Another method for position based ad hoc routing is proposed in the GRID [5]. It is a reactive protocol (On-Demand), which treats the geographic area as a number of logical grids, each as a square. In each grid, one mobile host will be elected as the leader of the grid. Routing is thus performed in a grid-by-grid manner through grid leaders. It uses the location information in route discovery, packet relay, and route maintenance. Given a route as long as there exists a leader in each grid that constitutes the route, the route is considered alive. If a leader leaves its original grid, a behavior similar to the "handoff" procedure in cellular systems will take place. In this case the leader will pass its routing table to the next leader through broadcast.

III. SECURE ROUTING

The absence of any fixed infrastructure and consequently absence of authorization facilities impedes the usual practice of establishing a line of defense, separating nodes into trusted and non-trusted [6]. Highly mobile nature of MANETs makes it difficult to maintain clear picture of the network topology. In such an environment there is no guarantee that a path between two nodes is free from malicious nodes. Such malicious behavior of nodes poses two major problems:

- Either they could disrupt the route discovery process by giving false routing information i.e. any node could claim that it is one hop away from the sought destination, causing all routes to destination to pass through itself.
- Malicious node could corrupt any in-transit route reply packet and cause data to be misrouted.

Ad hoc networks are infrastructure-less networks and the nodes in the network act as hosts as well as routers. To ensure secure routing, nodes must be reliable. It is very difficult to distinguish between malicious nodes and nodes suffering from bad links.

The existing ad hoc routing protocols do not accommodate any security and are highly vulnerable to arracks. Vulnerabilities like easy theft of nodes, tampering, limited computational abilities and transient nature of devices give birth to possibilities of various possible attacks.

Several protocols have been established to protect the network layer in a mobile ad hoc network. [7] proposed a method to alleviate the detrimental effects of packet dropping. It suggested two mechanisms for secure data forwarding (i) detecting misbehaving nodes and reporting such events and (ii) maintaining a set of metrics that reflect the past behavior of other nodes. The best route is that

which comprises of nodes that do not have a history of avoiding forwarding packets along established routes. The ratings of nodes along a well-behaved route are periodically incremented, while reception of misbehavior alert dramatically decreases the node rating. When a node wants to discover a route, it calculates a path metric, and selects the route with the highest metric.

Another approach is Secure Ad hoc On-Demand Distance Vector (SAODV) [10] that is an extension of AODV Routing Protocol. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. It makes use of (i) digital signatures to authenticate the non-mutable fields of the messages and (ii) hash chains to secure the hop count information. Each node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that ad hoc node.

A different approach is to provide incentive to nodes so that they properly relay the user data [8]. The nodes are loaded with fictitious currency, and they forward the packets in exchange for currency. Each node purchases from its predecessors the received data packet and sells it to its successors along the path to the destination. Eventually the destination pays for the received packet.

Secure Message Transmission (SMT) [9] follows a different approach. It determines a set of multiple paths between a source and destination. It disperses the message into N pieces, such that successful reception of any M out of N pieces allows the reconstruction of the complete message at the destination. Each piece of the message is equipped with a cryptography header and is transmitted along one of the path. When destination receives the pieces, it sends an acknowledgement to the source informing of which pieces and routes were intact. If less than M pieces arrive at destination, the source retransmits the remaining pieces over the intact routes. If too few pieces arrive at destination, the source determines a different set of path and re-encodes the undelivered messages and sends it along the new determined path. Otherwise it proceeds with subsequent message transmissions.

[36] presents a protocol ARIADNE that prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. It authenticates the routing message using broadcast authentication scheme, or digital signatures, which adds only a single message authentication code (MAC) to a message for broadcast authentication. A network-wide shared secret key limits the attacker to replaying messages. Another approach Secure Routing Protocol (SRP) [6], complements SMT. It safeguards the route discovery and makes use of cryptographic tools.

[11] proposed Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the DSDV routing protocol. In order to support use of SEAD with nodes of limited CPU processing capability, and to guard against Denial-of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, it makes use of one-way hash functions and do not use asymmetric cryptographic operations.

[12] discusses the problem of intrusion detection in MANET. It uses anomaly detection approach based on data mining technologies. A secure Link State Protocol (SLSP) [13] for Mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops, which is termed as their zone.

[14] incorporates security in a position based routing Grid Location Service (GLS). Each node maintains a neighbor table that contains the identity and position information of each neighbor, along with the cryptographic keys required for secure communication. Each node maintains public and private keys for each neighbor. The private key is to decrypt the routing and update messages.

IV. QOS ROUTING

The role of a Quality of Service (QoS) routing strategy is to compute paths that are suitable for the different types of traffic generated by the various applications, while maximizing the utilization of network resources [14]. To fulfill these objectives, we require an algorithm that find multi-constrained path taking into consideration the state of network and the traffic requirements such as its need in terms of delay, loss rate and available bandwidth. The core of the QoS routing is the path computation algorithm. Instead of using shortest path for routing the data from source to destination, Qos routing must select several alternative paths that are able to satisfy a set of constraints, such as bandwidth constraints or limited power supply. The issues and difficulties for QoS support in MANETs as compared to wired networks include *features* and *consequences*. Features include unpredictable link properties, node mobility and limited battery life whereas consequences include hidden and exposed terminal problems, route maintenance and security.

The QoS requirement of a connection is given as a set of constraints: A link constraint specifies a restriction on the

use of links, Bandwidth constraint specifies the end-to-end QoS requirements on a single path, A tree constraint specifies the QoS requirement for the entire multicast tree, and Delay constraint- the longest end-to-end delay from the sender to any receiver in the tree, not exceed an upper bound multicast connection [16]. Some researchers have been active in the area of QoS support in MANETs, and have proposed a number of QoS routing protocols for this environment. Most of these protocols provide QoS support for the available bandwidth requirement for a given path, because bandwidth is the most critical parameter in most MANET applications.

Bandwidth Conservation

Bandwidth is widely used as a metric for QoS routing, alone or associated with other metrics, such as delay or number of hops. [37] proposes a QoS-aware routing protocol based on bandwidth estimation that incorporates an admission control scheme and a feedback scheme to meet the QoS requirements of real-time applications. This QoS-aware routing protocol makes use of the approximate bandwidth estimation to react to network traffic. It implements these schemes by using two bandwidth estimation methods to find the residual bandwidth available at each node to support new streams.

Core Extraction Distributed Ad Hoc Routing (CEDAR) algorithm is proposed as a QoS routing scheme for small and medium ad hoc networks consisting of tens to hundreds of nodes [15]. It has three main components (i) core extraction (ii) link state propagation (iii) route computation.

[20] Gives a detail description of the QoS models and QoS routing protocols and enlists the QoS extension of existing protocols. The QoS routing algorithm in [17] is an extension of the DSR protocol. It is on-demand and can operate in a single channel/code or multiple channel/code environments.

[18] presents a multi-path QoS routing protocol which is also an extension of DSR. The source searches for a multi-path QoS route to a particular destination satisfying certain bandwidth requirements. A number of tickets are distributed from the source to search for a satisfactory multi-path. This protocol provides a higher success rate for finding a QoS path satisfying the required bandwidth requirements when the bandwidth is very limited. When the available bandwidth is sufficient, this protocol performs similar to the protocols finding a uni-path to the destination.

A Five-Phase Reservation Protocol (FPRP) is given in [19] for QoS support in synchronous TDMA-based MANETs. FPRP uses a contention based mechanism to reserve TDMA slots. It performs both channel accessing and node broadcast scheduling at the same time. It also takes into account hidden terminal interference in the reservation process.

QoS-AODV an extension of AODV protocol incorporates path finding with the bandwidth reservation mechanism. QoS-AODV is fully aware of the bandwidth resource availability by coupling together routing and MAC TDMA layers. The source node establishes a virtual connection (VC) with the destination before sending the data. The VC establishment process includes route discovery, path bandwidth calculation and bandwidth reservation components [20].

Another protocol, named QoS-TORA is based on the link reversal best effort protocol TORA. Real-Time MAC (RT-MAC) is a MAC layer protocol for MANETs, which is an extension of DSDV. It is responsible for finding an end-to-end path that satisfies the QoS Bandwidth requirements.

Another protocol discussed in [21] presents network architecture for multimedia. The architecture assumes a code division access scheme. Another protocol that supports multimedia traffic over ad hoc WLAN is proposed in [22]. In [23] a QoS Routing Protocol with Mobility Prediction (QRMP) is presented. QRMP uses mobility prediction and QoS requirements on bandwidth and delay to select the most stable path. A different approach of using ticket based probing is presented in [24] which tries to provide QoS-constrained paths with a two staged approach. It uses a proactive routing to provide stations with rough knowledge about the state of the network.

Energy Conservation

All the above-discussed QoS routing protocol deal with the two widely used QoS constraints i.e. *Bandwidth* and *Delay.* However, another QoS constraint, which is equally important in MANETs, is *Limited Power supply.* Unlike the wired networks, mobile devices rely on batteries for energy. Battery is finite and is one of the greatest constraints in MANETs. When a node runs out of energy it must be turned off to replace, service or recharge its energy provider. During that time the node cannot be used in the network. Thus, the routing protocol must select a path whose nodes do not run out of energy while the data transmission takes place. The objective of using power control is to correctly adjust the power level of transmitting node, hence its transmission range to minimize the interference with its neighbors. This increases the performance of the wireless network by reducing packet loss, increasing the spatial reuse and reducing power consumption. A number of routing algorithms are developed which takes into account this aspect.

A system energy model is given in [25]. It computes the minimum transmission energy required at any node u to transmit to other node v in its transmission range as

$E_{(u,v)} = k\, d^{\alpha}_{(u,v)}$

Where k and α are constants, and α is either 2 or 4. and d is the distance between u and v. It models the ad hoc network by a weighted graph G = (N,L), where N is the set of mobile nodes and L is the set of full duplex communication links. The weight associated with a link $(u,v) \in L$ is the power level of its two endpoints u and v and its residual energy. The remaining energy of the battery at node u at any time t is $E_t(u)$. During the path selection, only that path is selected where node energy is greater than or equal to the required energy. This way the probability of packet loss is reduced due to low power, and hence throughput is increased.

In the routing protocol given in [26], each node is provided with Global Positioning System (GPS). The location of the node is obtained from GPS. From the location information each node can calculate the distance to its neighbor node.

[33] presents an algorithm which finds a single optimal path to transmit an amount of data from source to destination. It calculates the duration of the transmission and present a method to find the amount of energy that each node along the path must have to ensure that the data transmission will take place. It assumes that each node in the network is able to estimate its battery life.

TCP issues

TCP is a connection-oriented protocol that provides efficient flow control and congestion control to ensure reliable data transmission. TCP was originally designed for the wired networks. TCP/IP is the standard networking protocol on the Internet and is also the most widely used. Link failures in Ad-hoc networks are more due to mobility than congestion. TCP is unable to distinguish between losses due to route failures and losses due to congestion. It assumes all the packet losses as a result of congestion in network, and deals with this by adjusting the congestion window size. As a result, the throughput degrades significantly when nodes move.

TCP congestion window size may have a significant impact on the performance of Mobile Ad hoc networks. According to [34], there exists an optimal value of TCP congestion window size for a given network topology and traffic pattern at which the channel can be utilized maximum. However, TCP does not operate at this optimal point but with a larger window size, which results in decreased throughput and increased packet loss. The losses are due to the link layer drops, caused by mobility and interference of other stations. Small congestion window typically provide the best performance [35].

Different approaches have been used for TCP optimizations including the MANET issues and adaptation of TCP error-detection and recovery strategies in the ad hoc environment. In [34], the intermediate nodes upon detection of link failure, notify the sender TCP about the route failure and route reestablishment. Thus, TCP after a link failure does not activate its congestion window mechanism, rather freezes its status to resume later when a new route is found. This method minimizes the impact of mobility and link failure on TCP performance.

V. MULTICAST ROUTING

Multicast is an efficient way to distribute information from single source to multiple destination or many-to-many in communication networks [27]. Multicast protocols used in static networks (e.g. Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Core Based Trees (CBT), and Protocol Independent Multicast (PIM)) do not perform well in wireless ad hoc networks because multicast tree structures are fragile and must be readjusted as connectivity changes [28]. Mobile ad hoc network needs special multicast routing protocol to adopt its characteristics including local broadcast capacity, arbitrary topology change, and bandwidth constraint and power limitation.

[27] proposes a routing protocol called Adaptive Core-based Multicast Routing Protocol (ACMP) which constructs and maintains a group shared tree using adaptively selected core only when group traffic exists. ACMP reacts to broken tree edge by detecting link failures during data forwarding. Once a link failure is detected, this protocol uses local route discovery to establish a temporary route and periodical tree refreshing to maintain an optimal multicast tree.

The Reservation-Based Multicast (RBM) routing protocol [29] builds a core (or a Rendezvous Point) based tree for each multicast group. RBM is a combination of multicast, resource reservation and admission control protocol where users specify requirements and constraints.

Another protocol Lightweight Adaptive Multicast (LAM) algorithm [30] is a group shared tree protocol that does not require timer-based messaging. Similar to other core-based protocols, it suffers from disadvantages of traffic concentration and vulnerability of the core.

[31] presents another multicast protocol Ad-Hoc Multicast Routing Protocol utilizing Increasing id-numbers (AMRIS),

which builds a shared tree to deliver multicast data. Each node in the multicast session is assigned an ID number and it adapts to connectivity changes by utilizing the ID numbers.

The On-Demand Multicast Routing Protocol (ODMRP) [28] is a mesh-based, multicast protocol that provides richer connectivity. To establish a mesh for each multicast group, ODMRP uses the concept of forwarding group. The forwarding group is a set of nodes responsible for forwarding multicast data on shortest paths between any member pairs.

The Core-Assisted Mesh Protocol (CAMP) [32] generalizes the notion of core-based trees introduced for multicasting into multicast meshes. A shared multicast mesh is defined for each multicast group. CAMP consists of the maintenance of multicast meshes and loop-free packet forwarding over such meshes. Within the multicast mesh of a group, packets from any sources in the group are forwarded along the reverse shortest path to the source, just as in traditional multicast protocols based on source-based trees.

VI. ROUTING IN UNIDIRECTIONAL LINK

A unidirectional link arises between a pair of nodes in a network when only one of the two nodes can directly communicate with the other node [26]. Links may be unidirectional due to *hidden terminal problem* or due to difference in the transmission power of the nodes at either ends of a link. Routing using unidirectional links is complex and entails high overheads [26]. Main difficulty comes from the asymmetric knowledge about a unidirectional link at its end nodes. Dynamic Source Routing (DSR) requires two route discoveries to discover unidirectional paths- one from the source and other from the destination, as opposed to a single route discovery to find bi-directional links. [26] Presents and evaluate three techniques to improve basic AODV performance in networks with unidirectional links.

VII. CONLUSION AND FUTURE WORK

In this paper we have presented various MANET routing strategies and different work done in these areas. It discusses a wide range of research issue on routing generated by the challenges faced by the Mobile Ad hoc Networks. We have discussed in detail five different ways of routing namely: Position based Routing, Secure Routing, QoS aware Routing, Multicast Routing and Routing in Unidirectional Links, which would provide a good means for further exploring and modifying the different strategies and protocols studied. The different strategies could be combined to achieve an efficient algorithm to overcome the challenges still suffered by MANETs and improve the performance.

REFERENCES

1. S. Sesay, Z. Yang and J. He, “A survey on Mobile Ad Hoc Wireless Network”, Information Technology Journal 3 (2): 168-175, Asian Network for Scientific Information, 2004.

2. Mauve, M., Widmer, J., and Hartenstein, H., “A Survey on Position-Based Routing in Mobile Ad-Hoc Networks”, Network Laboratories, NEC Europe ltd. Heidelberg, Germany, Carried out within the framework of the ‘FleeNet’ project as part of BMBF contract no. 01AK025D.

3. Young-Bae Ko and Nitin H. Vaidya, “Location-Aided Routing (LAR) in mobile ad hoc networks”, Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA.

4. S. Basagni, I. Chlamatac, V. Syrotiuk, and B. Woodward, “A Distance Routing Effect Algorithm for Mobility (DREAM)”, In proc. of the 4th annual ACM/IEEE int. Conf.on mobile computing and networking (MOBICOM) ’98, pages 76-84, Dallas, TX, USA,1998.

5. Wen-Hwa Liao, Yu-Chee Tseng, and Jang-Ping Sheu, “GRID: A Fully Location Aware Routing Protocol for Mobile Ad Hoc Networks”, Department of computer science and Information Engineering, National Central University, Taiwan.

6. A. Zafar, A. Iqbal and S. Lehri, “Mobile Ad-Hoc Network – A Research Perspective” in the proceeding of National Conference INDIACom-2012, February 23-24, 2012.

7. S. Marti, T.J. Guili, K. Lai, M. Baker, “Mitigating Routing Misbehavior in Mobile Ad hoc Networks”, 6th MobiCom, BA Massachusetts, Aug. 2000.

8. L.Buttyan and J.P. Hubaux, “Enforcing service Availability in Mobile Ad hoc WANs,” 1st MobiHoc, BA Massachusetts, Aug.2000.

9. P. Papadimitrators and Z.J. Haas, “ Secure Message Transmission in Mobile Ad hoc Networks,” submitted for publication.

10. Manel Guerrero, “Secure Ad hoc on-demand distance vector (SAODV) routing, INTERNET DRAFT draft-guerrero-manet-saodv-00.txt, August 2001.

11. Yin-Chun Hu, David B. Johnson, Adrian Perrig, "SEAD : Secure Efficient Ad hoc Distance vector routing for mobile wireless ad hoc networks", Ad Hoc Networks 1 175-192, 2003.

12. Yi-an Huang, Wei Fan Wenke Lee Philip S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies".

13. P. Papadimitrators, Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in proc. of the IEEE Workshop on Security and Assurance in Ad Hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, January 28,2003.

14. Marilia Curado, Edmundo Monteiro, "A Survey of QoS Routing Algorithms", International Journal of Information Technology Volume I Number I ISSN:1305-239X, 1999.

15. Special issue on Wireless ad hoc networks, IEEE JSAC, Aug.1999

16. Shigang Chen, Klara Nahrstedt, "An overview of Quality of Service routing for Next generation High-Speed Networks: Problems and Solutions", IEEE 1998.

17. W.H. Liao, Y.C. Tseng, S.L. Wang, and K.P. Shih. "A TDMA-based bandwidth reservation protocol for QoS routing in wireless mobile ad hoc network," Communications, ICC 2002.IEEE International Conference on, 5:3186-3190, 2002.

18. W.H. Liao, Y.C. Tseng, S.L. Wang, and J.P. Sheu. "A multi-path QoS routing protocol in a wireless mobile ad hoc network", IEEE International Conference on Networking, 2:158-167, 2001.

19. C. Zhu and M. S. Corson, "A five-phase reservation protocol (FPRP) for mobile ad hoc networks", INFOCOM '98 seventeenth annual joint conference of the IEEE computer and communications societies. Proceedings. IEEE, 1:322-331, 29 March – 2 April 1998.

20. I. Gerasimov and R. Simon. "A bandwidth reservation mechanism for on-demand ad hoc path finding", IEEE/SCS 35th Annual Simulation Symposium.

21. C. R. Lin and M. Gerla. "A distributed control scheme in multi-hop packet radio networks for voice/data traffic support", Communications, 1995. ICC 95 Seattle, Gateway to Globalization, 1995 IEEE Int. Conf. On 2: 1238-1242, June 1995.

22. S.T Sheu and T.F. Sheu, "Dbase: a distributed bandwidth allocation/sharing /extension protocol for multimedia over IEEE 802.11 ad hoc wireless LAN. INFOCOM2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 3:1558-1567, April 2001.

23. J. Wang, Y. Tang, S. Deng, and J. Chen, "QoS routing with mobility prediction in manet", Communications. Computers and Signal Processing, 2001. PACRIM. 2001 IEEE Pacific Rim Conference on, 2:357-360, August 2001.

24. Shigang Chen and Klara Nahrstedt, "Distributed Quality-of-Service in Ad Hoc Networks." In IEEE Journal on selected areas in communication, vol. 17, no.8, August 1999.

25. V. Sumathy, Dr. P. Narayanasamy, J. Jaywin James, S. Kanimozhi, "Throughput Maximization Routing in Mobile Ad-Hoc Network by Link Break Prediction", Academic Open Internet Journal, Volume 16, 2005.

26. Mahesh K. Marina, Sameer R. Das, "Routing performance in the presence of Unidirectional Links in Multihop Wireless Networks.", MOBIHOC'02, June 9-11, EPFL Lausanne, Switzerland 2002.

27. R. Prakash, "A routing algorithm for Wireless Ad Hoc Networks with Unidirectional Links", Wireless Networks 7, 617-625, supported in part by the NSF grants CCR-9796331 and ANI-9805133, 2001

28. Sung-Ju Lee, William Su and Mario Gerla, "On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks", Mobile Networks and Applications 7,441-453, 2002.

29. M.S. Corson and S.G. Batsell, "A Reservation-based Multicast (RBM) routing protocol for mobile networks: Initial Route construction phase", wireless Networks 1(4), 427-450, December 1995.

30. L. Ji and M.S. Corson, "A lightweight adaptive multicast algorithm", in proceedings of IEEE GLOBECOM'98, Sydney, Australia, pp.1036-1042, Nov.1998.

31. C. W. Wu, Y.C. Tay and C.-K. Toh, "Ad hoc Multicast Routing protocol utilizing Increasing id-

numberS (AMRIS) functional specification", Internet Draft, Work in progress, draft-ietf-manet-amris-spec-00.txt, November 1998.

32. J.Garcia-Luna-Aceves and Ewerton L. Madruga, "The core-assisted mesh protocol", IEEE Journal on Selected Areas in Communications 17(8), 1380-1394, August 1999

33. S. Tragoudas and S. Dimitrova, "Routing with Energy Considerations in Mobile Ad-Hoc Networks", supported in part by the NSF grant CCR-0096119.

34. Zhenghua, F., Z. Petros, X. Kaixin, L. Haiyun, L. Songwu, Z. Lixia and G. Mario, "The impact of multihop wireless channel on tcp throughput and loss", In Proceedings of INFOCOM 2003. San Francisco, April 2003.

35. Tang, K. and M. Gerla,. "Fair sharing of MAC under TCP in wireless ad hoc networks", In Proceedings of IEEE MMT_99, Venice (I), October, 1999. ad hoc routing algorithms (TIARA). In Proceedings of MILCOM,1999.

36. Yih-chun hu, Adrian Perrig and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks 11, 21–38, 2005.

37. L Chen, WB Heinzelman, "QoS-Aware routing based on Bandwidth Estimation for Mobile Ad Hoc Networks", Journal on Selected Areas in Communications, IEEE, 2005.