Topology Control in Cooperative Mobile Ad Hoc Networks

C. Sridevi[1] G. Gayathri[2]
[1]M.Phil Student [2]Assistant Professor
[1,2]Prist University, Thanjavur, India

Abstract— The topology of the network can change randomly due to unpredictable mobility of nodes. This behavior results in certain issues like partitioning, merging, duplicate address detection, security, authenticity, related to IP address allocation to the mobile nodes. Cooperative communication in wireless networks significantly increase transmission reliability and bandwidth efficiency. However, many of the aspects of the cooperative communication layer in this review paper merits further research network topology and network capacity, which aspects, such as physical layer, path, lambAi, etc. is determined by examining its effects on cooperative communications relay network topology and selection effects. physical layer, since we have the potential to directly enhance cooperative communication with a Capacity-Optimized cooperative (Coco) topology control scheme for mobile ad hoc networks (MANETs).Topology control problem is a discrete stochastic optimization problem in MANETs, a stochastic approximation approach can be resolved using as. Moreover, an improved cocoa network topology changing environment to track mobile dynamically presented to reconfigure.

Key words: Topology Control, Network Capacity, Cooperative Communications, MANETs

I. INTRODUCTION

In contrast to infrastructure-based networks, MANET's support autonomous and spontaneous networking and, thus, should be capable of self- organization and self-configuration. An Ad hoc network is a group of mobile and wireless computers which communicate between each participant can, at any moment, act as a router to ensure a communication between two other distant nodes. Those networks are thus based on the cooperation between nodes without the assistance of any infrastructure. MANET applications include supporting battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room, and other security-sensitive computing environments. The ad-hoc networking technology has stimulated substantial research activities in the past years [15].

Before proper routing of data packets in a network, all nodes must be configured with unique IP address. Pre configuring is not possible always as well as it has some drawbacks.

Many issues of research involving large-scale situations for MANETs are deployed for mobile ad- hoc network studies. Researchers, they collect and arrange the literature related to need to spend a lot of time to research issues are presented here and MANET. Aspects of MANETs identified fifteen [15] are grouped into the categories. These issues have the potential to significantly increase survivability MANET

1) Routing

Routing is an essential protocol in this field, because changes in network topology occur frequently.

2) Multicasting Broadcasting

Multicast service supports users communicating with other members in a multicast group. Broadcast service supports users communicating with all members on a network.

3) Location Service

Location information uses the Global Positioning System (GPS) or the network- based geo-location technique to obtain the physical position of a destination.

4) Clustering

Clustering is a method to partition the hosts into several clusters and provide a convenient framework for resource management, routing and virtual circuit support.

5) Mobility Management

In the ad-hoc network environment, mobile hosts can move unrestricted from place to place. Mobility management handles the storage, maintenance and retrieval of the mobile node position information.

6) TCP/ UDP

TCP and UDP are the standard protocols used in the Internet, Data applications running over MANETs, such as http and real audio need transport layer protocols like TCP and UDP to send packets over the links.

7) IP Addressing

One of the most important issues is the set of IP addresses that are assigned to the ad- hoc network. IP addressing and address auto- configuration have attracted much attention in MANETs.

8) Multiple Accesses

A major issue is to develop efficient medium access protocols that optimize spectral reuse, and hence, maximize aggregate channel utilization in MANETs.

9) Radio Interface

Mobile nodes rely on the radio interface or antenna to transmit packets. Packet forwarding or receiving via radio interface or antenna techniques in MANETs are useful investigations.

10) Bandwidth Management

Bandwidth management in MANETs is a typical characterization. Because the bandwidth is usually limited, effectively managing and using it is a very important issue.

11) Power Management

A power management approach would help reducing power consumption and hence prolonging the battery life of mobile nodes. Because most devices operate on batteries, power management becomes an important issue.

12) Security

The mobile nodes in MANETs are highly susceptible to malicious damage. Security issues are important in MANETs to prevent potential attacks, threats and system vulnerabilities.

13) Fault Tolerance

This issue involves detecting and correcting faults when network failures occur. Fault tolerance techniques are

brought in for maintenance when a failure occurs during node movement, joining, or leaving the network.

14) QoS/ Multimedia

Quality of Service (QoS) and Multimedia require high bandwidth, low delay, and high reliability.

15) Standards/ Products

The standards and products issues that allow the development of small scale is emerging for this field. For instance, Bluetooth is a low-cost technology for short-range communications techniques.

Recently, wireless applications, the demand for higher bandwidth and reliability is important in the use of development. The combination of wireless communications such as new technology is in diversity wireless bandwidth and reliability increase. conventional broadcasting information to direct source-destination signal, while cooperative communication [1], [2] to take advantage of user diversity combined signal decoding the source destination signs direct and relayed signals of interest based interpretation from helper to relay to the United Signal noise ratio (SNR) of a better signal non- cooperative communication than you can as a result, this paper at the cooperative we split various methods of brain tumor image review to take goal. We different MRI images Dataset communications now spectral and Riddhi and power efficiency are regarded as a promising approach to network coverage [3] currently at different stages of the method as well, and outage probability [4] are aiming to reduce. Important cooperative Protocol Relay selection techniques [5].

Selection of proper relay transmission rate and can maximize reliability [4]. In particular, the relay selection cooperative communication in MANETs is of significant impact on the network topology. in short, the network topology control determine where to deploy and how to link the link a good network topology as wireless network to work in a certain global graph (i.e. The preservation of the global network connectivity) can optimize performance of a good topology [6], [7]. While there has been extensive research on cooperative communications, physical layer issues, and most existing works such as lower outage probability and outage capacity [4], which are only focusing on link-wide metrics. However, from the point of view of the network, overall network performance, such as a whole may not be enough network capacity. Therefore, cooperative communication ability and many aspects of the upper layer For example, network infrastructure and topology control in mobile ad hoc networks (MANETs), especially the effects on research. In fact, most current study, adapt the MANETs, and traditional simplified to non-wireless link to manage a complex network based on effort.

The upper layer network capacity and physical layer relay selection, this paper a capacity-optimized cooperative (Coco) topology control scheme for cooperative communication with MANETs. Most existing topology control plans assume that wireless channels well. However, in practice, it's a dynamic channel [8] [9] is difficult to have the right knowledge of the meaning, Coco Chanel estimates only. Accordingly, a discrete stochastic optimization problems in topology control MANETs as the problem, and it is a stochastic approximation approach [10] can be solved using-[13], which is to prove the optimal solution by converging iteratively to move towards a better solution analysis and simulation in the paper by the one of the advantages of iterative approach that it dynamically reconfigure the network topology change can track mobile environment. To the best of our knowledge the first topology control scheme for MANETs cocoa cooperative communication with and noise channel with this plan. Choose a network-wide behavior; Riley taking into account network capacity is increased.

II. REVIEW OF DIFFERENT METHODS

Many works have been based on DHCPV6 MANET address auto-configuration, such as dynamic configuration and distribution Protocol (DCDP), basic user registration Protocol (BURP), dynamic mobility agent (DMA), MANET conf, BOleng, Prophet, buddy, CAC, Perkins, HCQC, PACMAN.

[15] In pervasive computing for auto-configuration, registration and dynamics management. To meet the challenges of the future, we must increase that many existing network protocols explained. Here, we auto- configuration, IP layer network enhancements to user registration, And mobility management solutions need to be argued about the types of hosts and nodes of any individual. manual configuration much more dynamic, networked nodes and future network topologies are characterized by a fairly large number is impractical in dynamic configuration Distribution Protocol (DCDP) with automatic IP address and other information to configure large networks presented here quite a while Protocol to enhance the capabilities of future comprehensive network number of additional problems, such as security, still totally needs to be worked.

Unfortunately these processes, often inspired of the traditional wired networks, are not always well adapted to the MANET model and appear relatively resources greedy. Moreover, they apply only to ideal networks in which all nodes can trust each other. In this manner, they do absolutely not consider the security aspects and are thus not adapted to a real use. One of the main threats against the security of MANET routing protocols is the identity usurpation (spoofing). Protocol intended to achieve automatic nodes configuration and addresses authentication. It uses the concept of recursive binary trees to efficiently provide addresses to the nodes and that of inter-certification in order to guarantee the origin of the forwarding packets. It can be used in a complementary way with algorithms especially dedicated to the securization of the routing process.

Auto-Configuration Protocol for traditional networks either stateless or stateful approach can be classified using the DHCP protocol to implement a MANET. With its highly dynamic topology may not break running DHCP that node all nodes reachable by permanently. In contrast, the stateless approach by a protocol using the nodes know and so-called, duplicate address detection (dad) with a distributed manner to confirm its uniqueness. Hybrid protocols combine elements of both approaches performs stateful and stateless. This led to a more robust Protocol, but the high complexity and high protocol overhead can result in two such protocols are presented in the following: HCQA and PACMAN.

A. Partitioning of MANET

The division of a network into two or more sub- networks is known as partitioning. It leads to IP address leak. Partitioning can be of two types: graceful and graceless. If nodes leave after informing their neighbors then it is graceful otherwise graceless. In graceful partition, the newer nodes joining the network can reclaim IP addresses. But graceless partitioning leads to address leakage and there is requirement of some technique to detect it. Figure 1 explains IP address leakage. Before partition there is an only 192.168.1.51 192.168.1.54/24/24 MANET IP address range is split with each consisting of a few IP addresses originating from MANET's range is divided into two independent MANETs. Partition addresses-I Division-II unless it is able to detect this partition is not assigned a new incoming hostile node cannot be assigned. Leads to reduction in the number of IP addresses is a universal identifier for all conf MANET nodes to represent the lowest IP address node "n. MANET identifier has been configured with this designation, only one partition when self ' n (this has been A Division and b). When a new node is ' n m b Daddy is not able to respond to the request so that the initiator of m ' n it does not include the network. The network broadcast message initiator m then to inform split. Therefore, all nodes B to update your address from the list a procedure similar to the B Division address free address nodes. ZAL [6] assumes that partition is always lovely [16].

B. Merging of Several MANETs

The combination of two or more networks merges into a large network. This is what happens when independent networks fall into the category of each other. This IP address conflicts may figure 1 also explains the merger. Division-I, Division-II has its own independent network-I M & class IP address Are using some network nodes merge, but if these nodes to address same as D1 D2 &. To fix this problem, dad is required. A communication begin to exchange their two nodes in MANET conf, identifier if identifiers are different, then they realize their networks merged. Then they were configured as nodes in their network reconfiguration and initiators Act conflicting start with addresses on different sub networks spaces. Were because nothing in the chicken were the only part of larger networks to network be disjoint. Partition ID is used to find out that they belong to the same larger network. If merging networks never met before, ZAL proposes to convert addresses of nodes in smaller networks to that of larger networks. Only addresses in one of the networks can be preserved. The others have to convert. It is a gradual process in which first nodes at the boundaries of smaller networks and then slowly innermost are converted. It is desirable to minimize overhead by minimizing number of address conversions based on distributed algorithms [16].

C. Duplicate Address Detection (DAD)

Dad when either a new node joins a MANET or independent needs a new merge node picks up an interim IP address determines that the dad process. all nodes is a valid IP address is the IP address of their father accidentally new node by sitemap being participate in protecting the uniqueness check send a duplicate address detection. "(DAP) struggles to address a certain timeout period and notice (ACN) is based on the expected." N "If the number of retries, ACN, the node can assume that address Use this process is illustrated in Figure 2, but in the network where the message cannot be bounded delay, timeouts lead to unreliability, there may be duplicate addresses can merge in MANET's case, the several nodes duplicate addresses would increase network overhead to process each node suddenly dad may be due to the beginning of the address automatically. Configuration method as it must treat a particular case.

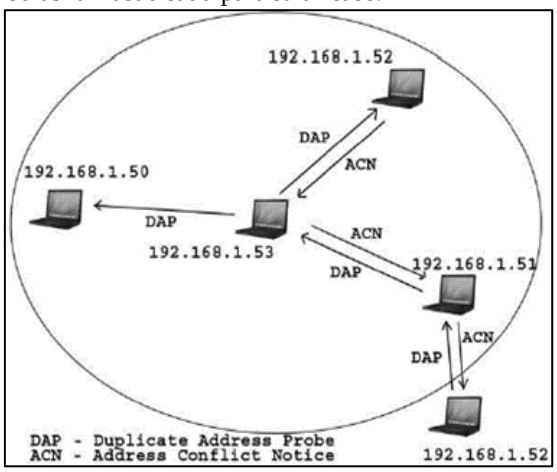

Fig. 1: Duplicate Address Detection Mechanism

Introduces Strong DAD & Weak DAD Strong DAD allows at least one node to detect duplicate immediately after it has been chosen by another node. Practically it is not possible. Weak DAD is based on enhancement of link state routing. Each node of network owns a unique identifier. A node sends control packet indicating its link state along with its identifier each node link state is connected to the corresponding address & identifiers. If a node N receives a control packet from a known address, but with a different identifier, then this is a copycat. "N" duplicates and knows it will keep sending packets for the first node start to announce. MANET Conf is a reliable process is two step dads. Recognition a new node: initiation & (requester) to achieve a preconfigured neighbour (the initiator) to help address the initiator. A requester responds to this request all nodes broadcast. This ensures that the requester of a temporarily disconnected node is not used if a node tries to give an answer after a number of the address was assigned as [16] can be treated.

D. Scalability of Address Auto-Configuration

The number of messages to be sent to the address assigned needs. These messages above the ground with the leading networks nodes overheads can be caused also merge and split. Poor scalability and network paralyze critical address can lead to leaks. [8]One way to identify mobility patterns have been discussed by using these mobility patterns, it ensures the reliability of any service in MANET. Trace a MANET the future partitions to allow the server to include a mechanism at this address auto configuration. Low overhead, which a large number of nodes in the MANET lead with scaling of guarantee can increase even though partition detected a strong centralized approach to use these solutions and their applicability, can be suspected as such. This Division creating a distributed manner in determining likely will be interesting to evaluate the range of IP addresses. When at the same time

e.g. during merge nodes are involved in a large number of IP addresses should not run out of availability.

E. Secure & Authentic Auto Configuration

Security & authenticity in mobile ad hoc networks are hard to achieve due to frequently changing and fully decentralized system. Usage of security system can be dependent upon the application area. Possible address auto configuration attacks are: Address Spoofing attack, a malicious node can operate independently of any one node configured as a victim, his or her IP address hijacking your traffic betray &. A false address conflict victims intentionally attack targeted a wrong address conflict message transmitted. Since victims could not verify the authenticity of the alleged address conflictive up your current address, and to seek a new one. Address exhaustion attack, an attacker maliciously as possible can claim multiple IP addresses if the attacker exhausts all valid IP addresses, a new node will not be able to get an address. Negative responses to attack an aggressor a new persistent configuration node Safe auto configuration use the self-contained authentication to prevent sending negative responses. By using one-way hash function, it binds a node's address with public key. Address owner can use corresponding public key to unilaterally authenticate it, Employs the concept of challenge which obliges a node to answer a question to prove its identity. New node sends a request with its public key and a temporary identifier. Neighbors calculate a nonce that they return to new node, after having ciphered it with the public key. The mission of new node is then to return this nonce incremented to concerned nodes, after having ciphered it with its private key [16].

III. COMPARATIVE STUDY OF METHODS USED IN MANET

A. Network Model

A network topology consists of two aspects: the connection between network nodes and links. in General, a set of network nodes in MANET where □ and □ is set to represent a graph edge wireless link □ (□, □), can be a mapped link in the two nodes usually classical MANETs are in transmission range of each other. This is such a classic MANET topology some controllable parameters the existence of the wireless link directly by defining parameterized. Usually, these parameters may be transmitting power and antenna directions by the introduction of cooperative communication, etc., we consider three MANETs transmission mode: direct broadcasting, broadcasting and multiple-hop cooperative. Live broadcast and broadcasting cooperative communications hop can be considered as a specific type. A direct transmission utilizes no relays while a multi-hop transmission does not combine signals at the destination. Obviously from, it is known that the cooperative channel is a virtual multiple input single outputs (MISO) channel, where spatially distributed nodes are coordinated to form a virtual antenna to emulate multi-antenna transceivers. A cooperative transmission consists of two types of channels: broadcast channel and multiple access channels. The channel time is divided into two orthogonal consecutive slots to implement cooperative transmissions.

Its message relay and the first slot in the source, and the other source and destination slot technology receive signals from relay through multiplexing. As a result, (S, R, D) is presented and the link topology where fiC (V, $\mathcal{E}$ C) C = {(S becomes $\mathcal{E}$, RS, R, D, D) V} ∈ |. Relay broadcasting changed, changed link to performance. Therefore, the relay can be set also wireless link selection criteria for each transmission mode to evaluate the potential for a Raleigh fading channel.

The protocol interference model which confines concurrent transmissions in the vicinity of the transmitter and receiver is adopted in this study. This model fits the medium.

The destination combines the two signals from the source and the relay to decode the information. Access control function well e.g., the popular IEEE 802.11 MAC in most mobile devices in MANETs. Herein, interference of a link is defined as some combination of coverage of nodes involved in the transmission,

Definition 1 (Node coverage). The coverage of a node refers to its neighbors, i.e., Cov (u) = VN (u) for node u. In the physical meaning, it includes nodes covered by this node.

Definition 2 (Link interference). It refers to the number of influenced nodes during the transmission. Topology control Formulation

As topology control is to determine the existence of wireless links subject to network connectivity, the general topology control problem can be expressed as fi∗ = argmax$f$ (fi) or fi∗ = argmin$f$ (fi), (1)

S.t. network connectivity the above topology control problem consists of three elements, which can be formulated by a triple ⟨Æ, ℙ, ®⟩, where Æ represents network model, ℙ represents the desired network property, which often refers to network connectivity for most topology control algorithms, and ® refers to the optimization objective. The problem (1) uses the original network topology fi, which contains mobile nodes and link connections, as the input. According to the objective function, a new good topology fi∗ (V, $\mathcal{E}$∗) will be constructed as the output of the algorithm. fi∗ should contain all mobile nodes in fi, i.e., they have the same node set. The link connections $\mathcal{E}$∗ should preserve network connectivity without partitioning the network. The structure of resulting topology is strongly related to the optimization objective function, which is f (fi) in (1).

MANETs, it is difficult to collect information throughout the network. Therefore, the above centralized topology controls a distributed algorithm, which typically requires only local knowledge, should be resolved using the algorithm on each node independent RS.Triggers option. as a result, each node in the network to all its neighbors only links is responsible for managing all neighbor connections are protected end-to-end connectivity, then a hop by hop manner is guaranteed through a neighborhood graph fiN (VN, $\mathcal{E}$ N), we have a distributed topology can be defined as the control problem

fi∗ N = argmax$f$ (fiN) or fi∗ N = argmin$f$ (fiN), (2)

S.t. connectivity to all the neighbors the objective functions are critical to topology control problems. They may be energy consumption, interference and network capacity, or QoS provisioning under some constraints of delay and bandwidth. They are achieved by adjusting some controllable parameters, such as transmission power, antenna direction,

channel assignment and even cooperation level, which affect the link status.

Energy-saving topology control zone has attracted a great deal of attention. The lack of network connectivity, transmission of each mobile node range adjusts the topology control in order to save energy. NP-hard or NP-complete problems in total power consumption to minimum and maximum power consumption are minimizing it. The researchers adapted to distributed sub MANETs problems which are more practical to solve the complex problem try again. For example, the reference path energy constructs a spanner topology. Some estimated based graph algorithms approach to protected network connectivity while the multiple short hops long link nodes saves energy and prolongs the lifetime network to access remotely. It is generally agreed in the literature that the reduced graph should be sparse to mitigate collisions and packet retransmissions, leading to reduce power consumption and extend network lifetime.

If too many edges are removed from the topology, however, unacceptably long data packets in the way that a multiple-hop wireless network performance increases as the number of hops will degrade faster than a fundamental issue is can a traverse nearest neighbor, which generates a closest neighbor forest, connecting to network interference is not enough to reduce the fact With interference-aware topology control schemes emerge. It assumes that an intervention to reduce network capacity, which is multi-hop, is an important resource for wireless networks can raise the ability a network. In decline as the number of nodes to be revealed to this end, proposed a capacity-aware topology control. It confines the degree of each node in the network to reduce interference and thus increase network capacity. It shares the same principle as interference- aware topology control, but without connectivity guarantee. However, reducing interference merely is not sufficient for network capacity improvement.

Definition 3 (Network capacity). Network capacity refers to the maximum achievable throughput of bits per second for each node on average that can be sent to its destination. The network capacity defined here includes all the end-to end throughput in the network and it is in fact the average throughput capacity per node [16].

B. Objective Function

As an optimization problem, the objective function's paramount component in the objective function network capacity. Coco's status is set to reflect. As concluded, expected network capacity is determined by various factors. On the one hand, one of the main factors link in practice, we have a data rate, outage, which is a little outage probability □, the ability to link to the stand drawing, called supported study shows that the cooperative is not always outperform live broadcast transmission if the cooperative large outage capacity that a relay there exist, we transmit information directly or via multiple hops but. For this reason, the best links and links to optimize the ability to best Relay determines the cocoa. on the other hand, other transmission range Due to the shared wireless nodes open media transmission in order to not disrupt the silent is to be affected include the coverage of the source node (definition 1), destination coverage, as well as the affected nodes, which relayed coverage. Refers, also has a significant impact on network capacity. Higher intervention reduces the simultaneous broadcast network, thus reduces the potential of the network, and vice versa.

C. Direct Transmissions

A direct transmission is the conventional point-to- point transmission. Let y0, y1 and y2 denote the received SNRs from the source to the destination, from the source to the relay and from the relay to the destination, respectively.

D. Multi-Hop Transmissions

The multi-hop transmission here is actually a two-hop transmission. It consumes two time slots. In the first slot, messages are transmitted from the source to the relay and the messages will be forwarded to the destination in the second slot.

E. Cooperative Transmissions

This study uses the fixed decode-and-forward (DF) relaying scheme with only one best relay, which is selected proactively before transmissions.

IV. CONSTRAINTS

At least two constraint conditions are necessarily taken into consideration in the capacity-optimized topology control problem. One is network connectivity, which is also the basic element ℙ in the topology control triple ⟨Æ, ℙ, and ®⟩. Actually, the end-to-end network connectivity is guaranteed via a hop-by-hop manner in the objective function. Every node is in charge of the connections to all its neighbors. If all the neighbor connections are guaranteed, the end-to-end connectivity in the whole network can be preserved [16].

V. CONCLUSION

This review paper auto-configuration IP address a major issue that needs attention from researchers still active. cooperative communications network capacity of MANETs with to improve, we have both the ability and the upper layer network physical layer considers a relay selection Capacity-Optimized sahakAri (Coco) topology control scheme only a discrete stochastic approximation approach proposed is imperfect channel knowledge is available when topology control to resolve the issue was presented. simulation results that cooperative communication techniques is significant impact on network capacity, and Coco is an efficient algorithm with cooperative communications and MANETs are shown well.

REFERENCES

[1] Nosratinia T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," IEEE Commun. Mag., vol. 42, no. 10, pp. 74-80, 2004.
[2] L. Cottatellucci X. Master, E. G. Larsson, and A. Ribera, "Cooperative communications in wireless networks," EURASIP J. Wireless Commun. Newt. vol. 2009, 2009.
[3] Scaglione and Y. Hong, "Opportunistic large arrays: cooperative transmission in wireless multichip ad hoc networks to reach far distances," IEEE Trans. Signal Process., vol. 51, no. 8, pp. 2082-2092, 2003.

[4] K. Woradit, T. Quek, W. Suwansantisuk, M. Win, L. Wuttisittikulkij, and H. Wymeersch, "Outage behavior of selective relaying schemes," IEEE Trans. Wireless Commun., vol. 8, no. 8, pp. 3890-3895, 2009.
[5] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062-3080, 2004.
[6] R. Rajaraman, "Topology control and routing in ad hoc networks: a survey," SIGACT News, vol. 33, no. 2, pp. 60- 73, 2002.
[7] P. Santi, "Topology control in wireless ad hoc and sensor networks," ACM Compute. Surveys, vol. 37, no. 2, pp. 164- 194, 2005.
[8] H. Meyr, M. Moeneclaey, and S. Fechtel, Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing. John Wiley & Sons, Inc., 1997.
[9] L. Tong, B. Sadler, and M. Dong, "Pilot-assisted wireless transmissions: general model, design criteria, and signal processing," IEEE Signal Process. Mag., vol. 21, no. 6, pp. 12-25, 2004.
[10] H. Kushner, "Stochastic approximation: a survey," Wiley Interdisciplinary Reviews: Computational Statistics, vol. 2, no. 1, pp. 87-96, 2010.
[11] S. Andrad otter, accelerating the convergence of random search methods for discrete stochastic optimization ACM Trans. Model. Compute. Simul., vol. 9, no. 4, pp. 349-380, 1999.
[12] Berenguer, X. Wang, and V. Krishnamurthy, "Adaptive MIMO antenna selection via discrete stochastic optimization," IEEE Trans. Signal Process. vol. 53, no. 11, pp. 4315-4329, 2005.
[13] Krishnamurthy and S. Chung, "Large-scale dynamical models and estimation for permeation in biological membrane ion channels," Proc. IEEE, vol. 95, no. 5, pp. 853-880, 2007.
[14] P. Gupta and P. Kumar, "The capacity of wireless networks," IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 388- 404, 2000.
[15] Jagrati Nagdiya, Shweta Yadav, Study of Various IP Auto- configuration Techniques, International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013
[16] Harish Kumar, R.K. Singla, Siddharth Malhotra, Issues & Trends in Auto Configuration of IP Address in MANET
[17] M. Burkhart, P. von Rickenbach, R. Wattenhofer, and A. Zollinger, "Does topology control reduce interference?" in Proc. 5th ACM Int. Symp. Mobile Ad Hoc Newt. Compute. May 2004.
[18] E. Lloyd, R. Liu, M. Marathe, R. Ramanathan, and S. Ravi, "Algorithmic aspects of topology control problems for ad hoc networks," Mobile Newt. Appl., vol. 10, no. 1, pp. 19- 34, 2005.
[19] X. Jia, D. Li, and D. Du, "QoS topology control in ad hoc wireless networks," in Proc. IEEE INFOCOM, Mar. 2004.
[20] Q. Guan, Q. Ding, and S. Jiang, "A minimum energy path topology control algorithm for wireless multichip networks," in Proc. IWCMC, June 2009.

