# DESIGN AND PERFORMANCE EVALUATION OF A FUZZY LOGIC CONTROLLED CHEAT-PROOF ADAPTIVE DEMAND-DRIVEN ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS (MANET)

Anuradha Banerjee
Lecturer, Department of Computer Applications
Kalyani Government Engineering College
Dist. – Nadia
West Bengal
PIN – 741235

**SUPERVISOR:**

Dr. Paramartha Dutta
Professor & Head, Department of Computer Science and Engineering
Kalyani Government Engineering College
Dist. – Nadia
West Bengal
PIN – 741235

Submitted to the West Bengal University of Technology for partial fulfillment of the requirements for the degree of philosophy

August 2007

**Background of the study:**

Mobile ad hoc networks (MANETs) belong to the class of infrastructure-less networks, which do not require the support of wired access points for intercommunication. It is dynamically re-configurable i.e. very flexible in topology structure and suitable for applications like battlefield communication, disaster recovery, coordinated task scheduling, vehicular communication for traffic management, data and information sharing in difficult terrain. Due to limited radio propagation range, nodes of a MANET communicate through either single-hop or multi-hop transmissions. Each node acts as both wireless host and router. On account of random node dynamics in ad hoc networks, design of a suitable algorithm has become a key problem.

Our present initiative relates to one such area. The author has tried to convert nodes to fuzzy controlled intelligent systems capable of

i) selecting the near optimal route between any arbitrary pair of source and destination nodes
ii) geocasting and multicasting with excellent accuracy of delivery at reduced and/or restricted message cost
iii) enforcing cooperation among themselves

The proposed thesis has also considered issues like protocol control overhead and its robustness, limited use of resources (bandwidth, energy etc.) and network scalability. Performance of each of the proposed communication algorithms have been extensively studied and supported by rigorous mathematical analysis. Below is presented a small survey of literature regarding existing proactive and reactive routing protocols, detection and treatment of selfish and malicious nodes, techniques of multicasting and geocasting.

i) Proactive and Reactive Routing Protocols

Proactive routing protocols such as DSDV (destination-sequenced distance vector), WRP (wireless routing protocol), GSR (global state routing), STAR (source-tree adaptive routing), CGSR (cluster-head gateway switch routing) and reactive routing protocols like AODV (ad-hoc on-demand distance vector routing), DSR (dynamic source routing), ROAM (routing on-demand acyclic multi-path), LMR (light-weight mobile routing) etc. are some noteworthy communication protocols available in literatures on ad hoc networks [1,2,3,6,7,8,9,12]. In proactive routing protocols, each node maintains routing information to every other node in the network. Routing information is kept in different tables, which are periodically updated with the change in network topology. The proactive routing protocols differ by the procedure of storing routing information in tables. These protocols suffer from extremely huge storage overhead and often criticized as power inefficient, since thy exchange messages even when there is  no traffic. On the other hand, reactive routing is widely regarded as the technique of choice for ad hoc networks. All of them rely on some form of flooding to identify paths on-demand [3,8]. Since, identification of optimal route by available proactive and reactive routing protocols is based on hop count or number of intermediate nodes, frequent flooding sessions may need to be initiated during route discovery. This worsens the network throughput by increasing packet collision and transmission delay [9,10,11,15]. It has been demonstrated in references with nos. 11,13, 14 and 15 that use of flooding for route establishment causes salability problems in large networks with many active connections.

### ii) Detection and Treatment of Selfish / Malicious Nodes

Marti. Et. Al. [16] proposed a reputation based method which considers uncooperative nodes in general, including selfish and malicious nodes. In order to cope with this problem, they proposed two tools; a watchdog, which identifies misbehaving nodes and a pathrater which selects routes avoiding misbehaving nodes. Buchegger and Le Boudec proposed and evaluated their CONFIDANT [17,18] protocol, which detects and isolates misbehaving nodes. However, there are several issues that these systems need to address. They have not presented any formal specification and analysis of the type of incentive provided by such systems. They have not considered the possibility that selfish nodes can collude with each other in order to maximize their welfare. Buttyan and Hubaux proposed a stimulation approach based on virtual currency, called nuglets [20], the authors proposed two payment models: the Packet Purse Model and Packet Trade Model. In Packet Purse Model, the sender of a packet pays by loading some nuglets in the packet before sending it. Intermediate nodes require some nuglets from the packet when they forward it. If the packet runs out of nuglets, then it is dropped. In the Packet Trade Model, each intermediate node buys a packet from its previous nodes for some nuglets and sells it to the next node for more nuglets. Ultimately, destination of a packet pays for the packet. To implement these models, a tamper-proof hardware is required at each node to ensure that the correct amount of nuglets is deducted or credited at each node.

### iii) Multicasting and Geocasting

Little work has been done in the area of multicast routing in ad hoc networks. The only current research effort in the field is the Shared-Tree Wireless Network Multicast (ST-WNM) [13] algorithm. The ST-WNM approach is based on adapting sparse-mode algorithms to ad hoc networks. Since fixed network multicast routing is based on state in routers (either hard or soft), it is fundamentally unsuitable for ad hoc network environment with unconstrained mobility. This is confirmed by ST-WNMs own simulation results, which show that the performance of both hard and soft-state multicast tree maintenance mechanisms degrade rapidly with increased mobility. Host mobility was simulated by having hosts roam randomly with a preset average speed.

Navas and Imielinski [21] suggested three methods for geographically targeted advertising geo-routing with location-aware routers, geo-multicasting modifying IP multicast and an application layer solution using extended Domain Name Services (DNS). Young-Bae-Ko and Nitin. H. Vaidya [15] proposed two geocast algorithms (location based multicast schemes 1 and 2) which attempt to reduce the forwarding space for multicast packets. Limiting the forwarding space definitely results in fewer geocast messages although it fails to produce significant improvement in success rate of delivery.

**Plan of work:**

Communication in ad hoc networks is either single hop or multi-hop. In single hop communication, the destination node is within the radio-range of the source and there is no problem in communication. Various intermediate nodes or routers need to bridge the gap between source and destination node if the destination node is not within the radio-range of source node. The wireless connectivity between the source and first router, first and second router, second and third router … , last router and the destination, should be strong enough so that they can survive until the end of the communication session irrespective of the mobility of nodes in the route. The main two challenges to survival of a route are the residual energy and velocity of the nodes. If the relative velocity between every two consecutive node in a route, is small and the residual energy of the nodes is high, then the route is expected to live long. If any link from node $n_i$ to node $n_j$ in an established route breaks, then in order to repair the broken link, a lot more route_request packets need to be injected into the network to discover route from $n_i$ to any node between $n_j$ and the destination. These route_request packets are flooded into the network resulting in huge message cost. These route_requests need to be forwarded by all the nodes that have received it and are less than H hops away from $n_i$ where H is maximum allowable hop count in the network. The message forwarding activity consumes energy of nodes and drives them to speedy exhaustion of battery reducing their lifetime. Complete exhaustion of battery of certain nodes may hamper network connectivity in some situations. For example, let there be only one connection between the uplink and downlink neighbourhood of a node $n_i$ and the connection is through $n_i$ only. So if the battery of $n_i$ becomes completely unable to operate then the network will be partitioned. In one partition there will be the uplink neighbours of $n_i$ whereas in the other partition there will be it's downlink neighbours. Increased message overhead also causes signal collision reducing the data packet delivery ratio. Moreover the delay in completion of communication also increases due to the additional time required for repairing the broken links. So, the main purpose of the thesis is to decrease the message overhead of the system by incorporating stability in the links as much as possible.

In the literature of ad hoc network, there exists some techniques for identifying stable links during unicast operations among all other available options but the approach presented in the thesis is much more rigorous and effective. Not only unicast, but also for multicast, broadcast and geocast efficient protocols have been presented along with a detailed evaluation of performance with respect to total number of nodes in the network and maximum node speed. For improving scalability of the system, binary search based efficient location discovery techniques have been proposed for tracking destination. Also a multi-hop clustering scheme is designed to properly organize the nodes into a structure as much stable as possible. It may be noted that the multi-hop communication in ad hoc networks is completely based on the selfless message forwarding service of nodes. It is the interest of every node to save its own energy whereas forwarding messages of others requires consumption of a node's energy for the network's interest. These two conflicts each other and nodes tend to be selfish. They may choose not to forward the packets of others and simply drop them. This also results in link breakage for repairing which more route_requests are injected into the network increasing the message overhead once again. Along with the selfish nodes there may be some malicious nodes that try to cause harm to the system even at the cost of their battery power. The techniques followed by them are intentional packet drop or link breakage attack, deliberately delaying the network traffic, injecting enormous traffic, slander and masking attack. For running the network operations smoothly, the thesis proposes a method that encourages the nodes to behave honestly and selflessly. Malicious nodes are blacklisted network-wide as soon as they are caught red-handed. This threatens the malicious nodes so that they refrain from causing harm to the network. Overall, the present thesis may be considered as an all-round approach to unicast, multicast, broadcast and geocast communications in a scalable clustered mobile ad hoc network environment consisting of selfish and malicious nodes.

In almost every chapter of the thesis (except chapter 2), the behaviour of the nodes with respect to the communication problem tackled in the chapter (clustering in chapter 3, unicasting in chapter 4, multicasting in chapter 5, broadcasting in chapter 6, geocasting in chapter 7 and selfish and malicious node detection in chapter 8), is expressed in the form of if-then rules. Then they are mapped to rule bases of fuzzy controllers depending upon their comparative strength in solving the corresponding problem. The reason behind proposing fuzzy logic based solution is that if-then rules are the basic unit of fuzzy function approximation. Advantages of fuzzy logic are that it is flexible, conceptually easy to understand and based on natural language. Moreover, it is tolerant of imprecise data and can model non-linear functions of arbitrary complexity. All these encouraged me to propose fuzzy-logic based solution to the problem of node tracking and communication in ad hoc networks.

## **Chapter – 1 : Survey of Various Routing protocols**

In this chapter, a detailed discussion is provided on different categories of routing protocols in ad hoc networks. The classification of unicast routing protocols are typically proactive and reactive routing protocols, zone-based hierarchical routing protocols, cluster-based routing protocols, core-node based routing protocols, power-aware and link stability based routing protocols. Then there are discussions on multicast, broadcast and geocast algorithms along with the clustering and scalability techniques along with the methods for selfish and malicious activity detection.

## **Chapter – 2 : Binary location Search (BinLS) Based Scalable Method For Tracking Destination**

In chapter 2, a binary location search based scalable routing is proposed. It divides the network into some equal sized rectangular grid cells. Each node is assigned a home grid cell from where it starts its activity. The home grid cell is decided on the basis of a hash function on the node identifier. Nodes on the periphery of each grid cell store information about all nodes present in the cell. Whenever a node $n_s$ (source) tries to communicate with another node $n_d$ (destination), $n_s$ computes home grid cell of the destination by applying a hash function on $n_d$. If $n_d$ is not found in the grid cell specified by its home grid cell, BinLS applies an intelligent binary search technique to locate it. In order to reduce message cost in the network, BinLS utilizes the information about most recent previous location of the destination. Depending upon this information, all possible grid cells within which the destination node may reside at the current timestamp is computed. Then any peripheral node of those grid cells is asked about the clusterhead that presently contains the destination. The peripheral node redirects the query to its own clusterhead if it is not a clusterhead itself. Clusterhead of the peripheral node checks to see whether the destination node is a member of its cluster. If it is, then the clusterhead replies with the present location of the destination, otherwise it forwards the query to its neighbour clusterheads within the same grid cell. The neighbour clusterheads also repeat the same procedure. Here it must be mentioned that isolated nodes are also treated as clusterheads. As soon as the destination is tracked, then its present geographical position in terms of latitude and longitude is sent back to that peripheral node which forwards it to the source. If the peripheral node is a clusterhead then it processes the query on its own in the same way. This decreases the area of the geographical region within which the route_request packet is to be broadcasted into the network. Hence the message cost is reduced increasing data packet delivery ratio and decreasing the time required for tracking a destination node.

## Chapter – 3 : Fuzzy Controlled Multi-hop Adaptive Clustering (FMAC)

In chapter 3, a fuzzy controlled multi-hop clustering technique is proposed. It efficiently incorporates stability during formation of clusters. A stable cluster is formed if its clusterhead is capable of continuing as clusterhead for a substantially long time and the routes from the clusterhead to the cluster members are stable. The pre-requisites for longevity of a clusterhead are high residual energy, low rate of energy depletion, strong wireless bond with downlink neighbours which are also members of the cluster and high radio-range. Measuring the strength of a wireless bond is very important from the perspective of ad hoc networks because of its inherent uncertainty and arbitrary dynamism. There are several factors that affect the

A considerable part of the thesis is particularly directed towards incorporating intellect in behavior of mobile ad hoc network elements (nodes). Range specification of fuzzy variables along with fuzzy rule bases are embedded in each and every node for this purpose. Performance of individual hops as estimated by intermediate nodes or routers, contribute to determination of acceptability of the path solution by the goal node, as per the proposed fuzzy inference engines.

The first chapter of the proposed thesis is expected to contain introduction along with a review of the related literature. In chapter 2, the author tries to rigorously formulate the criteria of stability and agility of a path solution and its effectiveness in the present scenario of network congestion and remaining battery life of source and destination nodes. Characteristics of parameters of those criteria are precisely investigated and dynamically mapped to fuzzy premise variables (depending upon other competitor solutions), as their influence over performance of a communication link is non-specific by default. Minimization of transmission delay should be treated with utmost importance if at least one of the sender or receiver is on the verge of complete exhaustion; on the other hand, the criteria of durability dominates as longevity of both of them increase. This gives rise to the concept of pareto-optimal solutions, on occasions when these objectives conflict with one another. It justifies formulation of the problem as a multi-objective optimization construct. Unique credit points are assigned to routes by the destination and the solution with highest credit point is picked up for the entire session. Elegance of the proposed protocol is that, it completely outperforms existing proactive, reactive and hybrid routing protocols. Empirical findings presented in this chapter firmly establish that our demand adaptive fuzzy controller (DAFC) significantly improves network throughput, even when the network is highly congested. Also the message overhead and transmission delay are greatly reduced in DAFC.

Hardware design of both stability and agility component controllers of DAFC consists of two parts:

i) hierarchical sequential magnitude comparator (HSMC)
ii) combinational circuits with D flip flop gateways

HSMC determines fuzzy premise variable corresponding to a crisp input, whereas rule bases are modeled by combinational circuits. Detailed explanation of operation of these circuits successfully conclude our discussion on DAFC, in this chapter.

Apart from multicast flooding, two location based multicast schemes [15] proposed by Young-Bae-Ko and Nitin. H. Vaidya, are noteworthy geocast algorithms reported in literature on MANETs so far. In chapter 3 of the thesis the author concentrates on identification of shortcomings inherent in these schemes and proposes a fuzzy controlled adaptive geocast communication scheme that promises maximum success of message delivery at minimum cost. The adaptive procedure ensures that, all nodes belonging to the geocast region at the time of initiation of some geocast transmission, will at least receive the notification that they are members of a geocast group(s) with respective identification numbers and in order to receive the multicast message, they are advised to stay within a logically (in fuzzy sense) specified bounded geographical region, very negligible in size compared to the network area traversed during flooding, for a predefined time period. The region is termed as AC (accuracy control) zone and its shape and size are computed on a per packet basis. Numerical results section of this chapter, strongly support the merit of the adaptive geocast communication scheme in comparison to existing multicast flooding and location based multicast schemes proposed in reference 15.

Chapter 4 is dedicated to the issue of multicast routing in ad hoc networks. The only current research effort, to the best of my knowledge, reported in this field is “shared tree wireless networks multicast (ST-WNM)”, which is based on adapting sparse mode algorithms of fixed infrastructure networks to MANETs. Since fixed network multicast routing is based on the state in routers (hard / soft), it is fundamentally unsuitable for a MANET environment with unconstrained mobility. This is confirmed by ST-WNM’s own simulation results, which show that performance of both hard-and-soft state multicast tree maintenance mechanism degrade rapidly with increased mobility.

We present an algorithm which is based on the idea that, a MANET comprising of a large number of hosts spanning huge geographical areas, would lend itself to some kind of hierarchy. This is especially applicable to military scenarios, which are inherently hierarchical. It generates the idea of partitioning a MANET into clusters ensuring the following characteristics:

i) A cluster is still a multi-hop MANET
ii) Intra-cluster mobility is arbitrary but inter-cluster migration are relatively less likely
iii) Each cluster elects a cluster head by a fuzzy logic oriented procedure
iv) Intra-cluster multicast is performed with hyper-flooding
v) Inter-cluster multicast is accomplished by adaptive geocasting among cluster heads. Cluster heads maintain state information regarding multicast group membership of their constituent hosts

Like earlier chapters, hard core simulation results have been tabulated and graphically interpreted to confirm the elegance of our fuzzy cluster-based multicast routing algorithm.

For any ad hoc communication protocol to be a success, each and every node needs to be cooperative enough to selflessly forward others messages. Since forwarding a message will incur cost (of energy, bandwidth etc.) a selfish or economically rational node, whose sole objective is to maximize its own welfare (benefit-cost of actions), will need incentive in order to act as a router for others. The incentive scheme that the author has used in chapter 5, is a reputation based scheme. A vulnerability fuzzy controller (VFC) has been embedded in each network element so that it can distinguish between intentional misbehavior and indispensable selfishness due to acute energy scarcity. The controller is intelligent enough that it does not depend on broadcast nature of wireless networks in order to monitor other nodes. Furthermore, this potential of VFC is necessary and sufficient in the current era of directional antennas and asymmetric links when nodes are capable of using power control. Another novel feature of this proposed reputation based mechanism is that it does not need any tamper-proof hardware. Each node is motivated to report its actions honestly, even when a collection of selfish nodes collude. A dishonest node is penalized by its neighbors through the process of blocking its calls for a pre-calculated time period. The author has structured the system with a simulation solution with formal proofs of correctness under the model of game theory. The algorithm has been tested under situations like message forwarding in both unicast, multicast transmissions and route discovery. Evaluations of a prototype implementation prove that overhead of the system is small compared to other reputation based approaches like i) watchdog by Marti. Et. Al. [16] ii) CONFIDANT by Buchegger and Le Boudec [18] and credit based fairness monitoring systems like i) nuglet based simulation by Buttyan and Hubaux [20] ii) Sprite by Zhong, Chen and Yang [14]. The chapter concludes by claiming that cooperation is the best policy for nodes as far as our system is concerned, irrespective of the detection of misbehavior, unless the resource pool of each node is extremely poor.

Chapter 6 is devoted to the use of dynamic addressing to enable scalable routing in ad hoc networks. It is well known that the current proactive, reactive and hybrid routing protocol suites do not scale to work efficiently in networks of more than a few thousands nodes. All of these protocols rely on some form of flooding for route establishments which cause scalability problems in large networks with many active connections. In this chapter, the author provides design of a routing layer based on dynamic addressing and evaluate its performance. Each node is assigned a unique permanent identifier and a transient routing address which indicates its location in the network at a given time. In brief, the mechanism to efficiently implement dynamic addressing is described here.

When a node joins the network, it listens to periodic routing updates of its neighboring nodes and uses these to identify the next unoccupied address. The joining node registers its unique identifier and newly obtained address in the distributed node lookup table. Due to mobility, the address may subsequently change and then the lookup table needs to be updated. Selection of a node for storage of the lookup table is made based on fuzzy logic again. When a node wants to send message packets to a node known only by it's identifier, it will use the lookup table to find its current address based as a function of geographical location. Once the destination address is known, the routing function takes care of rest of the communication.

Set of achievements of the proposed solution are:

i) localization of overhead – a local change affects only the immediate neighborhood, limiting the overhead incurred due to those changes or updates
ii) lightweight, decentralized protocol – concentrating responsibility at any single node has been avoided
iii) zero configuration – complete removal of the need for manual configuration beyond what can be done at the time of manufacture

Chapter 7 is primarily dedicated to drawing a overall conclusion and presenting future scope in the relevant areas of investigation on mobile ad hoc networks.

References:


[1] S. Ramanathan and M. Streenstrup, " A survey of routing techniques for mobile communications networks", ACM / Baltzer MANET, October 1996
[2] C. Perkins, "Ad hoc on-demand distance vector routing" , MobiHoc 1997
[3] Charles Perkins and Pravin Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", ACM SIGCOMM'94
[4] Yih-Chun.Hu, David B. Johnson and Adrian Perrig, "Sead: Secure efficient distance vector routing in wireless ad hoc networks", in Fourth IEEE workshop on Mobile Computing Systems and Applications, June 2002
[5] Yih-Chun.Hu, David B. Johnson and Adrian Perrig, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in proceedings of Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)
[6] A. Banerjee, K. Mondal, P. Dutta, K. Mazumder, "Implementation of mobile ad hoc network using statistical models", BIG-2004,Calcutta
[7] A. Banerjee, K. Mondal, P. Dutta, K. Mazumder, "MANET as a finite-state machine", MobicomNet – 2004
[8] D. Grune "A text book on MANET", Pearson Education
[9] S. Karthikeyan & P. Chandra, "Modified AODV in mobile ad hoc networks", in Workshop on Distributed System, JU-1991, Calcutta
[10] A. Banerjee, P. Dutta, "Fuzzy-controlled intelligent tracking and communication in a mobile environment", proceedings of the International Conference on intelligent Systems (ICIS – 2005) Kualalumpur, Dec 1-3, 2005
[11] A. Banerjee, P. Dutta, "Fuzzy-controlled energy-efficient management of selfish users in mobile ad hoc networks ", proceedings of the IEEE sponsored ICIIS – 2006, Peradeniya, Sri Lanka, August 8-11, 2006

[12] D.B. Johnson and D.A. Maltz "Dynamic source routing in mobile ad hoc networks", Mobile Computing, Chapter 5,Kluwer Academic Publishers, pages 153-181, 1996
[13] C.C. Chiang, M. Gerla and L. Zhang "Shared-tree wireless networks multicast", Proceedings of IEEE Sponsored ICCCN'1997
[14] Sheng Zong. Et. Al., "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks", in Proceedings of IEEE Infocom 2003
[15] Young Bae Ko, Nitin. H. Vaidya, "Location-based multicast schemes 1 & 2", Proceedings of IEEE Infocom 2004
[16] S. Marti, T. Gui LI, K. Lai and M. Bawer "Mitigating routing misbehavior in mobile ad hoc networks", Proceedings of sixth International Conference on Mobile Computing and Networking 2000, Boston
[17] S. Buchegger and L. Boudec, "Nodes bearing grudges: Towards routing security fairness and robustness in mobile ad hoc networks", in 10th Euromicro Workshop on Parallel, Distributed and Network-bsaed processing 2002
[18] S. Buchegger and L. Boudec, "Performance analysis of CONFIDANT protocol: cooperation of nodes – fairness in dynamic ad hoc networks", in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc – June 2002)
[19] J.E. Wieselthier, G.Nguyen, "Energy-limited wireless networking with directional antennas", in Proceedings on IEEE Infocom 2002, New York
[20] M. Jakobsson, J.P. Hubaux and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks", Proceedings of Financial Crypto 2003, La Guadeloupe
[21] J.C. Navas, T. Imielinski "Geocast: geographic addressing and routing", in ACM/IEEE International Conference on Mobile Computing and Networks (MobiCom – 1997)

**Future Application:**

For an ad hoc network to be robust, effective and efficient, it requires a routing protocol (unicast, multicast and broadcast) which will provide maximum possible throughput (successful delivery of packets) at minimum possible time and cost (utilization of resources of network, like battery power of nodes, allotted bandwidth etc.). The present thesis aims at contributing significantly in designing such a communication protocol for MANETs in spite of the provision for inclusion of selfish and malicious nodes.