Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Monterrey

División de Electrónica, Computación, Información, y Comunicaciones

Programa de Graduados

Evaluating Organization and Connectivity in Ad-Hoc Wireless Networks

THESIS

Presented as a partial fulfillment of the requeriments for the degree of

Master of Science in Electronic Engineering

Major in Telecommunications

Aldo López Gudini

Monterrey, N.L. June 2003

Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Monterrey

División de Electrónica, Computación, Información, y Comunicaciones

Programa de Graduados

The members of the thesis committee recommended the acceptance of the thesis of Aldo López Gudini as a partial fulfillment of the requeriments for the degree of Master of Science in:

Electronic Engineering

Major in Telecommunications

THESIS COMMITTEE

César Vargas Rosales, Ph.D.
Advisor

Jorge Carlos Mex Perera, Ph.D.
Synodal

Artemio Aguilar Coutiño, M.Sc.
Synodal

Approved

David Garza Salazar, Ph.D.
Director of the Graduate Program

June 2003

Acknowledgements

To my parents Maria del Pilar and Genaro Noe, for their unconditional support in all my life. To my brother Miguel Angel for support to me at any moment.

I am very grateful to my thesis advisor César Vargas Rosales Ph.D. for all these time in which we works together, for all his professional advice for the accomplishment of this work and for his friendship. Because, without his guidance this thesis would not have been possible. Sincerely thanks Doc. Also I want to thank to Jorge Carlos Mex Perera, Ph.D. and Artemio Aguilar Coutiño, M.Sc. for their valuable comments for the enhancement of this work.

To the ITESM and CONACYT for give me the oportunity of realize my graduate studies.

I want to thank too all my friends of CET, specially to Lluvia, Anabel, Martha, Dulce, Rodolfo, Oscar, Edson, Abraham, Luis, Ulises, Marco, Rafael, Fernando, Alejandro Trigos, and Rene. To all my friends of the 4th floor; Michelle, Vladimir, Max, Sergio and Roger.

Aldo López Gudini

Instituto Tecnológico y de Estudios Superiores de Monterrey
June 2003

Evaluating Organization and Connectivity in Ad-Hoc Wireless Networks

Aldo López Gudini, M.Sc.
Instituto Tecnológico y de Estudios Superiores de Monterrey, 2003

Los sistemas inalámbricos han experimentado un rápido crecimiento, donde el principal objetivo de este crecimiento es la de alcanzar la satisfacción del cliente, y de esta forma lograr que los usuarios puedan comunicarse sin la necesidad de una conexión convencional (alambrica). Las redes inalámbricas ad hoc están constituidas por nodos móviles conectados entres si por multienlaces de comunicación. Esta red inalámbrica a diferencia de las demás redes no tiene una estructura convencional como las redes inalámbricas tradicionales, las cuales presentan una estructura predefinida y además fija, de aquí el surgimiento de problemas de este tipo de redes con relación al ruteo y el mantenimiento punto a punto de un enlace dadas las circunstancias de movilidad que cada nodo presenta.

Otro problema relacionado con la poca cantidad de nodos es la conectividad, la cual es baja si existe una baja cantidad de nodos, pero esta de igual forma puede ser baja si los nodos están organizados en diferentes grupos.

Este trabajo considera estos problemas con el objetivo de presentar parámetros tales como la fragilidad de un cluster virtual y diferentes tipos de conectividad que nos proporcionen una idea y una visión para estos problemas.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The ad hoc wireless network consists of mobile nodes connected by links called multilinks of communication. This wireless network does not have a conventional structure as traditional wireless networks do, which present a predefined structure and fixed, the problems start here and they are related to routing, the maintenance of the point to point link, the bandwidth among which they directly affect the QoS of the ad hoc network degrading it, [1], [2].

Due to the benefits and to the unique versatility that present the ad hoc networks in certain environments and applications being implemented; the interest in the development of this type of network in special, has come to more; in the military areas, rescue, in zones of hostile natural and environment disasters. One of the main problems that appear in ad hoc networks is the updating of the topology, since the nodes have mobility and therefore the structure of the network varies with time; because nodes are added or eliminated randomly and such process takes us to an update in the topology for each case; the variability of the network can be so frequent that the update cannot be propagated to all the network by broadcasting messages, which consist of directions and alternative routes, or some other method of update like flooding. In other words knowing the positions the neighboring nodes to the node source so that at certain moment can be used to create a trajectory towards the destination node that would guarantee an acceptable QoS to us, [1], otherwise, if it were not gotten to possible alternative routes and the link failed in the central part, that is, when another node takes part in the trajectory between the node source and the destination, the connection would be lost and as consequence the QoS is also degraded in the ad hoc network, [3].

The study of the mobility of these nodes within the ad hoc network can be made dividing the area or space in cluster called cells where the network ad hoc is implemented for analysis and management of an easy way.

1.1 Objective

The objective of this thesis is to evaluate the performance of ad hoc networks with respect to the organization, connectivity and mobility of the nodes, using point processes to study of it.

1.2 Justification

The ad hoc networks are systems of fast implementation that do not count on permanent physical infrastructure. Due to this, to obtain the interconnections of nodes source and destination, it is necessary to establish topologies on which the routes are constructed that will transport the information, but given the ample class of stations (fixed, semi-portable, mobiles), is necessary to study the way in which the nodes will be organized to be able to define a topology, which will work the network and the necessary connectivity for its operation and their formation and its maintenance.

1.3 Contribution

We propose new parameters with the goal of analyzing the organization, connectivity and mobility of ad hoc wireless networks with different density of node.

1.4 Organization

This work is organized as follows. In Chapter 2, we presents an overview of the ad hoc history and some problems of this network. In this chapter we are going to detail some ad hoc routing protocols and some clustering protocols. Chapter 3 presents the model and parameters proposed to analyze the mobility and organization of an ad hoc network. Chapter 4 shows numerical results obtained from the simulation. Finally, Chapter 5 presents conclusions and future work.

Chapter 2

Background

Wireless systems have experienced a fast growth where their main objective is to look for customer´s satisfaction, so the users can be in communication without the necessity of a wired connection.

In the present Chapter we analyze briefly what an ad hoc wireless network is, its routing protocols and its self-organization for a best management.

2.1 Ad Hoc Wireless Networks

An ad hoc wireless network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range or one that is outside their range.

An ad hoc wireless network is self-organizing and adaptive. This means that a formed network can be de-formed on-the-fly without the need for any system management. The term "ad hoc" tends to imply "can take different forms" and can be mobile, standalone, or networked, [4], [6].

Since ad hoc wireless devices can take different forms (for example, palmtop, laptop, internet mobile phone, etc.), as show in Figure 2.1, the computation storage, and communications capabilities of such devices will vary tremendously. Ad hoc devices should not only detect the presence of connectivity with neighboring devices/nodes, but also identify what type the devices are and their corresponding attributes. There is no need for any fixed radio base stations, no wires or fixed route, [1], [2], [6]. Due the mobility, routing information will have to change to reflect changes in link connectivity.

Ad hoc wireless communications can occurs in several different forms. For a pair of ad hoc wireless nodes, communications will occur between them over period of time until the session is finished or one of the nodes has moved away. This resembles a peer-to-peer communication scenario.

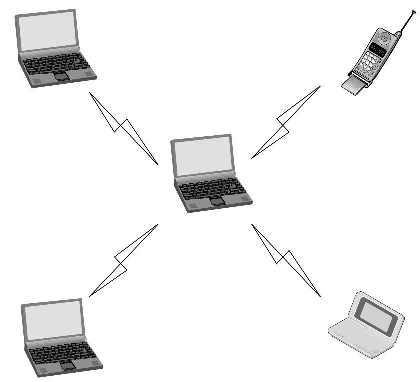

Figure 2.1: Mobile Host Network

Another form occurs when two or more devices are communicating among themselves and they are migrating in groups. The traffic pattern is, therefore, one where communications occur over a longer period of time. This resembles the scenario of remote-to-remote communication, [6].

Finally, we can have a scenario where devices communicate in a non-coherent fashion and their communication sessions are, therefore, short, abrupt, and undeterministic.

2.2 Types of Ad Hoc Mobile Communications

Mobile host in an ad hoc mobile network can communicate with their immediate peers, that is, peer-to-peer, that are in a single radio hop away. However, if three or more nodes are within range of each other (but no necessarily a single hop away from one another), then remote-to-remote mobile node communications exist.

This section examines the types of mobile host movements that can affect validity of routes directly.

2.2.1 Movements by Nodes in a Route

An ad hoc route comprises the source (SRC), destination (DEST), and/or a number of relay nodes (INs). Movement by any of these nodes will affect the validity of the route.

An SRC node in a route has a downstream link, and when it moves out of its downstream neighbor's radio coverage range the existing route will immediately become invalid.

Likewise, when a DEST node moves out of the radio coverage of its upstream neighbor, the route becomes invalid. However, unlike the earlier case, here, the upstream nodes will have to be informed so they can erase their invalid route entries, [6].

All these movements cause many conventional distributed routing protocols to respond in sympathy with the link changes. This results in an updating of all the remaining nodes within the network. The updating process involves broadcasting over the wireless medium, which results in wasteful bandwidth and an increase in the overall network control traffic. Hence new routing protocols are needed, [3], [6].

2.2.2 Movements by Subnet-Bridging Nodes

In addition to the above-mentioned mobility scenario, any movement by a node that is performing a subnet-bridging function between two mobile subnets can fragment the mobile subnet into smaller subnets. The property of a mobile subnet states that if both the SRC and DEST nodes are elements of the subnet, a route or routes should exist unless the subnet is partitioned by some subnet-bridging mobile nodes.(See Figure 2.2).

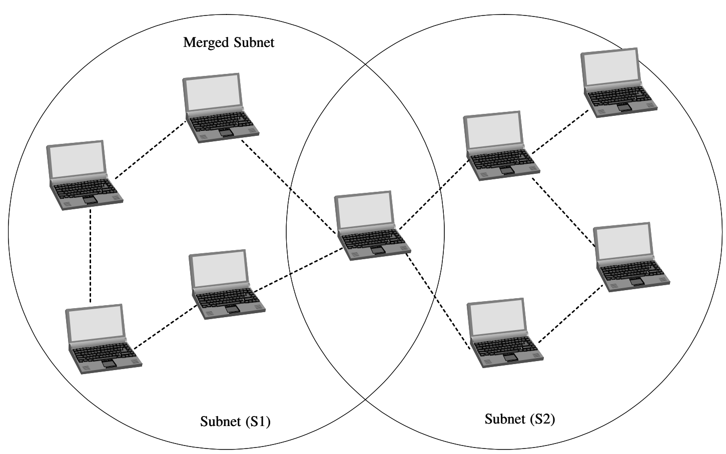

Figure 2.2: Mobile ad hoc subnets merging and fragmenting

2.3 Ad Hoc Routing Protocols

One of the major challenges in designing a routing protocol for the ad hoc networks stems from the fact that, on one hand, to determine a packet route, a node needs to know at least the reachability information to its neighbors. On the other hand, in an ad hoc network, the network topology can change quite often. Furthermore, as the number of network nodes can be large, the potential number of destinations is also large, requiring large and frequent exchange of data (e.g., routes, routes updates, or routing tables) among the network nodes. Thus, the amount of update traffic can be quite high. This is in contradiction with the fact that all updates in a wirelessly interconnected ad hoc network travel over the air and, thus, are costly in resources.

The presence of mobility implies that links make and break often in an indeterministic fashion. Note that the classical distributed Bellman-Ford routing algorithm is used to maintain and update routing information in a packet radio network. While distance-vector-based routing is not designed for wireless network, it is still applicable to packet radio networks since the rate of mobility is not high. Hence, ad hoc mobile networks are different from radio networks since nodes can move more freely, resulting in a dynamically changing topology. Existing distance-vector and link-state-based routing protocols are unable to catch up with such frequent link changes in ad hoc wireless networks, resulting in poor route convergence and very low communication throughput. Hence, new routing protocols are needed.

Since the advent of the DARPA packet radio network in the early 1970s, numerous protocols have been developed for ad hoc mobile networks, such protocols must fight with their own limitations of its network, which include high power consumption, low bandwidth, and high error rate, [3], [6], [15]. The routing protocols may generally be categorized as (Figure 2.3):

- Table-driven
- Source initiated on-demand-driven

2.3.1 Table-Driven Approaches.

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network, it mean, each node maintain one or more tables to store routing information, and they respond to changes in network

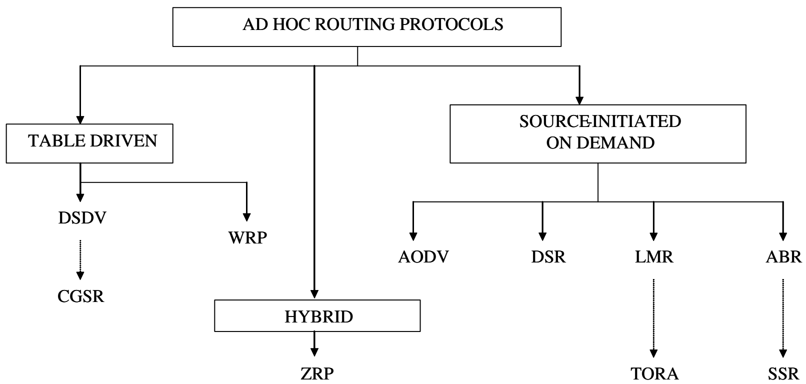

Figure 2.3: Categorization of ad hoc protocols

topology by propagating route updates throughout the network to maintain the consistent from, [3], [6].

Destination Sequenced Distance Vector (DSDV)

Destination Sequenced Distance Vector (DSDV) routing is a table-driven routing protocol based on the classical distributed Bellman-Ford routing algorithm. The improvement made here is the avoidance of routing loops in a mobile network of routers. Each node in the mobile network maintains a routing table in which all of possible destinations within the non-partitioned network and the number of routing hops (in this case, number of radio hops) to each destination are recorded.

A sequence numbering system is used to allow mobile hosts to distinguish state routes from new ones. Routing tables updates are sent periodically throughout the network to maintain table consistency; as a result we generate a lot of control traffic in the network, rendering an inefficient utilization of network resource. DSDV with the aim of alleviate this problem uses two types of route update packets; the called full dump; this type of packet carries all available routing information and require multiple network protocol data units (NPDUs). During periods of occasional movement, these packets are transmitted infrequently. Smaller incremental packets are used to relay only information that has changed since that last full dump, [3], [19], [16].

Wireless Routing Protocol (WRP)

WRP stems from the way in which it achieves loop freedom. In WRP, routing nodes communicate the distance and second-to-last hop information for each destination in the wireless network. It avoids the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This ultimately eliminates looping situations and provide faster route convergence when a link failure event occurs.

In WRP, nodes learn about the existence of their neighbors from the receipt of acknowledgments and other messages. If a node is not sending packets, it must send a HELLO message within a specified time period to ensure that information connectivity is properly reflected. When a mobile receive a HELLO massage from a new node, the new node transmits a copy of its routing table information.

WRP must maintain four tables, namely:

- Distance table
- Routing table
- Link-cost table
- Message retransmission list (MRL) table.

The distance table indicates the number of hop between a node and its destination. The routing table indicates the next-hop node. The link-cost tale reflects the delay associated with particular link. The MRL contains the sequence number of the update message, a retransmission counter, an acknowledgment required flag vector, and a list of the updates sent in the update message.

To ensure that routing information is accurate, mobiles send update messages periodically to their neighbors. The updated message contains a list of changes (the destination, the distance to destination, the predecessor of the destination), as well as a list of responses indicating which mobile should acknowledge the update, [20], [21].

Cluster Switch Gateway Routing (CSGR)

Cluster Switch Gateway Routing is a table-driven-based routing protocol where mobile nodes are grouped into clusters and each cluster has a cluster head. This grouping also introduces a form of hierarchy. A cluster head can control a group of ad hoc host, and clustering provides a framework for code separation (among cluster), channel accessing, routing and bandwidth allocation.

Although using a cluster head allows some form of control and coordination. When a cluster head moves away, another new cluster head must be selected. This can be problematic if a cluster head changing frequently and nodes will be spending a lot of time converging to a cluster head instead of forwarding data toward their intended destinations. To avoid invoking cluster head reselection every time the cluster membership changes, a least cluster changes (LCC) algorithm is introduced. The LCC algorithm, cluster head only change when two cluster head come into contact, or when a node moves out of all other heads.

CSGR uses DSDV as the underlying routing scheme. However, it modifies DSDV by using hierarchical cluster-head-to-gateway routing. Gateway nodes are nodes that are within communication range of two or more cluster heads. As show in Figure 2.4, a packet sent by a node is first routed to its cluster head, and then the packet is routed from a cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached.

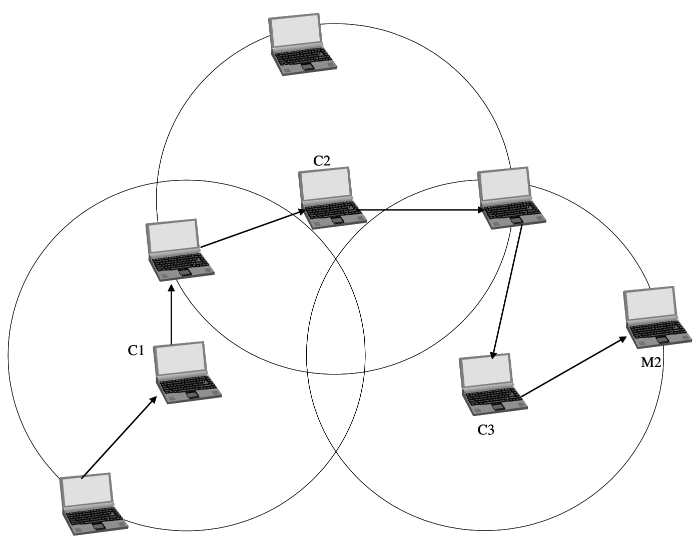

Figure 2.4: A CSGR path is constrained to cluster heads.

In CSGR, each node must keep a cluster member table, where it stores the destination cluster head for each mobile host in the network. These cluster member tables are broadcasted periodically by each node using the DSDV protocol. In addition to the cluster member table, each node must also maintain a routing table, which is used to determine the next hop to reach the destination, [22].

2.3.2 Source-Initiated On-Demand Approaches

An approach that is different from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined, [6].

Ad Hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance Vector Routing (AODV) routing protocol builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of route as in the DSDV algorithm. This protocol is classified as a pure on-demand route acquisition system.

When a source node wants to send a message to some destination node and does no already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (PREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located (Figure 2.5). AODV uses destination sequence members to ensure that all routes are loop-free and contain the most recent route information.

During the process of forwarding the PREQ, intermediate nodes record in their route tables the addresses of neighbors from which the first copy of the broadcast packet was received, thereby establishing a reverse path. If additional copies of the same PREQ are later received, these packets are silently discarded. Once the PREQ has reached the destination or an intermediate node with a "fresh enough" route, the destination/intermediate node responds by unicasting a route reply (PREP) packet back to the neighbor from which it first received the PREQ (Figure 2.5).

In AODV, routes are maintained as follows: if a source node moves, it has to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message (an PREP with an infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on, until the source node is reached. The source node may then choose to re-initiate route discovery for that destination if a

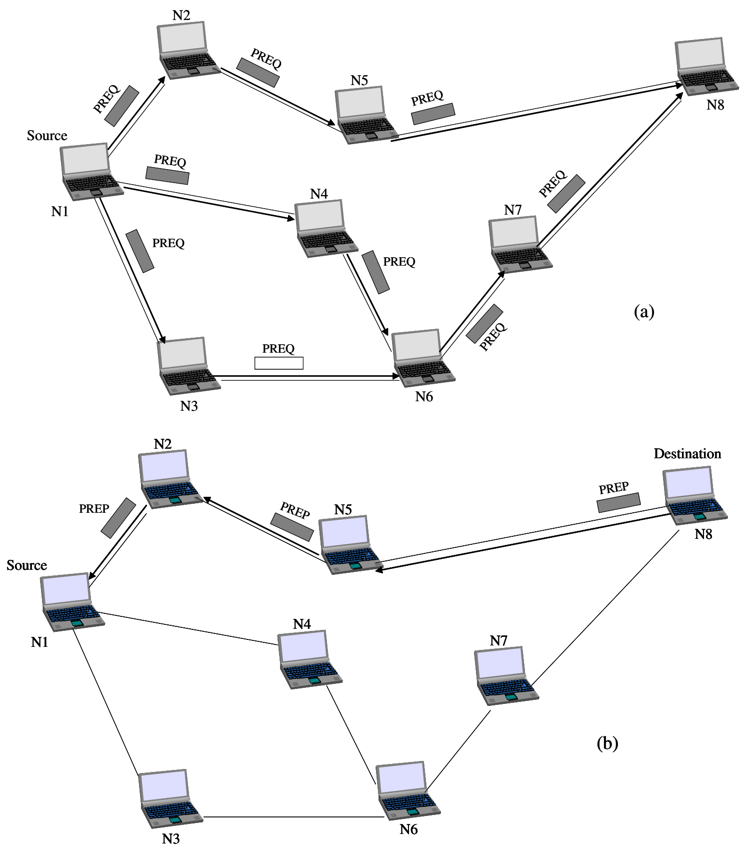

Figure 2.5: AODV route discovery.

route is still desired.

An additional aspect of the protocol is the use of HELLO message which are periodic local broadcast made by node to inform each mobile node of other nodes in its neighborhood. HELLO messages can be used to maintain the local connectivity of a node. However, the use of HELLO message is not required. Nodes listen for retransmissions of data packet to ensure that the next hop is still within reach, [3], [15], [16], [23].

Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR), is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new route are learned.

The protocol consists of two major phases:

- Route discovery
- Route maintenance

When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request message contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route request propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address has not already appeared in the route record. A route reply is generated when either the route request reaches the destination itself, or when it reaches an intermediate node that contains in its route cache an expired route to the destination.

Route maintenance is accomplished through the use of route error packets and acknowledgments. Route error packets are generated at a node when a data link layer encounters a fatal transmission problem. The source is always interrupted when a route is truncated. When a route error packet is received, the hop in error is removed from the node's route and all routes containing the hop are truncated at that point, [3], [24].

Temporally Ordered Routing Algorithm (TORA)

TORA is high adaptive, loop-free, distributed routing algorithm based on the concept of link reverse. TORA is proposed to operate in a highly dynamic mobile networking environment. It is source-initiated and provides multiple routes for any desired source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change (1-hop), [3]. The protocol performs tree basic functions:

- Route creation
- Route maintenance
- Route erasure.

During the route creation and maintenance phases, nodes use a “height” metric to establish a DAG (directed acyclic graph) rooted at the same destination.

Timing is an important factor for TORA because the “height” metric is dependent on the logical time of a link failure; TORA assumes all nodes have synchronized clocks (accomplished via an external time source such as the global positioning system (GPS)). Hence, it is unclear if TORA would function properly in an environment where GPS is not available or is not reliable.

TORA's metric is a quintuple comprising five elements, namely:

- Logical time link failure
- The unique ID of the node that defined the new reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

The first three elements collectively the reference level. A new reference level is defined each times a node loses its last downstream link due to a link failure. TORA's route erasure phase essentially involves flooding a broadcast “clean packet” (CLR) throughout the network to erase invalid routes, [25].

In TORA, there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Because TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will ultimately occur, [25].(See Figure 2.6).

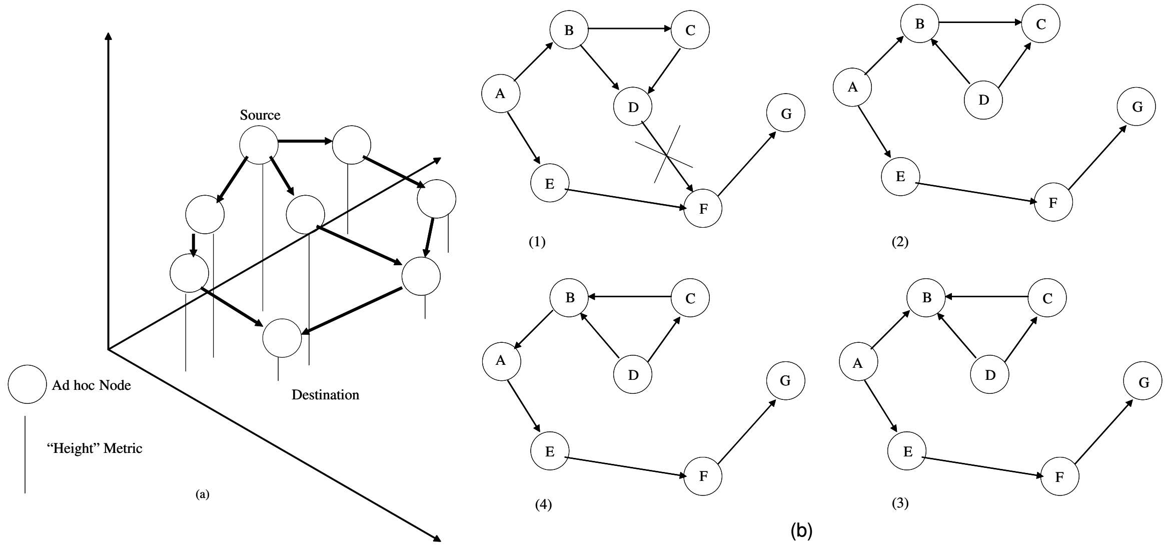

Figure 2.6: (a) Route creation, and (b) route maintenance in TORA

Signal Stability Routing (SSR)

Another on-demand protocol is the Signal Stability-Based Adaptive Routing (SSR) protocol. SSR is a descendent of Associativity-Based Routing (ABR), and ABR predates SSR. Similar to ABR, SSR selects routes based on the signal strength between nodes and a node's location stability. SSR route selection criteria has a effect of choosing routes that have "stronger" connectivities. SSR can be divided into two cooperative protocols, [3], [26]:

- The Dynamic Routing Protocol (DRP)
- The Static Routing Protocol (SRP)

The DPR is responsible for the maintenance of the signal stability table (SST) and the routing table (RT). The SST records the signal strength of neighboring nodes, which is obtained by periodic beacons from the link layer of each neighboring node. After updating all appropriate table entries, the DRP passes a received packet to the SRP.

The SRP processes packets by passing them up the stack if they are the intended receivers, or looking up their destination in the RT and then forwarding them if they are not. If not entry is found in the RT for the destination, a route-search process is initiated to find a route.

The assumption made in SSR is that route search packets arriving at the destination might have chosen the path of strongest signal stability, as the packets are dropped at a node if they have arrived over a weak channel.

When a failed link is detected within the network, intermediate nodes will send an error message to the source indicating which channel has failed. The source initiates another route process to find a new path to the destination. Thereafter, the source sends an erase message to notify all nodes of the broken link, [26].

Location-Aided Routing (LAR)

Compared to other ad hoc routing schemes, LAR utilizes location information (via, say, the GPS) to improve the performance of ah doc wireless networks.

LAR limits the search for a new route to smaller request zone, thereby resulting in reduced signaling traffic. LAR defines two concepts:

- Expected zone
- Request zone

LAR makes several assumptions. First, it assumes that the sender has advanced knowledge of the destination location and velocity. Based on the location and velocity, the expected zone can be defined. The request zone, however, is the smallest rectangle that includes the location of the sender and expected zone, [6]. (see Figure 2.7).

Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) is a hybrid protocol incorporating the merits of on-demand and proactive routing protocols. A routing zone is similar to a cluster with the exception that every node acts as a cluster head and a member of other clusters. Zones can overlap. Each node specifies a zone radius in terms of radio hops. The size of a chosen

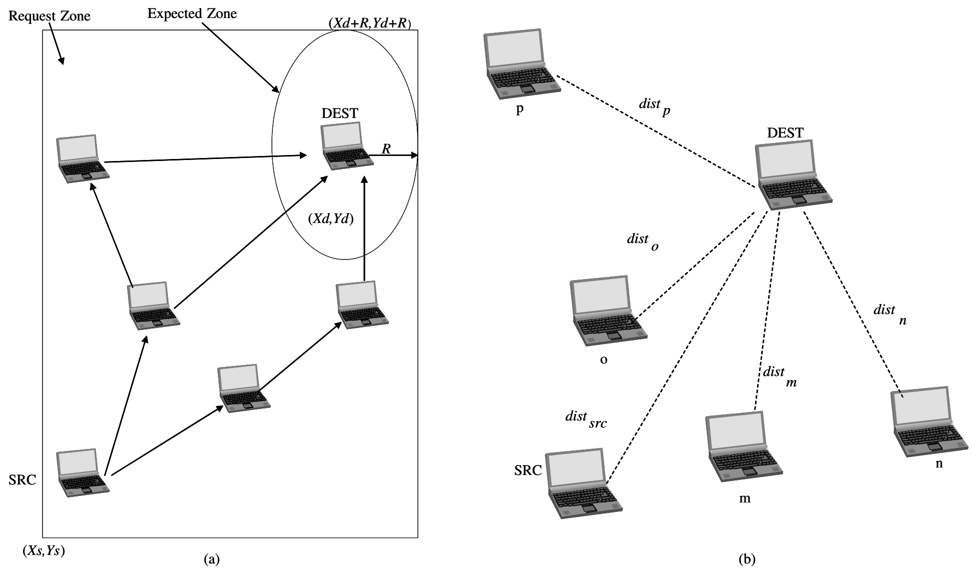

Figure 2.7: (a) Concepts LAR, and (b) route physical distance.

zone can, therefore, affect ad hoc communication performance, [4], [27].

In ZRP, a routing zone comprises a few mobile ad hoc nodes within one, two or more hops away from where the central node is formed. Within this zone, a table-driven-based routing protocol is used. A related issue is that of updates in the network topology. For a routing protocol to be efficient, changes in the network topology should have only a local effect. In other words, creation of a new link at one end of the network is an important local event but, most probably, not a significant piece of information at the other end of the network. Globally proactive protocols tend to distribute such topological changes widely in the network, incurring large costs. The ZRP limits propagation of such information to the neighborhood of the change only, thus limiting the cost of topological updates.

ZRP itself has three sub-protocols, see Figure 2.8:

- The proactive (table-driven) Intrazone Routing Protocol (IARP)
- The reactive Interzone Routing Protocol (IERP)
- The Bordercast Resolution Protocol (BRP).

IARP can be implemented using existing link-state or distance-vector routing. Unlike OSPF or RIP, propagated routing information is propagated to the border of the routing

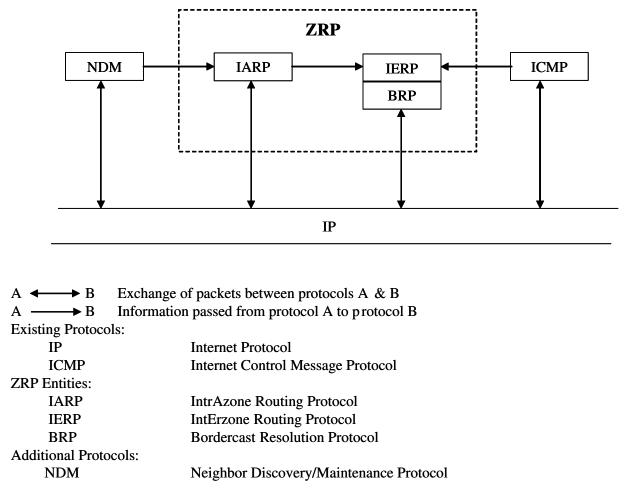

Figure 2.8: The ZRP Architecture.

zone.

ZRP's IARP relies on an underlying neighbor discovery protocol to detect the presence and absence of neighboring nodes, and therefore, link connectivity to these nodes. Its main role is to ensure that each node within the zone has a consistent routing table that is up-to-date and reflects information on how to reach all other nodes in the zone. An example of a radius $R = 2$-hop routing zone (for node A) is shown in Figure 2.9; in this example nodes B through F are within the routing zone of A. Node G is outside A's routing zone. Also note that E can be reached by two paths from A, one with length 2-hops and one with length 3-hops. Since the minimum is less than or equal to 2, E is within A's routing zone. Peripheral nodes are routing zone nodes whose minimum distance to the node in question is equal exactly to the zone radius. In the above figure, nodes D, F and E are A's peripheral nodes. These peripheral nodes play an important role in efficient querying based on bordercasting. We note that each node maintains its own routing zone. As a result, routing zones of nearby nodes may overlap heavily.

Each node proactively tracks the topology of its routing zone through an IntrAzone Routing Protocol (IARP). IARP is derived from globally proactive link state routing protocols (for example, OSPF), [28].

IERP, however, relies on border nodes to perform on-demand routing to search for routing information to nodes residing outside its current zone. Instead of allowing the query

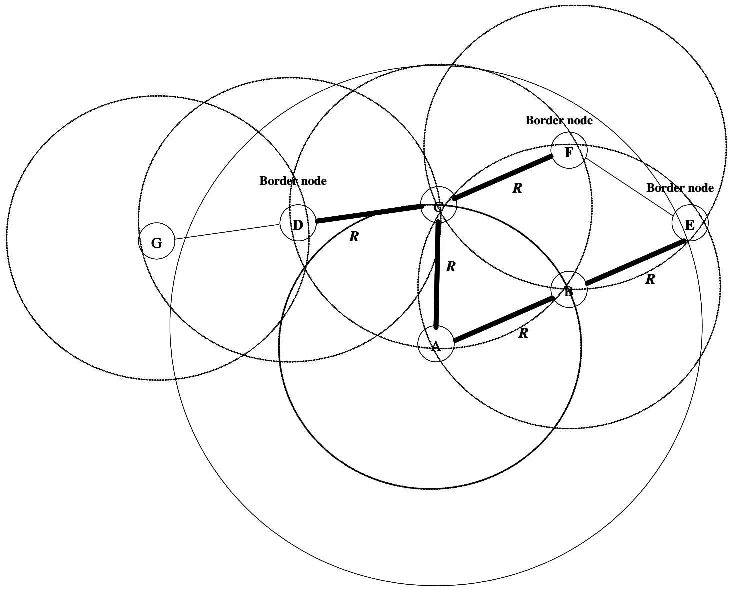

Figure 2.9: The proactive Intrazone Routing Protocol (IARP)

broadcast to penetrate into nodes within other zones, the border nodes in other zones that receive this messages will not propagate it further. IERP uses the bordercast resolution protocol. Bordercasting is possible as any node knows the identity and the distance to all the nodes in its routing zone by the virtue of the IARP protocol. (see Figure 2.10).

The IERP operates as follows: The source node first checks whether the destination is within its routing zone. (Again, this is possible as every node knows the content of its zone). If so, the path to the destination is known and no further route discovery processing is required. If, on the other hand, the destination is not within the source's routing zone, the source bordercasts a route request (referred to here as a "request") to all its peripheral nodes. Now, in turn, all the peripheral nodes execute the same algorithm: check whether the destination is within their zone. If so, a route reply (referred to here as a "reply") is sent back to the source indicating the route to the destination. If not, the peripheral node forwards the query to its peripheral nodes, which, in turn, execute the same procedure. An example of this Route Discovery procedure is demonstrated in the figure below. As we be shown, thus, a route within a network is specified as a sequence of nodes, separated by approximately the zone radius, [29]. In Figure 2.11 the node A has a datagram to node L. Assume routing zone radius of 2-hop. Since L is not in A's routing zone (which includes B, C, D, E, F, G), A bordercast a routing request to its peripheral nodes: D, F, E, and G. Each one of these peripheral nodes check whether L exists in their routing zones. Since

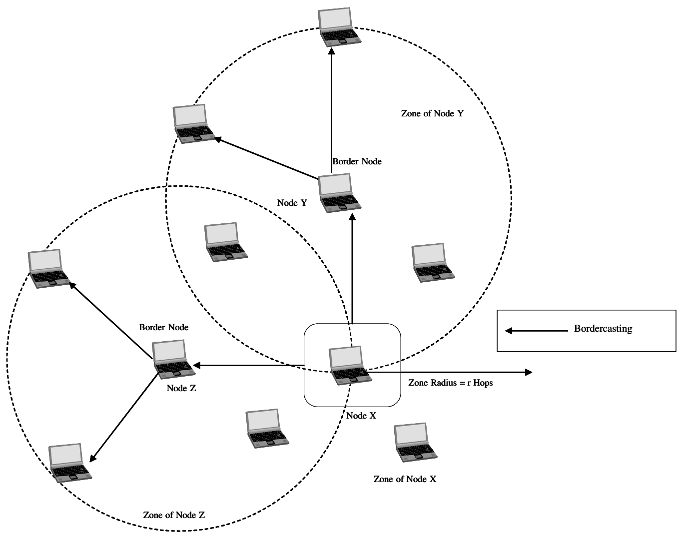

Figure 2.10: Hybrid Approach - Zone routing protocol.

L is not found in any routing zones of these nodes, the nodes bordercast the request to their peripheral nodes. In particular, G bordercasts to K, which realizes that L is in its routing zone and returns the requested route $(L-K-G-A)$ to the query source, namely A.

The IERP also provides a mechanism to reactively respond to route failures. A route failure is detected by the IP when the next hop in a source route is determined to be unreachable (i.e., does not appear in the Intrazone Routing Table). Upon detection of a route failure, the IERP is alerted, and a route failure packet is generated. The route failure packet propagates back to the route's source in the same manner as a route reply. When the route's source receives notification of the route failure, the expired route is removed from its Interzone Routing Table. The IERP may also be configured to locally repair the damaged Interzone route by initiating a route discovery to the unreachable next hop, [27], [31].

When a route is broken due to mobility, if the source of the mobility is within the zone, it will inform all other nodes in the zone. If the source of mobility is a result of the border node or other zone nodes, then route repair in the form of a route query search is performed, or in the worst case, the source node is informed of route failure.

The Bordercast Resolution Protocol (BRP) is included with the IERP in order to provide bordercasting services which do not exist in IP. The higher layer interface of the BRP is designed to be compatible with any IP based application. However, it is assumed

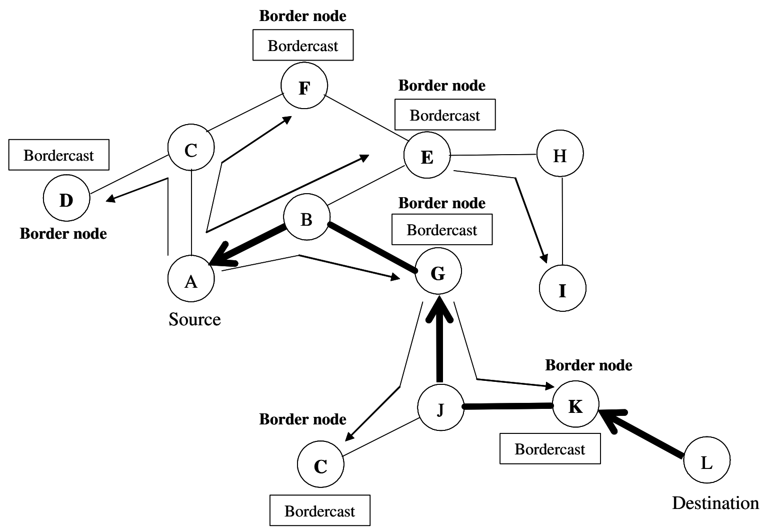

Figure 2.11: The reactive Interzone Routing Protocol (IERP)

that the routing zone hierarchy is visible only to the ZRP entities, making bordercasting services only of use to the IERP.

Upon receipt of a (IERP) packet to be bordercasted, the BRP resolves the bordercast address into the individual IP addresses of the peripheral nodes. The received packet is then encapsulated into a BRP packet and sent to each peripheral node (via IP broadcast transmission).

The bordercasting packet delivery service is provided by the Bordercast Resolution Protocol (BRP). The BRP uses a map of an extended routing zone, provided by the local proactive Intrazone Routing Protocol (IARP), to construct bordercast (multicast) trees along which query packets are directed. (Within the context of the hybrid ZRP, the BRP is used to guide the route requests of the global reactive Interzone Routing Protocol (IERP)). The BRP employs special query control mechanisms to steer route requests away from areas of the network that have already been covered by the query. The combination of multicasting and zone based query control makes bordercasting an efficient and tunable service that is more suitable than flood searching for network probing applications like route discovery.

When a BRP packet is delivered from IP, the (IERP) data is decapsulated and passed on to the higher layer. If the BRP packet has not reached its destination, the BRP is responsible for forwarding the packet to the next hop toward its destination, [30].

2.4 Clustering

There are several major difficulties for designing a routing protocol for MANET. Firstly, MANET has a dynamically changing topology due to the movement of mobile nodes which favors routing protocols that dynamically discover routes. Secondly, the fact that MANET lacks any structure makes IP subnetting inefficient. Thirdly, links in mobile networks could be asymmetric at times. If a routing protocol relies only on bi-directional links, the size and connectivity of the network may be severely limited; in other words, a protocol that makes use of uni-directional links can significantly reduce network partitions and improve routing performance.

Since we have mentioned until now, the networks ad hoc do not depend on some infrastructure of preexisting communication like in the cellular systems; in this networks the mobiles nodes can be found dispersed, reason why they probably do not have direct connection with all other nodes. These situations determine necessary the use of intermediate nodes to reach to the destination node. A solution taken from the cellular networks is that the nodes that are in the ad hoc network self-organize themselves into clusters. Three main advantages arise here, [2]:

1. In a multihop environment, the structure of clusters facilitates reuse of resources to increase the capacity. If it does not exist overlaps of multicluster, two clusters can use the same frequency or code set if they are not neighbors.

2. The update of topology becomes hierarchical. When a mobile node changes position, this event is sufficient so that single nodes pertaining to this cluster update their topology, and not all the network.

3. The propagated and generated routing information can be reduced.

This is why many clustering algorithms have been proposed for network management.

2.4.1 Cluster Based Routing Protocol (CBRP)

Cluster Based Routing Protocol (CBRP) is a routing protocol designed for use in mobile ad hoc networks. The protocol divides the nodes of the ad hoc network into a number of overlapping or disjoint 2-hop-diameter clusters in a distributed manner. A cluster head is elected for each cluster to maintain cluster membership information. The protocol efficiently minimizes the flooding traffic during route discovery and speeds up this process as well, [7].

CBRP has the following features:

- Fully distributed operation.
- Less flooding traffic during the dynamic route discovery process.
- Explicit exploitation of uni-directional links that would otherwise be unused.
- Broken routes could be repaired locally without rediscovery.
- Sub-optimal routes could be shortened as they are used.

The route shortening and local repair. Both features make use of the 2-hop-topology information maintained by each node through the broadcasting of HELLO messages. The route shortening mechanism dynamically shortens the source route of the data packet being forwarded and informs the source about the better route. Local route repair patches a broken source route automatically and avoids route rediscovery by the source, [7].

However, the overhead for maintaining up-to-date information about the whole network's cluster membership and inter-cluster routing information at each and every node in order to route a packet is considerable. As network topology changes from time to time due to node movement, the effort to maintain such up-to- date information is expensive and rarely justified as such global cluster membership information is obsolete long before they are used, [7]. CBRP terminology:

Node ID, is a string that uniquely identifies a particular mobile node. Node IDs must be totally ordered. In CBRP, we use a node's IP address as its ID for purposes of routing and interoperability with fixed networks.

Cluster, a cluster consists of a group of nodes with one of them elected as a cluster head. A cluster is identified by its Cluster Head ID. Clusters are either overlapping or disjoint. Each node in the network knows its corresponding Cluster Head(s) and therefore knows which cluster(s) it belongs to.

Host Cluster, a node regards itself as in cluster X if it has a bi-directional link to the head of cluster X. In such a case, cluster X is a host cluster for this node. A node could have several host clusters.

Cluster Head, a cluster head is elected in the cluster formation process for each cluster. Each cluster should have one and only one cluster head. The cluster head has a bi-directional link to every node in the cluster. A cluster head will have complete knowledge about group membership and link state information in the cluster within a bounded time once the topology within a cluster stabilizes.

Cluster Member, all nodes within a cluster EXCEPT the cluster head are called members of this cluster.

Gateway Node, any node a cluster head may use to communicate with an adjacent cluster is called a gateway node.

HELLO message, all nodes broadcast HELLO messages periodically every HELLO INTERVAL seconds; a node's HELLO message contains its Neighbor Table and Cluster Adjacency Table. A node may sometimes broadcast a triggered HELLO message in response to some event that needs quick action.

Conceptual Data Structures

Neighbor Table.

The neighbor table is a conceptual data structure that we employ for link status sensing and cluster formation, [7]. Each entry contains:

- The ID of the neighbor that it has connectivity with and
- the role of the neighbor (a cluster head or a member).
- the status of that link (bi-directional or uni-directional).

Cluster Adjacency Table.

The Cluster Adjacency Table keeps information about adjacent clusters. Each entry contains, [7], [15]:

- the ID of the neighboring cluster head
- the gateway node (a member) to reach the neighboring cluster head

- the status of the link from the gateway to the neighboring cluster head (bi-directional or uni-directional).

Two-hop Topology Database.

In CBRP, each node broadcasts its neighbor table information periodically in HELLO packets. Therefore, by examining the neighbor table from its neighbors, a node is able to gather complete information about the network topology that is at most two-hops away from itself.

Physical and Link Layer Assumptions

Each MANET node that runs CBRP is equipped with one wireless transceiver. CBRP is capable of handling multiple transceivers per host and multiple hosts per router if the concept of a router ID is introduced.

CBRP assumes omnidirectional antennas. Each packet that a node sends is broadcast into the region of its radio coverage. CBRP is designed to operate on top of a single-channel broadcast medium.

Link/Connection Status Sensing Mechanism.

Each node knows its bi-directional links to its neighbors as well as uni-directional links from its neighbors to itself. Each node periodically broadcasts its Neighbor Table in a HELLO message.

Upon receiving a HELLO message from its neighbor B, node A modifies its own Neighbor Table as follows:

1. It checks if B is already in the Neighbor Table; if not, it adds one entry for B if it has heard from B in the previous HELLO_INTERVAL before. If B's Neighbor Table contains A, A marks the link to B as bi-directional in the relevant entry else A marks the link to B as uni-directional (uni-directional from B to A).

2. If B is already in A's Neighbor Table.

- If the link_status field of B's entry says bi-directional but A is not listed in B's hello message, then change it to uni-directional.

- If the link_status field of B's entry says uni-directional but A is listed B's hello message, then change it to bi-directional.

3. Update the role of B in the Role field of B's entry.

Each entry in the Neighbor Table is associated with a timer. A table entry will be removed if a HELLO message from the entry's node is not received for a period of (HELLO_LOSS+1)HELLO_INTERVAL.

When a node's neighborhood topology stabilizes, the Neighbor Table of a node will have complete information of all the nodes that have a bi-directional or uni-directional link to it within a bounded time. However, a node would not know to whom it has a uni-directional link. For example in Figure 2.12, the Neighbor Table of node 7 will show that 4 has a uni-directional link to it, however node 4 would not know of the existence of such a link.

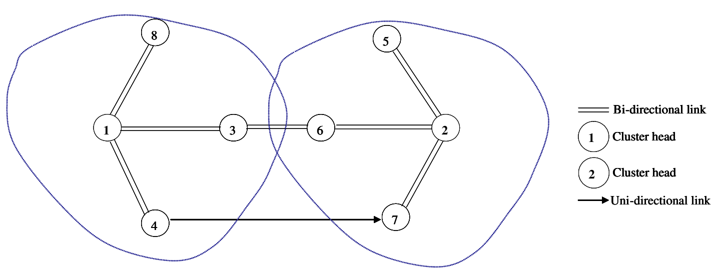

Figure 2.12: Link/Connection Status Sensing Mechanism

Protocol Operation

The operations of CBRP are entirely distributed. The major components are: Cluster Formation, Adjacent Cluster Discovery and Routing.

Cluster Formation

The goal of Cluster Formation is to impose some kind of structure or hierarchy in the otherwise completely disorganized ad hoc network. All nodes wake up in the Undecided state. A node uses the information obtained from the HELLO messages for Cluster Formation. When a cluster head receives a HELLO message from an Undecided Node, it will send out a triggered HELLO message immediately. If an undecided node receives a

HELLO message from a Cluster Head indicating a bi-directional link in between, it aborts its u_timer and sets its own status to C_MEMBER, [7].

A cluster head regards all the neighbors that it has bi-directional links to as its member nodes. A node regards itself as a member node for a particular cluster if it has a bi-directional link to the corresponding cluster head.(See Figure 2.13).

Rules for changing cluster head:

1. A non-cluster head never challenges the status of an existing cluster head, i.e. if X is a non-cluster head node with a bi-directional link to cluster head Y, X does not become a cluster head even if it has an ID lower than Y's.

2. When two cluster heads move next to each other (i.e. there is a bi-directional link between them) over an extended period of time (for CONTENTION_PERIOD seconds), then only will one of them lose its role of cluster head.

Adjacent Cluster Discovery

Cluster X and cluster Y are said to be bi-directionally linked, if any node in cluster X is bi-directionally linked to another node in cluster Y, or if there is a pair of opposite uni-directional links between any 2 nodes in cluster X and cluster Y respectively. For example in Figure 2.14, cluster 1 and cluster 2 are bi-directionally linked by the pair of links $3- > 4$ and $5- > 6$.

The goal of Adjacent Cluster Discovery is for a cluster to discover all its bi-directionally linked adjacent clusters. For this purpose, each node keeps a Cluster Adjacency Table (CAT) that records information about all its neighboring cluster heads, [7].

Routing Considerations

Routing in CBRP is based on source routing. It can be viewed as consisting of 2 phases: route discovery and the actual packets routing. Route Discovery is the mechanism whereby a node S wishing to send a packet to a destination D obtains a source route to D. the way S finds a route(or multiple routes) to D is also done by flooding.

Essentially, in Route Discovery, only cluster heads are flooded with Route Request Packets (RREQ) in search for a source route, [8].

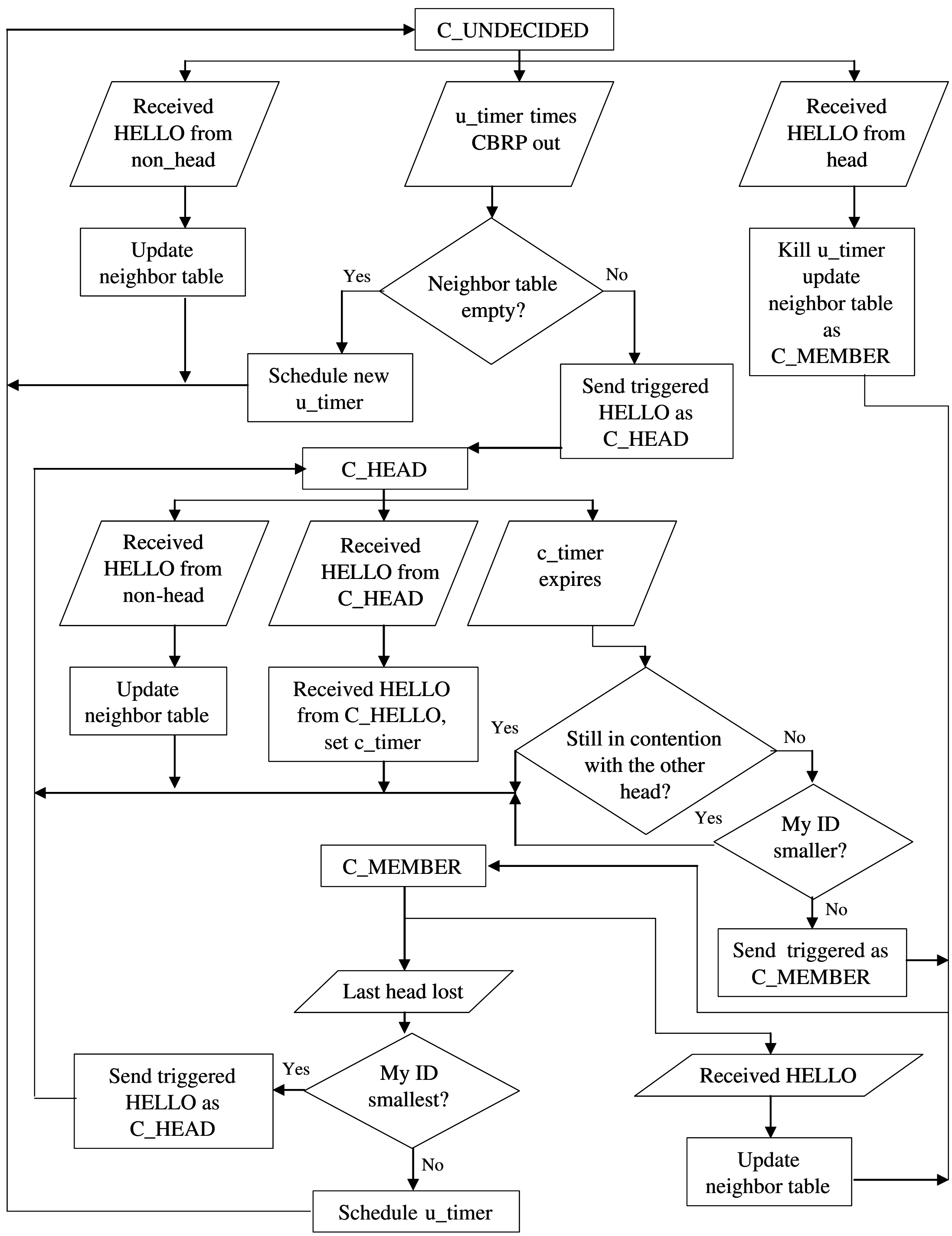

Figure 2.13: Transition diagram of a node in CBRP

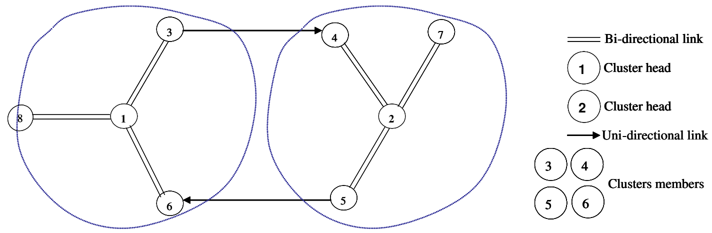

Figure 2.14: Adjacent Cluster Discovery

Routing

Route Shortening. Due to node movement or other reasons, a source route may become less optimal over time and should be shortened whenever possible. It works as follows: whenever a node receives a source-routed data packet, it tries to find out the furthest node in the unvisited route that is actually its neighbor. If it succeeds, it shortens the source route accordingly and sets the S flag before forwarding the packet. When a destination node receives a data packet with S flag set, it sends back a gratuitous RREP (setting the G flag in RREP) containing the shortened route to the packet source to inform it of the better route.

Route Error. When a forwarding node finds out that the next hop along the source route for an unsalvaged packet is no longer reachable, it will create a Route Error (ERR) packet and send it back to the packet source to notify it of the link failure, [7].

Local Repair. After the forwarding node detects a broken route and sends out an ERR packet, it will try to salvage the data packet the best way it can using its own local information:

1. It checks if the hop after next in the source route is reachable through an intermediate node other than the one specified as the next hop by searching through its 2-hop-topology database.

2. It checks if the unreachable next hop could be reached through an intermediate node by checking its 2-hop-topology database.

3. If the packet could be saved, it modifies the source route, sets the R flag and sends out the packet to the new next hop.

2.4.2 Access-Based Clustering Protocol (ABCP)

Nevertheless, the protocol that presents better characteristics for the process of update of the topology is the ABCP(Access-Based Clustering Protocol), since it provides generic characteristics, flexibility, rapidity in the update and a stable structure of cluster or cell. This protocol presents three main advantages that are: in which it concerns multiconnections (multihop), cluster facilitates the reuse of the resources to increase the capacity of the system, this is; two to cluster can use the same frequency or code as long as these cluster, he is not neighboring; the second advantage is that when changes its position in cluster the update of all the single system is not necessary that the node updates its information, and the third advantage is that the routing information and the propagation of this can be reduced, [2], [3], with the help of the clusterhead, a hierarchical routing or network management protocol can be more easily implemented with fewer overheads.

There are two criteria for cluster initialization, and begin to partition mobile users. One is based on the node ID and the other is based on degree (the number of direct links to its neighbors). But we think that criteria based on the node ID is much more stable than the based on degree criterion; because one method for cluster maintenance is periodically running the cluster initialization algorithm regardless of the current cluster structure. The cluster updating , is realized for transmission of framework using hierarchical routing over dynamic clusters that are organized according to set of system parameters that control the size of each cluster and the number of hierarchical levels.

How we already mentioned, the clustering can facilitate the implementation such as spatial reuse, network management and routing. In a multihop environment, the resulting nonoverlapping cluster structure can be used to support the resource assignment. For instance, clustering provides controlled access to the channel bandwidth and scheduling of the nodes in each cluster in order to provide quality of service (QoS) support.

The objective of ABCP is build a stable cluster structure that can be deployed rapidly and do not need a mass of maintenance overhead.

Access-Based Criterion and MAC Protocol on Control Channel

Because the ad hoc network has no established infrastructure the signaling more suitable for control information dissemination consider is out-of-band signaling. Therefore, two types of channels is utilized for the exchange of control messages such as topology update, cluster formation, etc. the data channels are used for user data transport; and the other channel is dedicated to the control purposed and it is time slotted. If two nodes that simultaneously want to send control messages are more than two hops away, message collision will not occur. Thus, the time slot can be spatially reused to enhance the channel efficiency.

Access-Based Clustering Criterion

Each cluster consists of one clusterhead and zero or more ordinary nodes which must be direct neighbors of the clusterhead. In the formation of the cluster structure, each node accesses the control channel to declare its intention to form a cluster. A node that successfully sends clusrehead declaration before its one-hop neighbors do becomes clusterhead. A node that hears the clusterhead declarations from its neighbor before it has the chance to declare itself as a clusterhead becomes a member of the clusterhead node from which it receives the clusterhead declaration the first. Once a node becomes a clusterhead and has at least one cluster member, it continues to posses this role until becoming inactive.

MAC Protocol for the Control Channel: TPMA

For out-of-band signaling, one channel is dedicated to disseminate control information. The MAC protocol on single control channel has two key requirements:

1. it is distributed
2. it is to set up the channel for reliable broadcast.

The control channel is divided into fixed-size frames as shown in Figure 2.15, the format of control used in a channel within cluster in a network Ad hoc with each one of its parts that constitute it; in which two main parts can be appreciated that are; elimination slot and message slot; first it is used to synchronize the connections between nodes in a network Ad hoc which are carried out by means of Multihop or Multihop; and the second part, Message slot or groove of message that contains solely the information that is desired to send.

The defined part as elimination slot or groove of elimination this subdivided in mini-slots Ms, which are divided in three phases that are, [2].

1. RTS (Request To Send, Answer to send), in this phase each node makes their answers to indicate that it can transmit.
2. CR (Collision Report, Report of Collision), each node reports here that to happened a collision in phase RTS or no.
3. RA (Receiver Avaible, Available To receive), in this phase if some node receives an indication of RTS (Phase 1), then this node sent a RA to present that this available one to receive.

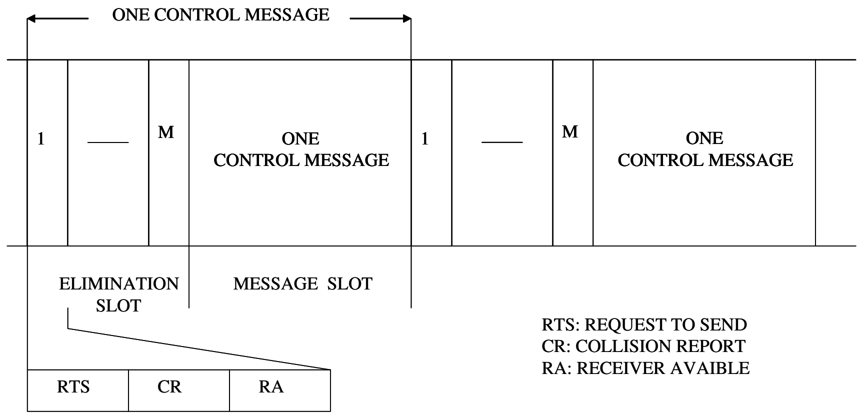

Figure 2.15: Format of control of channel in the Cluster of ad hoc network

Phases 1 and 3 are analogous to the RTS/CTS dialogue. However, instead of using a specific destination address (unicast), the RTS and RA indications are addressed to all one-hop neighbors (multicast). Phase 2 is used to indicate a collision occurrence if a node receives more than one RTS indications in phase 1. The following is a detailed description of the multiple access scheme.

- If a node A, wants to transmit a control message, it would wait the beginning of the next frame. In the first mini-slot of the elimination slot, node A sends an RTS in phase 1.

- If other nodes within two hops of node A also send RTS in the first mini-slot, collision will occur and be detected by one common one-hop neighbors of these transmitting nodes. The nodes that receive multiple RTSs will send a CR indication in phase 2 to indicate the collision.

- In the phase 3, the node that receives only one RTS in phase 1 will send a RA indication to acknowledge this RTS request. Phase 3 is designed to address the issue due to the restriction that a node cannot transmit and receive on the single channel simultaneously. In this phase, the node cannot transmit and receive on the single channel simultaneously.

Reason which we name this multiple access scheme for (local) broadcast as the Three-Phase Multiple Access (TPMA) scheme.

Thus ABCP is a simple broadcast request-response with first-come-first-serve (FCFS) and it is designed from a protocol's point of view in that it defines the message formats, describe how a node responds when a messages arrives, [2].

Protocol Description

ABCP is divided into two cases for consideration. First in the ordinary node case, three situations cause an ordinary node to send a REQ_TO_JOIN message:

- A node initially turns on its radio units and becomes a new come to this ad hoc network;
- A node detects that a link with its clusterhead is weakening; and
- A DISCONNECT message from its clusterhead is received.

The similar form that CBRP, it wait to receive one HELLO message of some clusterhead after that node had send a REQ_TO_JOIN message and set a timer. (See Figure 2.16).

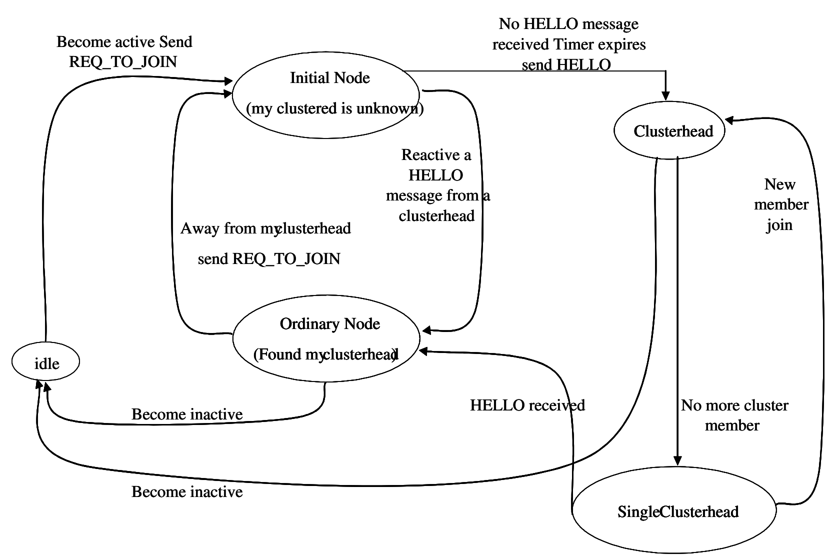

Figure 2.16: State transition diagram of a node in ABCP

2.5 Connectivity

We have spoken about the need to have an Ad hoc wireless network. Related to this fact a link maintenance is needed to hold a wireless connection of two nodes, this point is very important to guaranty a good Quality of service (QoS) in the hole network, voiding errors and even the loose links. This is why, a concept widely used must be introduced, which defines communication between two nodes, this new concept is “connectivity”.

A pragmatic definition of Connectivity; is the unbiased transport of packets between two ending points. This definition gives a very general idea to us of which we wished to present like connectivity; but for the case of an Ad hoc wireless network where the nodes are geographically dispersed and where more likely a node x cannot be connected with all others in a direct way or one hop; as a result we have h-hops to different intermediates nodes (IN) to reach our destination node; this is called h-connectivity.

A formal definition of which we called h-connetivity is; two nodes i and j in an undirected graph are h-connected if there is a path connecting i and j in every subgraph by deleting (h-1) nodes other than i and j together with their adjacent arcs from the graph. This definition is illustrated in Figure 2.17 where in (a) nodes 1 and 2 are 6-connected, nodes 2 and 3 are 2-connectivity, and 1 and 3 are 1-connected. Graph (a) nodes 1 and 2 are 1-connected. Graph (b) nodes 1 and 3 are 2-connected. Another notion of interest is the arc connectivity, which is defined as a minimum number of arcs that must be deleted before the graph becomes disconnected, [18].

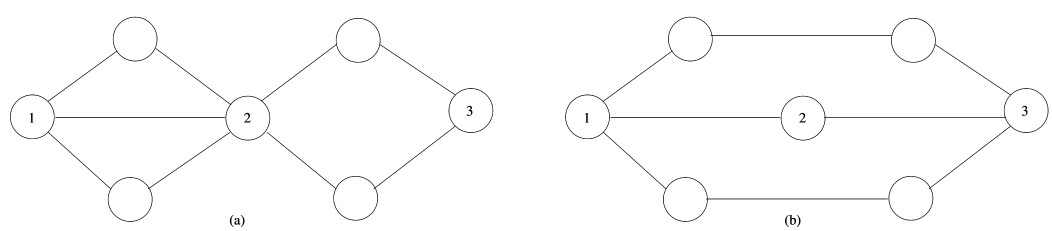

Figure 2.17: h-Connectivity

Chapter 3

Model Description

In this chapter we propose a model to analyze the ad hoc network connectivity, we develop concepts to describe the connectivity that exists in this type of networks which is important to know the network organization through time and we propose a parameter called fragility with the objective of analyzing the virtual cluster robust. We also analyze statistically the total absolute connectivity

Furthermore, we explain in this chapter the Virtual Cluster-based Routing Protocol (VCRP) idea and the form to generate nodes with point processes. Finally, we present an algorithm to evaluate the ad hoc network.

3.1 Point Processes

Based on the point processes, [5], we represent stations inside a limited area; at a specific moment in time they would be considered like static or without movement. We generate nodes within the study area using a Poisson distribution in the following way, [8],

$$P[X = k] = \frac{\gamma^k}{k!}e^{-\gamma}, \tag{3.1}$$

where γ is the average number of points per unit area, and X is the random variable for the number of nodes k=0,1,2,...

If we suppose that we have a square area with sides of length L then the total area is denoted as $A_{total} = L^2$, and the average number of points will be given by

$$\gamma = \lambda A_{total}, \tag{3.2}$$

where λ is the average rate of points per unit area; then we generate such points, within this area as Figure 3.1 shows, where we can define groups of nodes in an area determined by the coverage radius R that each node has, on the basis of its transmission power, represented by P_{T_x}.

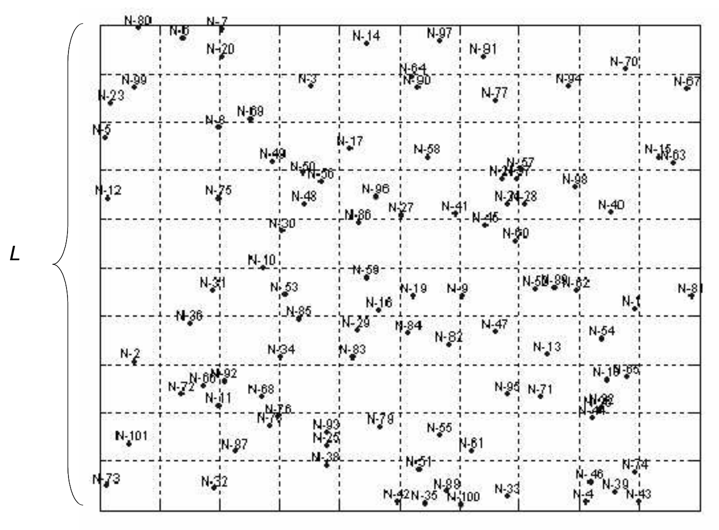

Figure 3.1: N-nodes with Poisson distribution

3.2 Virtual Cluster-based Routing Protocol (VCRP)

All the nodes in a network share the information with their neighboring nodes. Every node forms a virtual cluster with its (1-hop distant) neighbors as shown in Figure 3.3. As nodes belong to the same hierarchical layer, the effect of a Hybrid Routing Protocol (HRP) cluster can be realized, but without having to specify any node such as the cluster header. That is the reason why the local network is a "virtual cluster".

Clearly, there were as many virtual clusters as there are nodes in any network. It is due to this fact that it can significantly reduce the control overhead such as route query packets as well as the flooding time for collecting the network topology information at a destination, and efficiently carry out network management, [16].

3.2.1 Considerations to Group N-nodes within Virtual Clusters.

- The connections between pairs of nodes could be realized at h-hops maximum.

  1. Directly with another node using a single hop.
  2. Using intermediate nodes to make a connection of two or more hops.

- The "virtual cluster" radius of each node denoted by R will be determinated for a SNR acceptable for transmission. By convenience the nodes are considered equal. Figure 3.2 present the virtual cluster idea. In Figure 3.2 we can see that the coverage area of every node overlaps with other areas and therefore the virtual cluster has nodes shared with other virtual clusters, these nodes we call intermediates nodes.

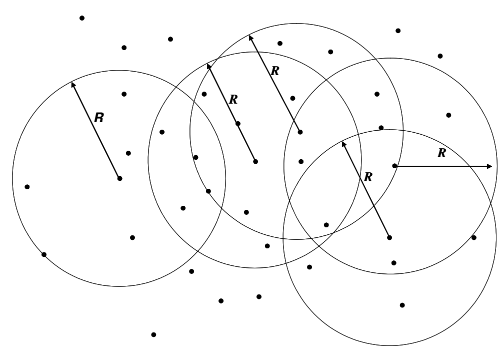

Figure 3.2: Virtual clusters formation of size R.

3.2.2 Connection between Two Nodes in a Two-Hop Trajectory.

The rules that must be fulfilled to have a link between two nodes at a distance of 2-hops are

1. The distance between node A to node B is greater than R but smaller than $2R$
2. The distance between intermediate node C to node A and node B must be smaller than R. (To see Figure 3.3).

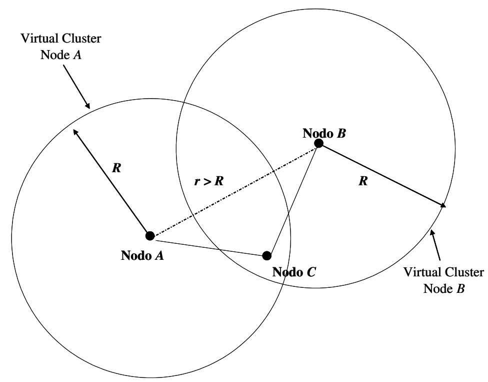

Figure 3.3: Two hops connection

3.3 Algorithm for Membership Allocation in a Virtual Cluster

Fulfilling the established conditions previously mentioned to assign membership of a node with a virtual cluster of another node, we define a matrix of the node membership as follows

$$Z = \{Membership\ 1 - hop\} = \begin{bmatrix} z_{11} & \cdots & z_{1j} \\ \vdots & \ddots & \vdots \\ z_{i1} & \cdots & z_{ij} \end{bmatrix} \tag{3.3}$$

where z_{ij} is equal to 1 if j-node belongs to i-node virtual cluster and 0 in any other case. For the power received at a node which is at a distance d from the transmitter, and with a path loss exponent α, we consider

$$P_{R_x} = P_{T_x} d^{-\alpha}. \tag{3.4}$$

If P_{R_x} is greater than a required threshold to produce a connection we assign a 1 and in any other case we assign a zero. For a membership of a node at 2-hops of distance, we define

$$H = \{Membership\ 2 - hop\} = \begin{bmatrix} h_{11} & \cdots & h_{1j} \\ \vdots & \ddots & \vdots \\ h_{i1} & \cdots & h_{ij} \end{bmatrix} \tag{3.5}$$

where h_{ij} is equal to 2 if j-node belong to i-node 2-hop neighborhood and 0 in any other case.

Successively for clustering to more hops, but with the restriction of always being member to one hop of the node that serves as bridge for the accomplishment of the connection; as in Figure 3.4.

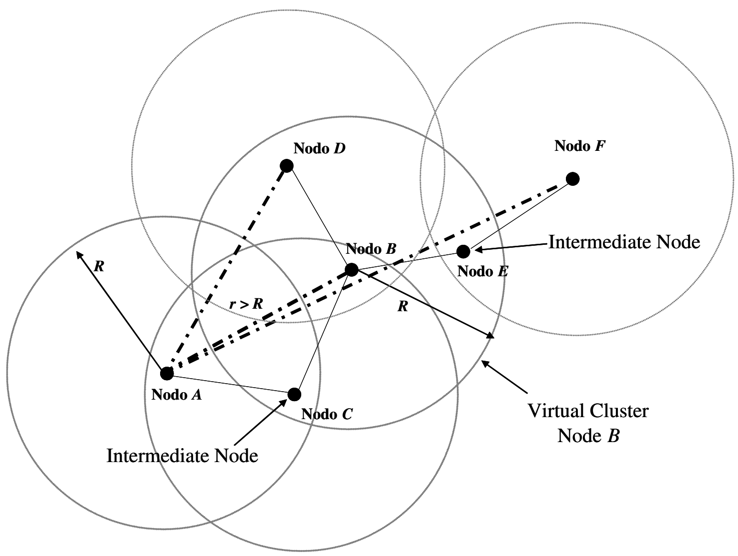

Figure 3.4: Clustering using ZRP and VCRP

3.3.1 Clustering By Distance

We consider to have connectivity based on the distance between two nodes (1-hop); since this can serve as an indicator of how the nodes are geographically distributed within the defined area as previously mentioned.

This membership allocation or clustering of the nodes serves like an approximation of the network behavior based on its connectivity and organization. Now considering a single parameter as the distance between two nodes does not show the connectivity of the node in the network; hence, propose a clustering based on minimum power threshold allocation that must receive the destination node so that the connection is completed; we call this algorithm clustering by power.

3.3.2 Clustering By Power

With a simple reasoning, we think that the link between two nodes fullfill the distance restriction, this is within R of neighboring node placed at 1-hop of it, but this does not assure us to have a good connectivity since the power of the signal received by the destination node could be below the established minimum threshold to complete the connection between these nodes, even if they are within the radius of coverage of the source node; this is due to the own effects of shadowing of the wireless channel due to environment surrounding the nodes consequently the signal that arrives at the destination node is below of the calculated as a function of the distance between these two nodes.

3.4 Log-normal Shadowing

The log-normal distribution describes the random shadowing effects which occur over a large number of measurement locations which have the same T-R separation, but have different levels of clutter on the propagation path. This phenomenon is referred to as log-normal shadowing. Simply put, log-normal shadowing implies that measured signal levels in dBs at a specific T-R separation have a Gaussian (normal) distribution about the distance, [32]. It is clear that due to random effects of shadowing, some locations within a coverage area will be below a particular desired received signal threshold. It is often useful to compute how the boundary coverage relates to percent of area covered within the boundary. This is

$$P_{R_x} = P_{T_x} d^{-\alpha}, \tag{3.6}$$

with shadowing, considering a Gaussian random variable ξ, we have

$$P_{R_x} = P_{T_x} d^{-\alpha} 10^{-\frac{\xi}{10}}. \tag{3.7}$$

3.5 Generation of Mobility and Packets

For the node mobility, we consider that each one of the nodes moves in an independent way of the others; in speed and direction. For such reasons we consider that all nodes have the possibility to move with uniform speed [0, $Vmax$], and also a direction uniformly distributed in [0, θ] as shown in figures 3.5 (a) and (b).

If the packet length in bits is represented by L_{pkt} and the link capacity is C in bps, then the required time to send a package of L_{pkt} length, will be

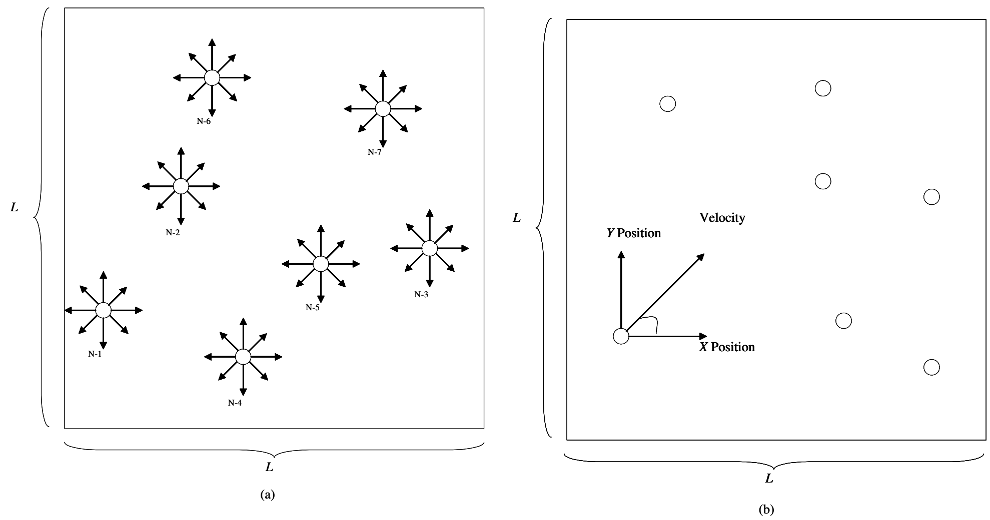

Figure 3.5: Nodes mobility in ad hoc network

$$t = \frac{L_{pkt}}{C}, \tag{3.8}$$

however, if we generate a certain number of packets in each node for its transmission with Poisson distribution, [18]; we have the required time to transmit that amount of packets as follows

$$t = \frac{L_{pkt}}{C}(\#pkts), \tag{3.9}$$

and then the distance that could move a node when transmitting a certain amount of packets will be as shown in Figure 3.6.

When every node has random values of speed and direction, we compute the rectangular components of the speed for every node as follows

$$V_x = V\sin(\theta), \tag{3.10}$$

$$V_y = V\cos(\theta), \tag{3.11}$$

where V_x, is the rectangular component of the velocity vector of every node, V_y is the rectangular component of the velocity vector of every node and θ is the direction of every node. We know the displacement of the node in the "x" and "y" axis of the following form

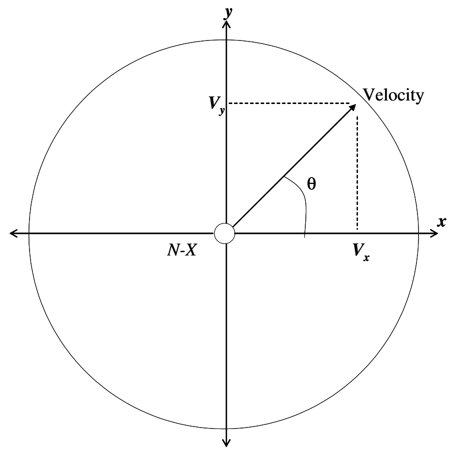

Figure 3.6: Node Mobility from its starting point

$$d_x = V_x t, \quad (3.12)$$

$$d_y = V_y t, \quad (3.13)$$

and therefore the new position by the node will be given of the following form, (see Figure 3.7)

$$Pos(x)_{new} = X_{original} + d_x, \quad (3.14)$$

$$Pos(y)_{new} = Y_{original} + d_y. \quad (3.15)$$

where $X_{original}$ is the actual coordinate in axis x, $Y_{original}$ is the actual coordinate in the axis y, $Pos(x)_{new}$ is the new coordinate in x for every node and $Pos(y)_{new}$ is the new coordinate in y for every node.

3.6 Types of Connectivity

As discussed in Section 2.5, the connectivity can give us a representation of the behavior of the nodes that interact in an ad hoc network, but now, we define new classes of connectivity more specifically; with the purpose of analyzing thoroughly and in a more realistic form the behavior of the ad hoc network. In the following section the connectivity classes are explained in detail to analyze the network and its topology changing

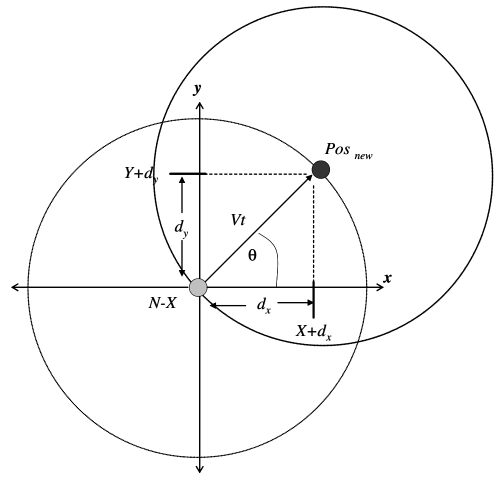

Figure 3.7: Shift of position of a node in a Ad hoc network

along the time and only for evaluation purposes in Figure 3.8 we show the algorithm that describes step by step the procedure followed to evaluate the ad hoc network; where i is the origin node, j is the destination node, L is the length of data packet, λ_{pkt} is the rate of packet generated for every node, d is the distance between the nodes i and j, C_MEMBER(i,j), C_MEMBER_2hop(i,j), C_MEMBER_3hop(i,j), C_MEMBER_4hop(i,j) and the arrays C_MEMBER_POT(i,j), C_MEMBER_POT_2h(i,j), C_MEMBER_POT_3h(i,j), C_MEMBER_POT_4h(i,j) are matrix of membership of nodes to 1, 2, 3 and 4 hops by distance and power respectively. With the information obtained we can make an analysis of each data and obtain fair interpretations.

3.6.1 Absolute Connectivity of Each Node.

The connectivity that we called absolute connectivity for each node represents how any node is connected to all the network or with other nodes at a specific moment in time. Let $\zeta_n(N_x, k)^h_{abs}$ be the absolute connectivity to h-hops at an instant of time; and $C(N_x, k)^h_{pot}$ be the amount of nodes reached by the origin node to h-hops considering the power level that receives the destination node. Let H_{max} be the maximum number of hops to which the origin node can connect to the destination node, N_{tot} be the total number of nodes in the ad hoc network, N_x be the origin node, k be the kth time slot in which the sample is taken and n pattern the variable normalized with respect to N_{tot}, then we have the following definition,

$$\zeta_n(N_x, k)^1_{abs} = \frac{1}{N_{tot}} C(N_x, k)^1_{pot}, \tag{3.16}$$

$$\zeta_n(N_x,k)^2_{abs} = \frac{1}{N_{tot}} C(N_x,k)^2_{pot}, \tag{3.17}$$

generalizing

$$\zeta_n(N_x,k)^h_{abs} = \frac{1}{N_{tot}} C(N_x,k)^h_{pot}, \;\; h = 1,2,\ldots,H_{max} \tag{3.18}$$

where $C(N_x,k)^h_{pot}$ considering $i = x$ is define,

$$C(N_i,k)^1_{pot} = \sum_{j=2}^{N_{tot}} z_{ij} \tag{3.19}$$

$$C(N_i,k)^2_{pot} = \sum_{j=2}^{N_{tot}} \frac{h_{ij}}{2} \tag{3.20}$$

successively to more hops,

$$C(N_i,k)^h_{pot} = \sum_{j=2}^{N_{tot}} \frac{matrix\ indicator\ membership(i,j)}{h} \quad h = 1,2,\ldots,H_{max} \tag{3.21}$$

Equation (3.18) represents in a general way the absolute connectivity of every node at a specific moment in time with respect to all node population that exists in the ad hoc network. If we consider only 1-hop for analyzing the absolute connectivity that a node has at any moment in time this will not represent the real potential connectivity value of the node.

We consider important to explain that if a node is linked to a 1-hop node, the former will not be linked to 2, 3, or h-hop and similarly if a node is linked to h-hop. With this consideration we ensure that the route selected to link any pair of nodes is the smallest in number hops.

3.6.2 Network Connectivity to h-hops

Having already defined what the absolute connectivity of a node is, now we calculate the connectivity of all the ad hoc network of a specific moment in time, as a function of the absolute connectivities of each node at these moment in time to h-hop, as follows

$$\zeta_n(W,k)^1 = \frac{1}{N_{tot}} \sum_{x=1}^{N_{tot}} C(N_x,k)^1_{pot}, \tag{3.22}$$

$$\zeta_n(W,k)^2 = \frac{1}{N_{tot}} \sum_{x=1}^{N_{tot}} C(N_x,k)^2_{pot}, \tag{3.23}$$

generalizing

$$\zeta_n(W,k)^h = \frac{1}{N_{tot}} \sum_{x=1}^{N_{tot}} C(N_x,k)^h_{pot}, \tag{3.24}$$

where $\zeta_n(W,k)^h$ is the normalized connectivity of the ad hoc network in a time slot to h-hops, W represents the ad hoc network, k is the kth time slot, N_x is the origin node and n is pattern the variable normalized.

3.6.3 Average Connectivity of each Node to h-hops in time.

We consider that it is not sufficient to know the connectivity at a moment in time, since the nodes present mobility. Then, we consider important to analyze the behavior of each node with its history of connectivity by using a time average the following way

$$\zeta_n(N_x,k) = \frac{1}{k} \sum_{s=1}^{k} C(N_x,s)^h_{pot}, \;\; h = 1, 2, \ldots, H_{max} \tag{3.25}$$

where k is the time slot, $\zeta_n(N_x,k)$ is the average connectivity normalized.

3.6.4 Total Absolute Connectivity of the Network by Power

As defined in Section 3.6.1, the absolute connectivity of each node must be analyzed to h-hop and now we define a new parameter that indicates us the total absolute connectivity of each node. This new connectivity is represented as follows;

$$\zeta(N_x,k)^T_{abs} = C(N_x,k)^1_{pot} + C(N_x,k)^2_{pot} + C(N_x,k)^3_{pot} + \cdots + C(N_x,k)^{H_{max}}_{pot} \tag{3.26}$$

where; $\zeta(N_x,k)^T_{abs}$ is the Total Absolute connectivity of a node by power at time slot k.

If we want to know the total absolute connectivity that a node has with respect to all the network, we only average the value of the total absolute connectivity in (3.26) with respect to N_{tot}, as follows

$$\zeta_n(N_x,k)^T_{abs} = \frac{1}{N_{tot}} \zeta(N_x,k)^T_{abs}, \tag{3.27}$$

therefore average the total absolute connectivity of the network at a moment in time is given by

$$\zeta_n(W,k)^T_{abs} = \frac{1}{N_{tot}} \sum_{x=1}^{N_{tot}} \zeta_n(N_x,k)^T_{abs}. \tag{3.28}$$

3.6.5 Total Absolute Connectivity of each Node by Power in time

Of similar form to the average connectivity concept of each node to h-hops, considering the history of the node through time, we would like to know the behavior the network based on the past time.

Taking from total absolute connectivity of a node Equation (3.27),

$$\zeta_n(N_x, k)^T_{abs} = \frac{1}{N_{tot}} \zeta(N_x, k)^T_{abs}, \tag{3.29}$$

we have

$$\zeta_n(N_x, k)^T_{abs} = \frac{1}{k} \sum_{s=1}^{k} \zeta_n(N_x, s)^T_{abs} = \frac{1}{k} \frac{1}{N_{tot}} \sum_{s=1}^{k} \sum_{h=1}^{H_{max}} C(N_x, s)^h_{pot}. \tag{3.30}$$

3.7 Virtual Cluster Fragility

Following the idea to analyze the connectivity of each node within the ad hoc network, in this section we propose the analysis of the virtual cluster robustness as a function of the amount of nodes that each virtual cluster is linked to.

The main idea in this topic is to propose a new parameter that represents to us during a time, how the virtual cluster was conformed and his tendency to divide. We call this new parameter “fragility”.

The fragility that we propose is defined by the amount of nodes linked to h-hops and the total alternative routes to the nodes linked and this parameter is obtained as follows

$$\Im(x) = \frac{\sum_{s=1}^{k} C(N_x, s)^h}{\sum_{s=1}^{k} \Re(N_x, s)}, \; h = 2, \ldots, H_{max}, \tag{3.31}$$

where $\Re(N_x, s)$ is the amount of routes that exist to reach all nodes link by a node or virtual cluster to h-hops in the kth time slot and $C(N_x, s)$ is defined before.

An example is shown in figures 3.9 and 3.10; where node A is the virtual cluster to analyze. In Figure 3.9, node A has more nodes within R but they are at the same time linked to other nodes and they have nodes linked in common which means that there exist alternative routes with the same hop number and consequently a major possibility to maintain the link with these node and the value of fragility is low; while for that in Figure 3.10, node A shows only link to the other nodes without alternative routes, this

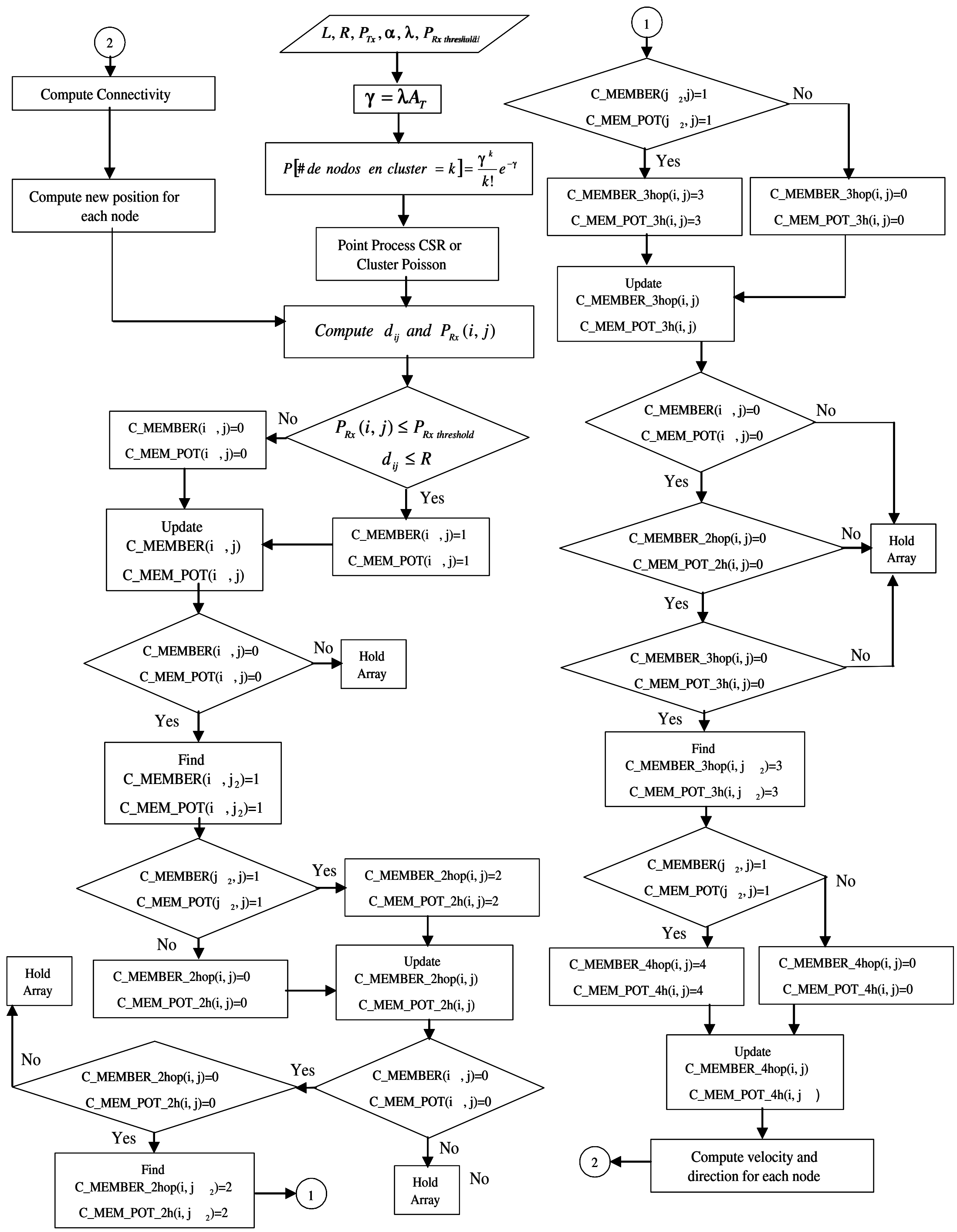

Figure 3.8: Algorithm evaluation of the ad hoc network

virtual cluster configuration shows us that the probability of changing the virtual cluster configuration is very high in time, as a result the fragility of the virtual cluster is high too.

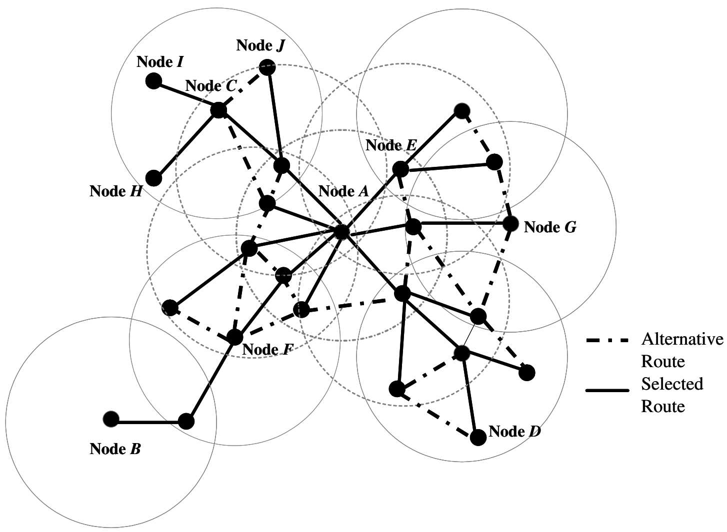

Figure 3.9: Virtual Cluster Fragility, with low fragility

Now that we defined the new parameters, the follow step is obtain results of the simulation and manipulate this statistic as we discussed in sections past. The result obtained with this parameters are shows in the Chapter 4 in tables and graphs. The main objective of this parameters are evaluate the ad hoc networks as a function of their nodes using the different types of connectivity and the organization using the fragility parameter.

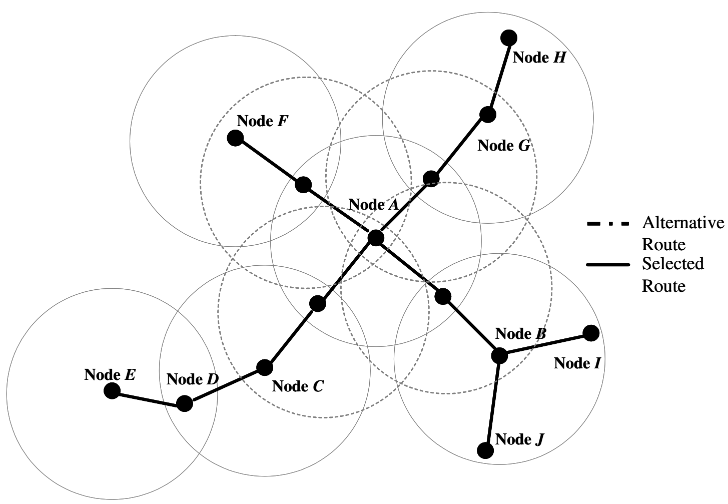

Figure 3.10: Virtual Cluster Fragility, with high fragility

Chapter 4

Numerical Results

This chapter shows the results of the simulation of the ad hoc network using the ideas of ZRP and VCRP. The parameters and considerations made in the simulation of the algorithm and the network are also shown. The simulation scenario and the results obtained are presented on charts, and the behavior of the new parameters as well.

4.1 Simulation

The simulation was carried out using MATLAB. In all scenarios, the links are selected consider the $P_{Rxthreshold}$ in each node for the case where we analyze the network as a function of the power received and the other case is when the links are function of distance within a virtual cluster; i.e., the node is within the coverage radius; furthermore the routes with minimum hop number are selected.

All the nodes transmit with the same power level in all scenarios, they move independently with different velocities and direction. The study area is the same in all scenarios and we use the ping-pong nobility model in the nodes so that they remain within this area as shown in Figure 4.1.

The characteristics of the nodes and parameters used in tha different scenarios of the simulations are presented in tables 4.1 and 4.2. Where L is the fixed length of the data packet, λ_{pkt} is the arrival rate of packets with Poisson distribution, C is the channel capacity, P_{Tx} is the transmission power of very node, R is the maximum transmission radius of every node, V_{max} is the maximum speed that reach every node with uniform distribution and $P_{threshold}$ is the minimum received power at a distance of R with a path loss exponent equal to 4.

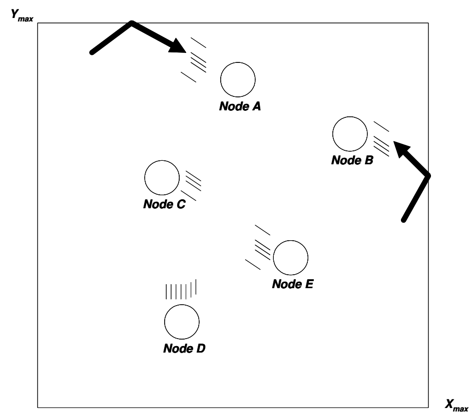

Figure 4.1: Closed coverage area

Table 4.1: Node Parameters of Simulation

Transmission power (P_{Tx})	5e-3 w
Minimum received power ($P_{threshold}$)	9.876e-12 w
Data Packet Length (L)	18496 bits
Maximum Transmission Radius (R)	150 mts
Maximum Node Speed (V_{max})	5 $\frac{mts}{sec}$

Table 4.2: Network Traffic Parameters

Simulation Time	3600 sec
Packet Arrival Rate per Node (λ_{pkt})	100 $\frac{packets}{sec}$
Service Packet Rate (C)	2 Mbps

4.1.1 General Scenario

All nodes are randomly distributed on a grid X_{max} by Y_{min} as shown in Table 4.3. In addition, the nodes generate packets in order to know the mobility that could exist in each node if they desire to transmit the packets. As a result we have a change in the topology of the ad hoc network, as discussed in Chapter 3.

4.1.2 Nodes Population Scenarios

Three node population are considered for this simulation. As already mentioned, the nodes in the scenarios have independent mobility with respect to others; each node moves with variable velocity between [0,V_{max}] as shown in Table 4.1 and an angle [0,360°].

In each scenario the nodes are set up randomly into the area according to a Complete Spatial Randomness (CSR).The first scenario is considered with a low node population because in this scenario the node number is of 25 nodes or ($\gamma = 0.000025\frac{nodes}{mts^2}$). Figures 4.2 and 4.3 presents the initial network topology for this scenario. Figure 4.2 shows the links connecting those nodes that are within the transmission radios R of each other. Figure 4.3 shows the links connecting those that receive the power P_{Rx} calculated with Equation 3.7.

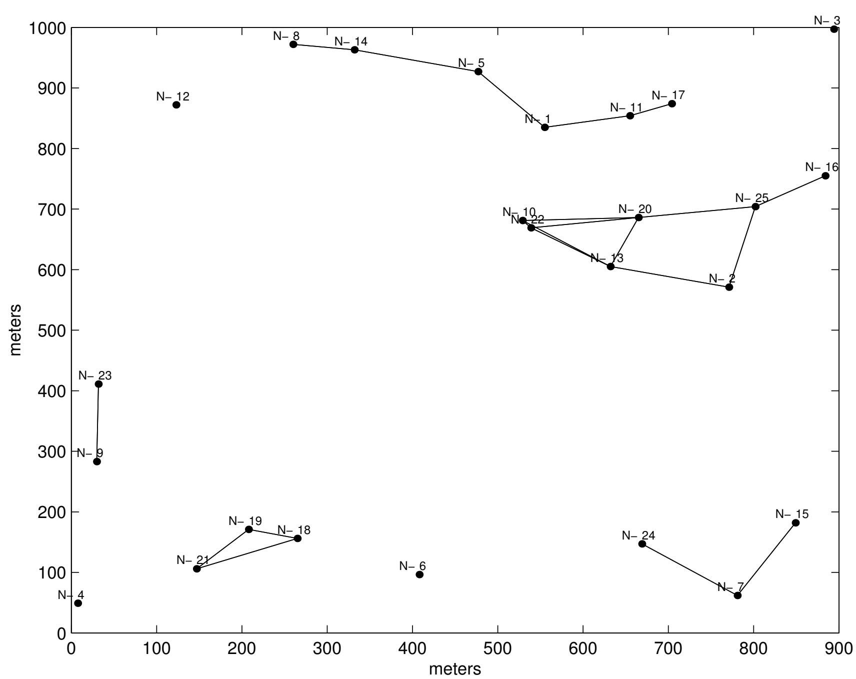

Figure 4.2: Initial scenario with 25 nodes and link d_{ij} ≤R

Table 4.3: Environment Scenario Specifications

Node Population (N_{tot})	25, 50, 100 nodes
Coverage Area (X_{max} x Y_{min})	1000 x 1000 mts
Path Loss Exponent (α)	4
Maximum hop number (H_{max})	4 hops
Log-Normal Shadowing	$N \sim (m = 0, \sigma = 8)$

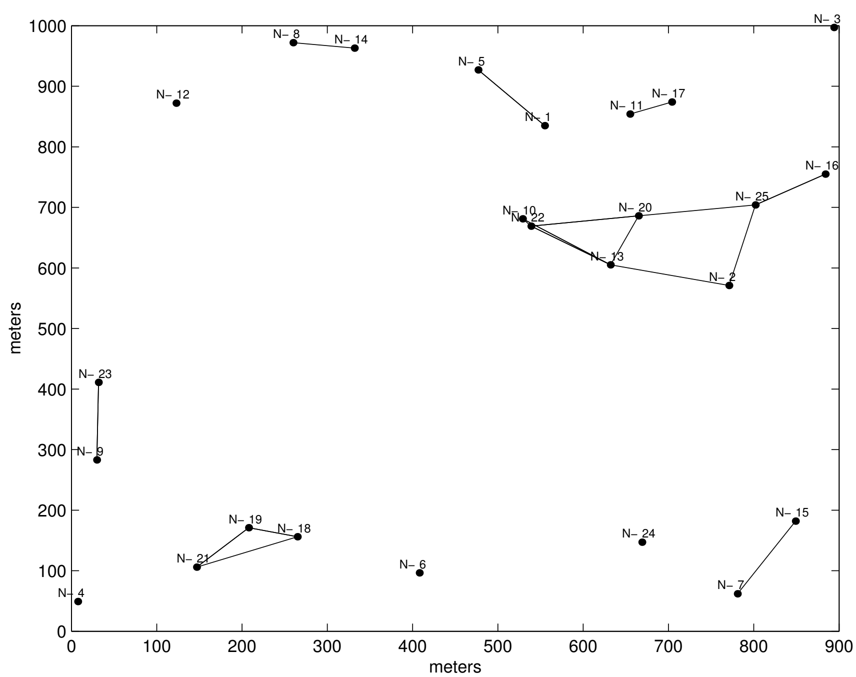

Figure 4.3: Initial scenario with 25 nodes and link $P_{threshold} \leq P_{Rx}$

The second scenario we considered increase the node population to 50 nodes ($\gamma = 0.00005 \frac{nodes}{mts^2}$) ; the Figure 4.4 and 4.5 presents the initial network topology in this case. At first sight we can see that the nodes are more distributed in all the region obtained as a result greater probability of reach minimum to one node. Figure 4.4 shows the links connecting those nodes that are within the transmission radios R of each other. Figure 4.5 shows the links connecting those that receive the power P_{Rx} calculated with Equation 3.7.

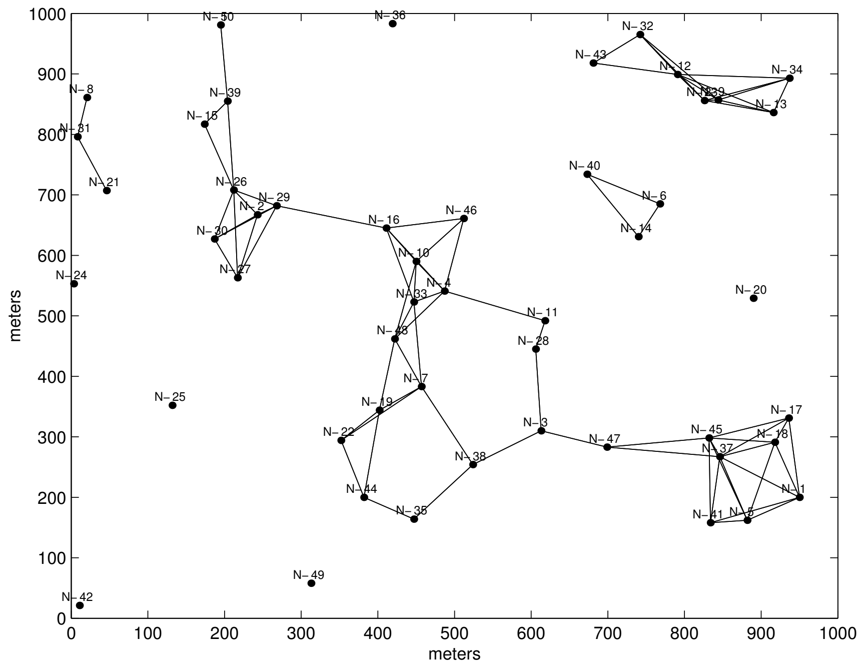

Figure 4.4: Initial scenario with 50 nodes and link $d_{ij} \leq$R

The third scenario we increase again the node population to 100 nodes ($\gamma = 0.0001 \frac{nodes}{mts^2}$); the Figures 4.6 and 4.7 presents the start network topology for this case. As we can see the network is better connected that the other case in both consideration without forgot that the connectivity is below when the connectivity is analyzing considering the power levels received in every node.Figure 4.6 shows the links connecting those nodes that are within the transmission radios R of each other. Figure 4.7 shows the links connecting those that receive the power P_{Rx} calculated with Equation 3.7.

In all scenarios every node updates its position according to update periods. Every second all nodes update their position. The value samples to analyze the ad hoc network mobility and connectivity are taken every five seconds of simulation time. At the end of the simulation the nodes will be in a different position from the one in which they started.

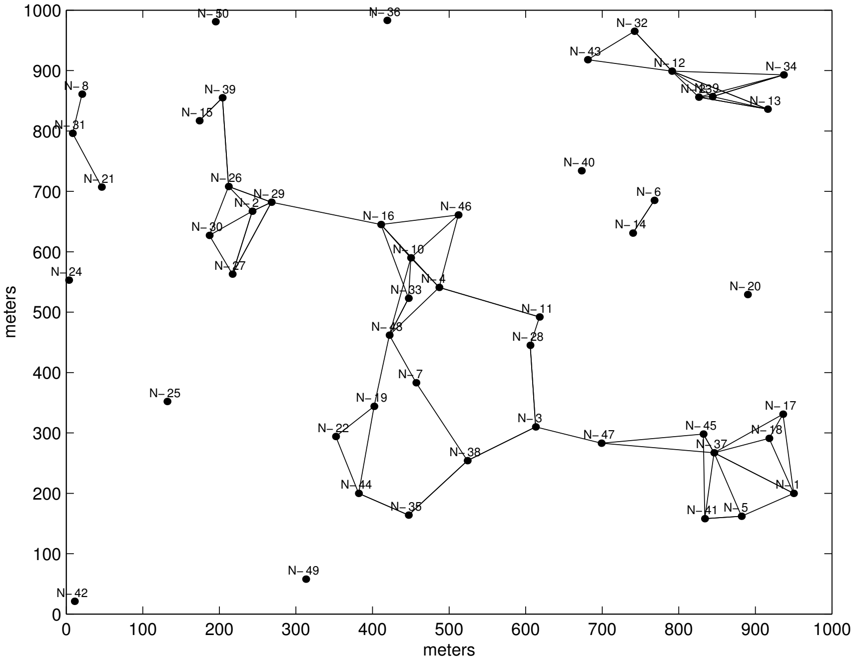

Figure 4.5: Initial scenario with 50 nodes and link $P_{threshold} \leq P_{Rx}$

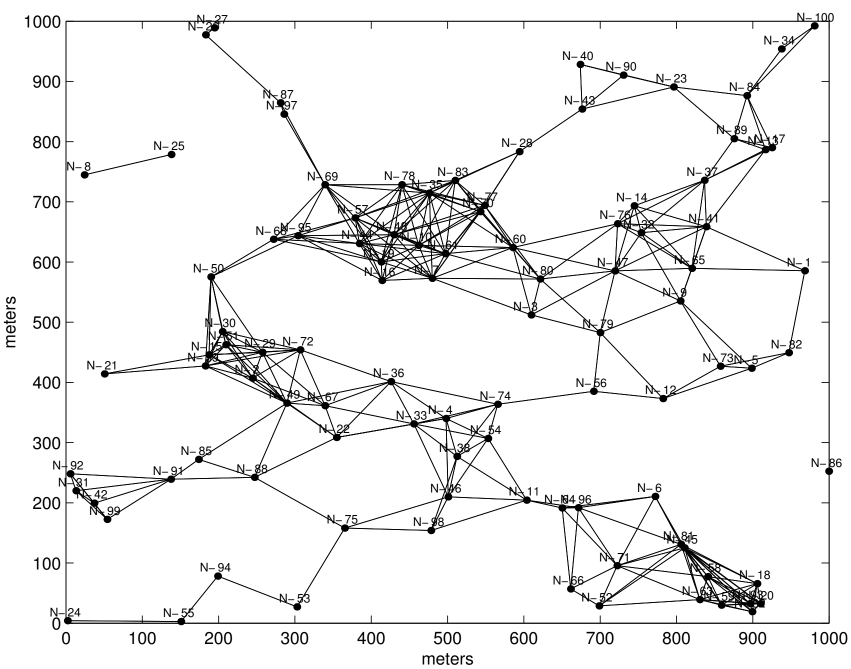

Figure 4.6: Initial scenario with 100 nodes and link $d_{ij} \leq R$

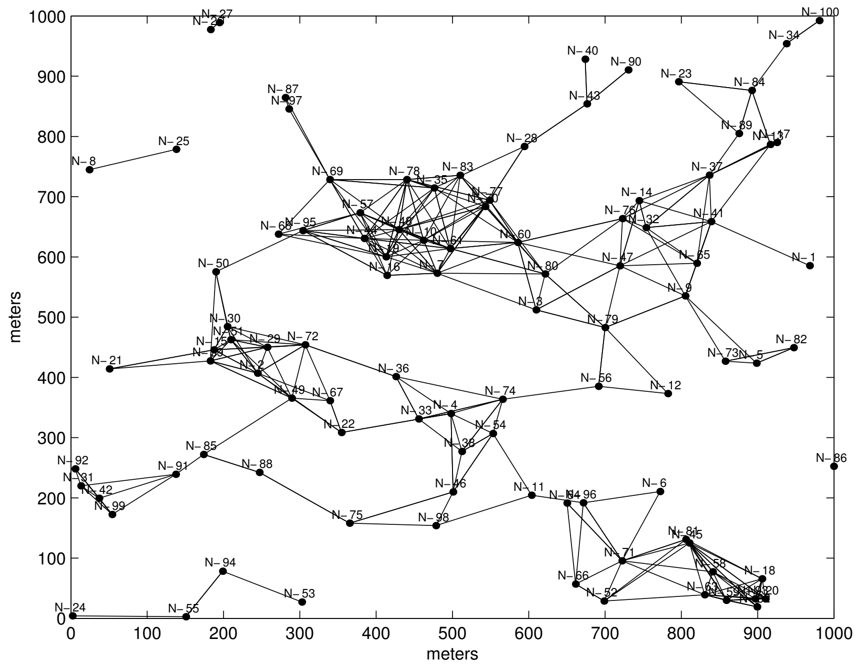

Figure 4.7: Initial scenario with 100 nodes and link $P_{threshold} \leq P_{Rx}$

Figures 4.8, 4.9, 4.10, 4.11, 4.12 and 4.13 present the node positions after 3600 sec with links considering the distance between nodes and power level received for every node. In these figures we observe that the nodes have the tendency to build "clusters" conformed as the time elapses. This node behavior in some case could benefit performance because if the node population is high the connectivity is increased.

4.2 Analyzing Node Connectivity

This section presents the average connectivity results for every virtual cluster. Recall that the average connectivity is the amount average of nodes that a node linked to h-hop in all time of simulation and is given by Equation 3.25. For the case where the node population is 25 we see that the connectivity to 1-hop considering the distance and the power level received is better than the connectivity to 2, 3 and 4 hops. We see the curves behaviors that are very similar for these cases as shown in figures 4.14 and 4.15.

For the case where the node population is increased to 50 nodes for the same conditions, we see obviously an increase in the average connectivity for every virtual cluster and we see that again the curve behaviors are similar, but now the average connectivity to 2,

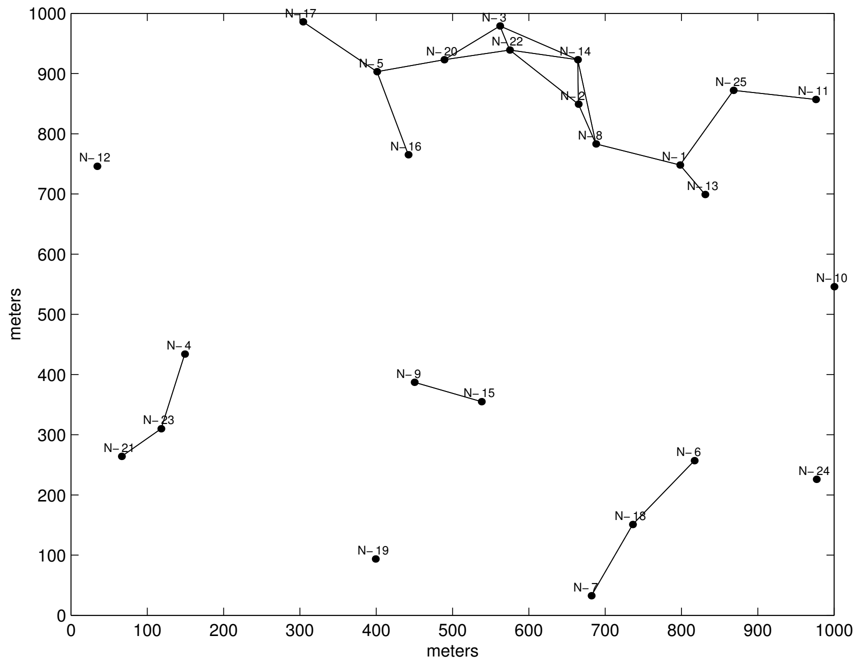

Figure 4.8: Final scenario with 25 nodes and link $d_{ij} \leq$R

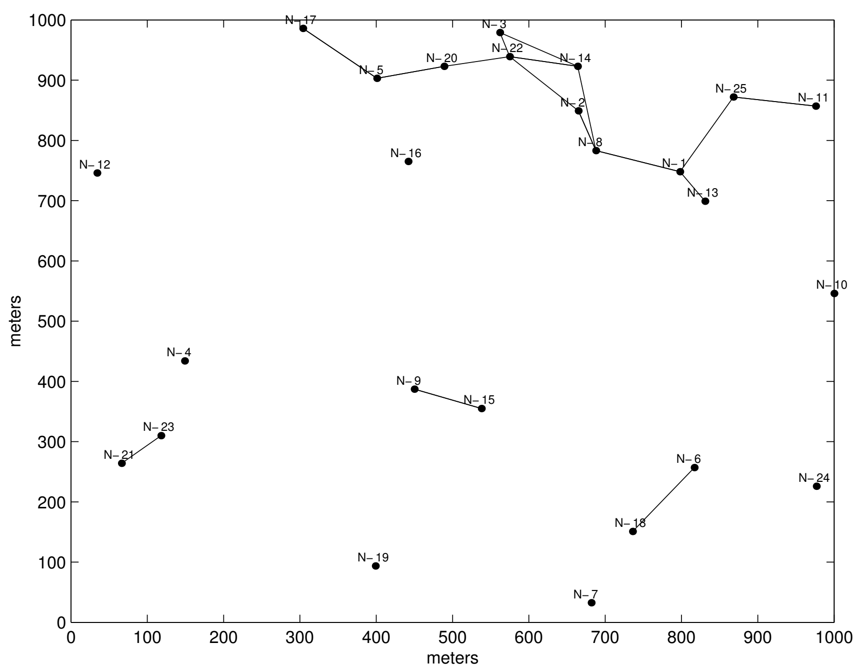

Figure 4.9: Final scenario with 25 nodes and link $P_{threshold} \leq$P$_{Rx}$

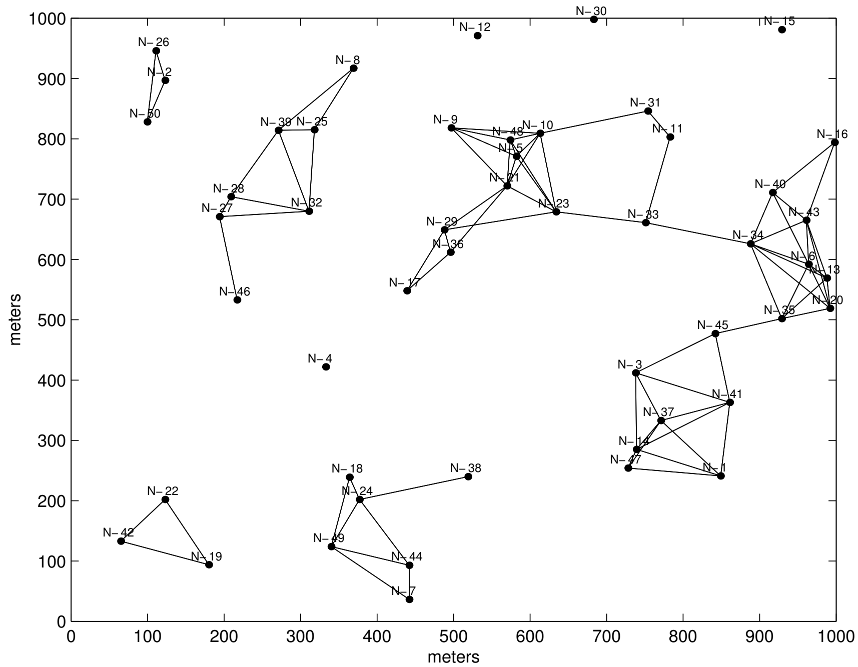

Figure 4.10: Final scenario with 50 nodes and link $d_{ij} \leq$R

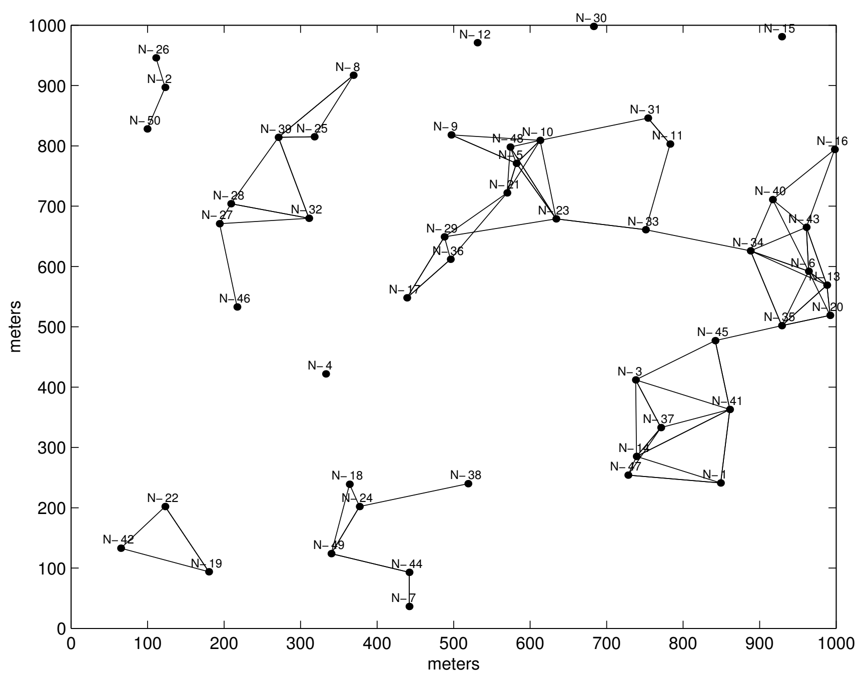

Figure 4.11: Final scenario with 50 nodes and link $P_{threshold} \leq$P$_{Rx}$

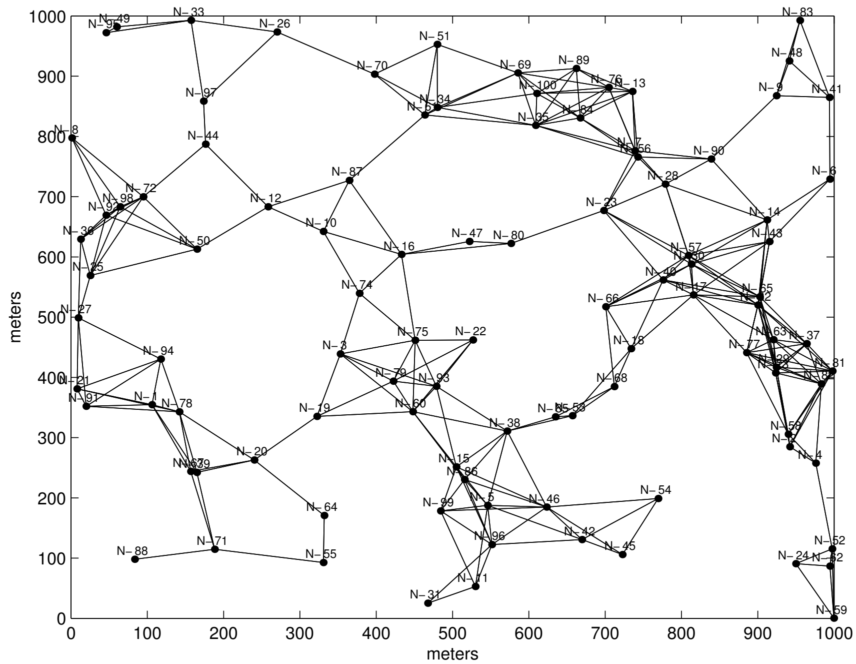

Figure 4.12: Final scenario with 100 nodes and link d_{ij}≤R

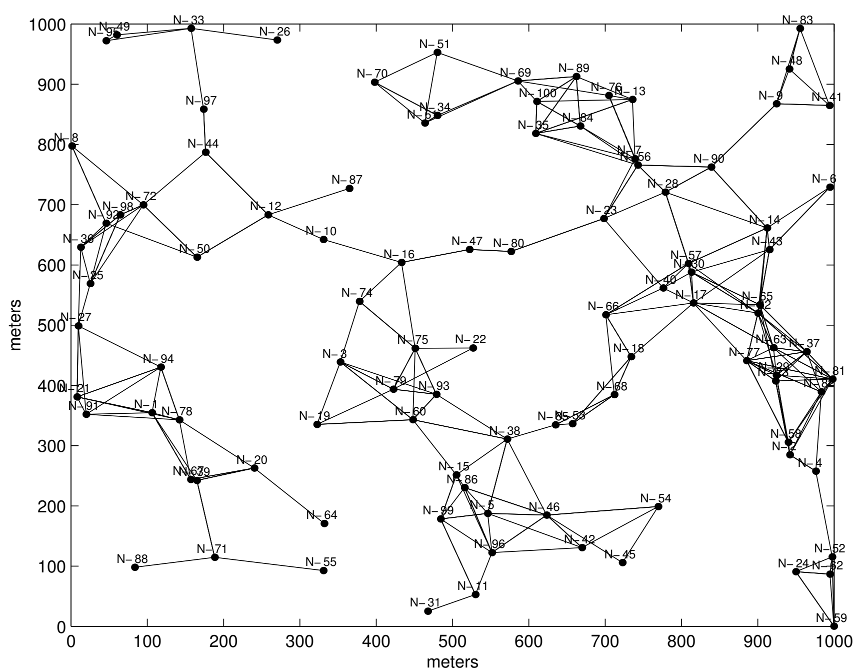

Figure 4.13: Final scenario with 100 nodes and link $P_{threshold}$≤P$_{Rx}$

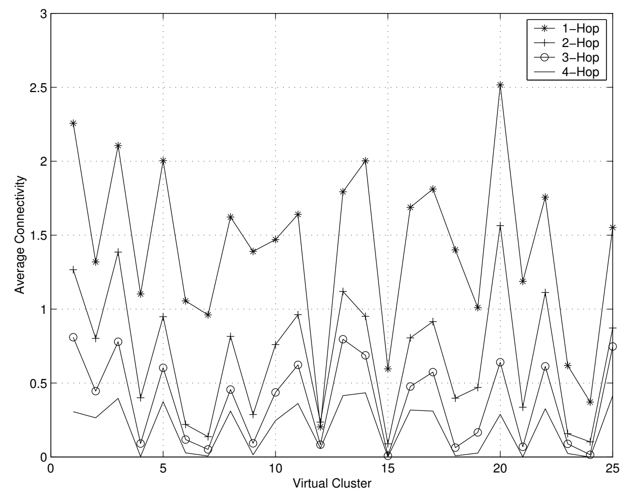

Figure 4.14: Average Connectivity with $N_{tot} = 25$ and link $d_{ij} \leq$R

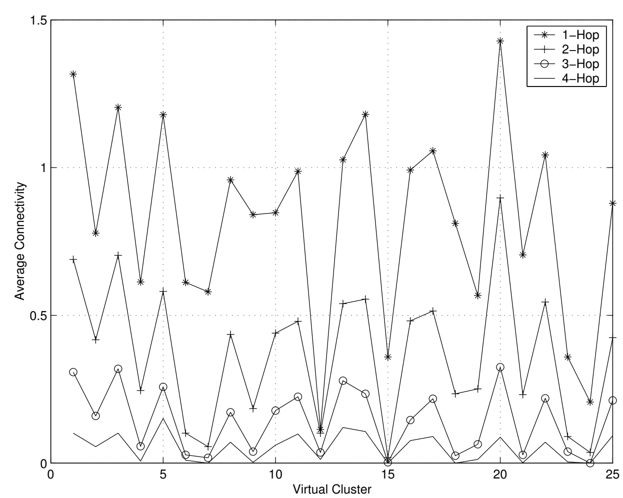

Figure 4.15: Average Connectivity with $N_{tot} = 25$ and link $P_{threshold} \leq$P$_{Rx}$

3 and 4-hops is increase to similar level as the average connectivity to 1-hop because the node neighbor number to 1-hop is greater for every node and as a result a virtual cluster will reach other virtual cluster obtaining in some cases better average connectivity to 2 and occasionally to 3 and 4 hops, but this is only for the case where the distance is considered as show in Figure 4.16. For the case where the power levels received are considered, Figure 4.17 presents the average connectivity to 2-hop better than 1-hop in the majority of virtual clusters. But the curve behaviors again are similar and the average connectivity to 3-hop generally is below the average connectivity to 1-hop and 2-hop. The average connectivity for 4-hop in this scenario is the lowest in all the virtual clusters.

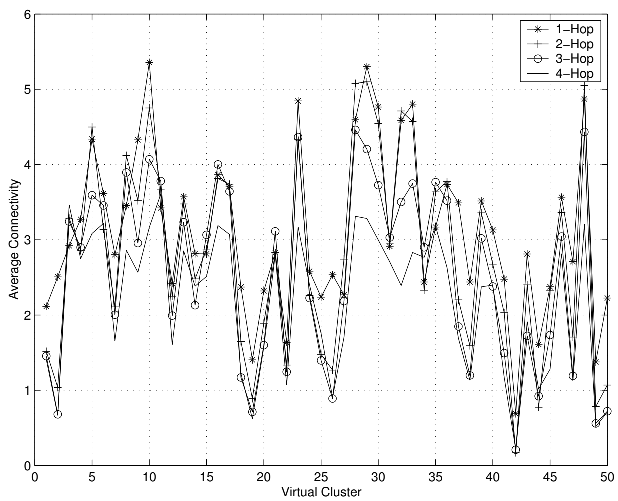

Figure 4.16: Average Connectivity with $N_{tot} = 50$ and link $d_{ij} \leq$R

Finally, in the case of the node population of 100 nodes, the average connectivity is around 6 nodes linked to 1-hop considering the distance as shown in Figure 4.18. This scenario presents an important increment in the average connectivity to 4-hop and 3-hop and now the average connectivity to 1-hop is generally the lowest and the highest is to 4-hop. For the case where the power levels received are considered Figure 4.19 presents a similar behavior to that of Figure 4.18 but the difference between 1-hop curve and the other is more visible. Tables 4.4 indicate the average of connectivity.

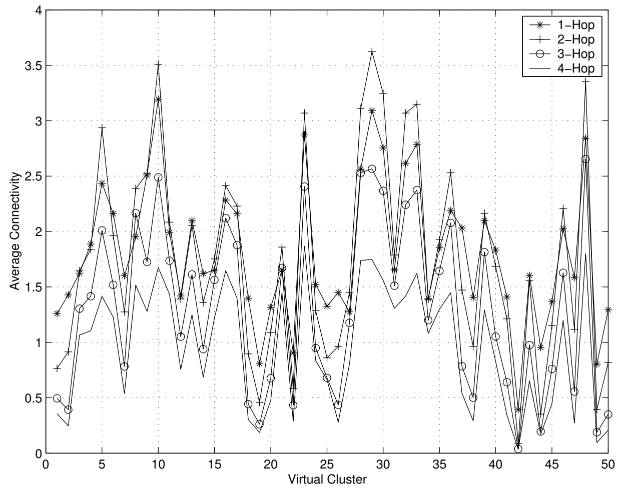

Figure 4.17: Average Connectivity with $N_{tot} = 50$ and link $P_{threshold} \leq P_{Rx}$

Table 4.4: Average of Connectivity

Node	d_{ij}≤R				$P_{threshold}$≤P_{Rx}			
Population	1-hop	2-hop	3-hop	4-hop	1-hop	2-hop	3-hop	4-hop
25	1.41	0.68	0.38	0.19	0.82	0.37	0.14	0.05
50	3.11	2.79	2.52	2.17	1.80	1.75	1.29	0.94
100	5.93	7.26	8.86	10.20	3.45	5.09	5.23	5.50

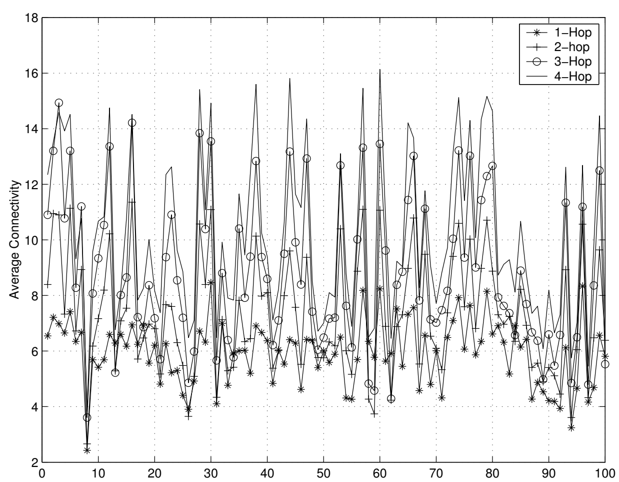

Figure 4.18: Average Connectivity with $N_{tot} = 100$ and link d_{ij}≤R

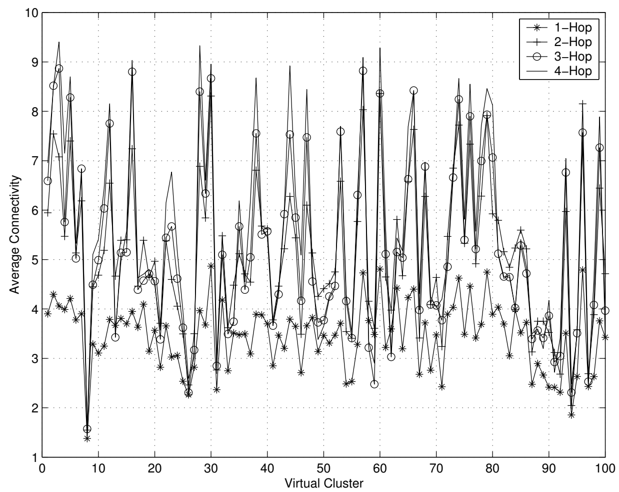

Figure 4.19: Average Connectivity with $N_{tot} = 100$ and link $P_{threshold} \leq P_{Rx}$

4.3 Analyzing Network Connectivity to h-hops

Recall that network connectivity is defined as the connectivity of all the ad hoc network in a specific moment time to h-hop and is given by Equation 3.24. In Figures 4.20, 4.21 the behavior that present the network connectivity to 1-hop in all scenarios in time is very similar and the values are approximately twice as much as those of the scenario before for both considerations and the network connectivity to 1-hop in the case where the node population is equal to 100 nodes is decreased slowly in time.

In figures 4.22, 4.23, 4.24 and 4.25 show us again a behavior similar but now the graph that pattern the network connectivity to 2-hop of 50 nodes is increase in time while the graph that pattern the network connectivity of 100 follow decrease slowly in time. The behavior is very similar in Figures 4.26 and 4.27 but in this; the graph values with 50 nodes are very approximate to the graph with 100 nodes in some case.

4.4 Analyzing Total Absolute Connectivity of the Network

Recall that total absolute connectivity of the networkis defined as the sum of the network connectivity in a specific time until H_{max} normalized and is given by Equation 3.28. Figures 4.4 and 4.29 show the behavior of the total absolute connectivity for 25,50 and 100 nodes.

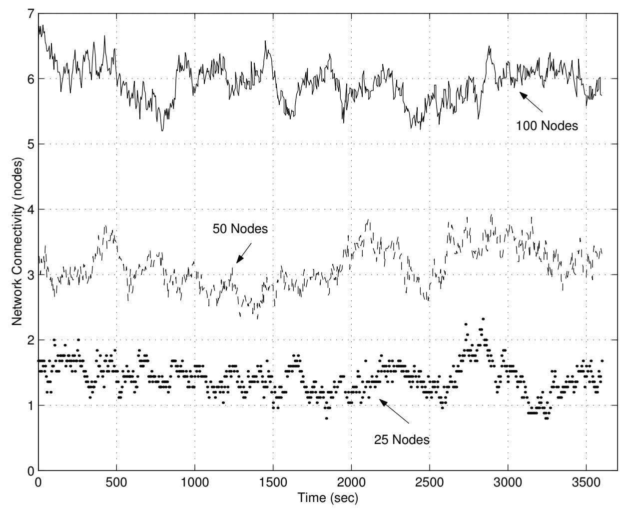

Figure 4.20: Network Connectivity to 1-hop and link $d_{ij} \leq$R

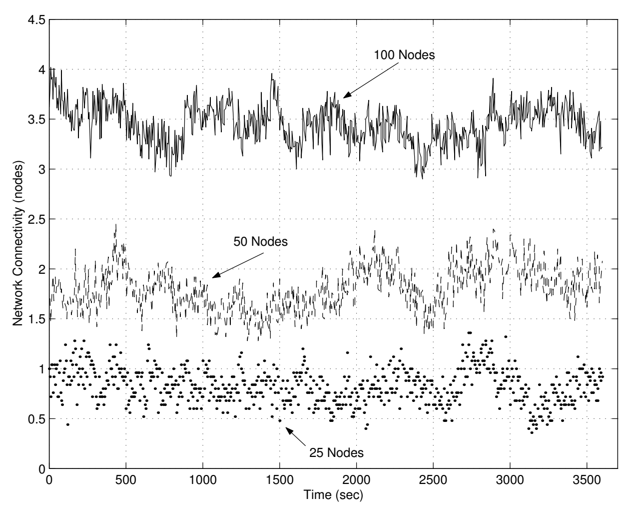

Figure 4.21: Network Connectivity to 1-hop and link P$_{threshold} \leq P_{Rx}$

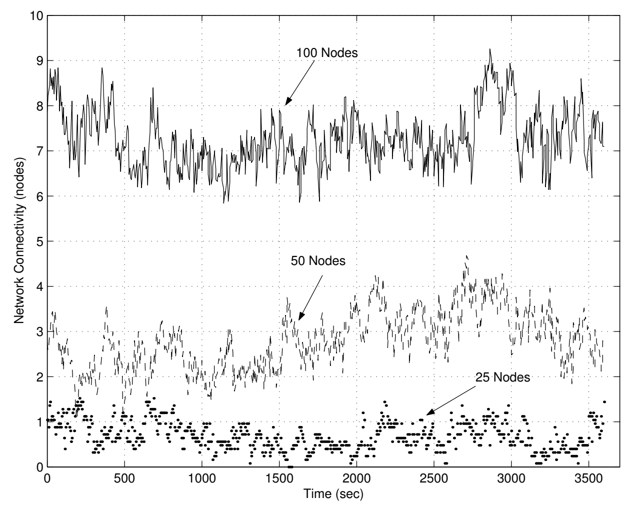

Figure 4.22: Network Connectivity to 2-hop and link $d_{ij} \leq$R

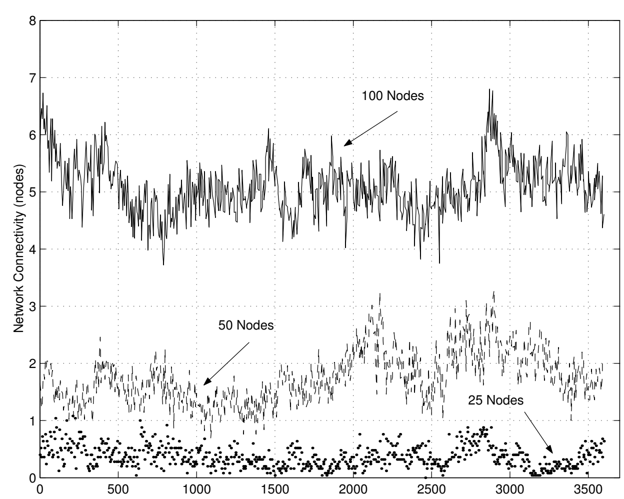

Figure 4.23: Network Connectivity to 2-hop and link P$_{threshold} \leq P_{Rx}$

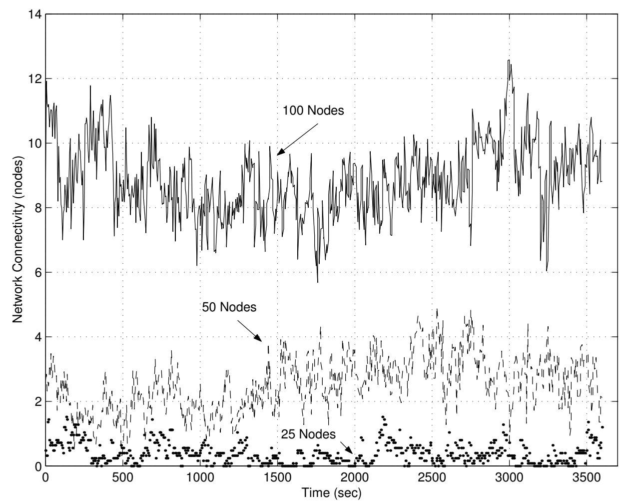

Figure 4.24: Network Connectivity to 3-hop and link $d_{ij} \leq$R

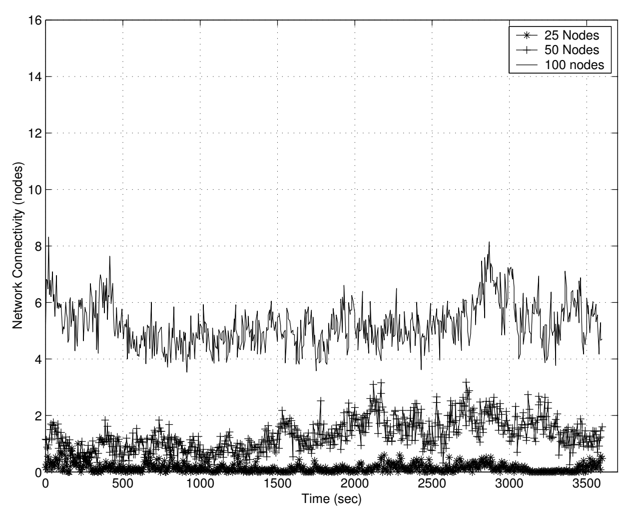

Figure 4.25: Network Connectivity to 3-hop and link P$_{threshold} \leq P_{Rx}$

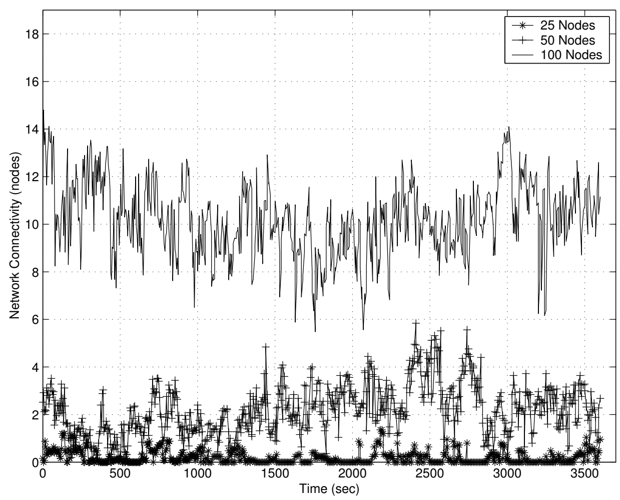

Figure 4.26: Network Connectivity to 4-hop and link $d_{ij} \leq$R

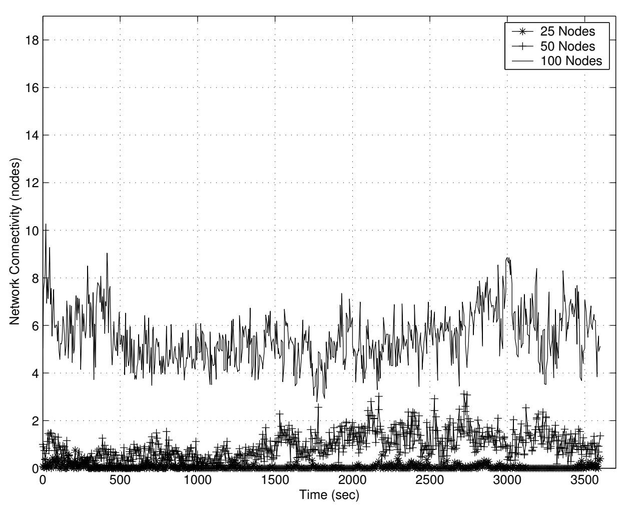

Figure 4.27: Network Connectivity to 4-hop and link $\mathrm{P}_{threshold} \leq P_{Rx}$

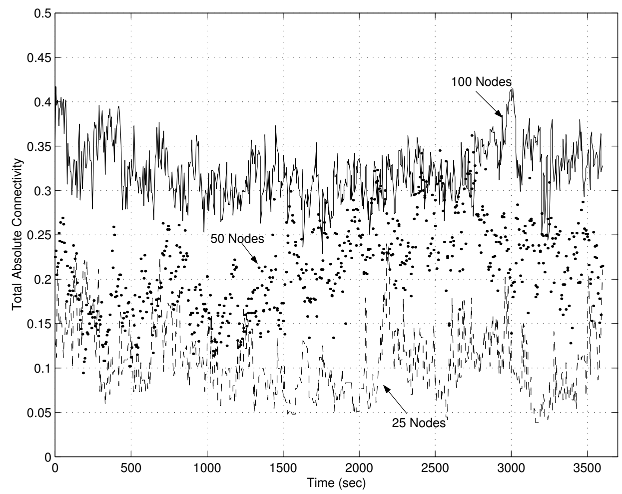

Figure 4.28: Total Absolute Connectivity considering d_{ij}≤R

With the objective to observe in a better form the behavior of the connectivity and compare it with all cases, we obtain the empirical CDFs and its corresponding histograms standardized on the samples taken from the simulation as shown in Figures 4.30 and 4.31.

Both figures show us a similar behavior in particular Figure 4.30 presents a greater probability of having total absolute connectivity value in the network in all case proposed in this simulation than the values shown in Figure 4.31; the total absolute connectivity in both considerations for 25 nodes increase rapidly until reach the probability of 1; for the cases when the node porpulation are 50 and 100 the empirical CDFs values increase more slowly when the values of the total absolute connectivity are increased. Trying to analyze the behavior in each case we presents the histograms standardized in figures 4.32 and 4.33.

Now that we have the histograms the idea of observe the behavior is more clear because in this graphs we see that the worst case of connectivity is when the node population is low and the network has a probability high of being disconnected all the time, while the node population is increase the network probability of being disconnected start to decrease and present a maximum value of total absolute connectivity when the node population is equal to 100 and we observe in this curve that the values are around of the mean. Is important explain that the histogram where the power levels received in every node are considered for realized the links the total absolute connectivity probabilities of the network are decrease faster than the histogram where the distance only is considered.

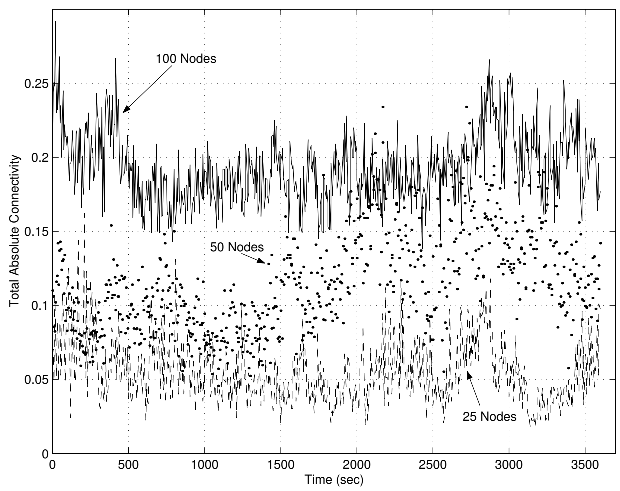

Figure 4.29: Total Absolute Connectivity considering $P_{threshold} \leq P_{Rx}$

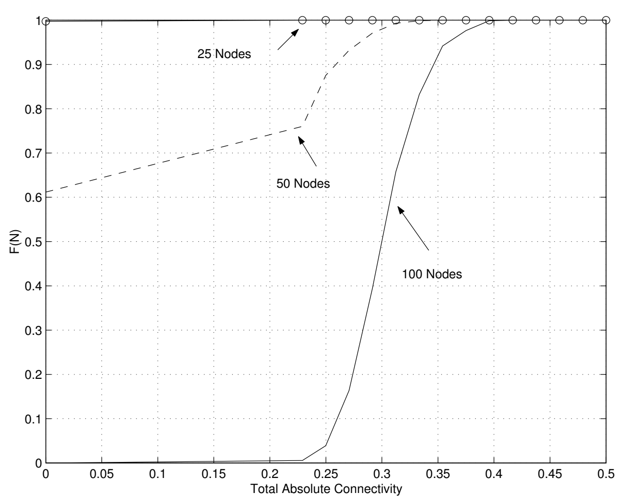

Figure 4.30: Empirical CDF of the Total Absolute Connectivity considering R

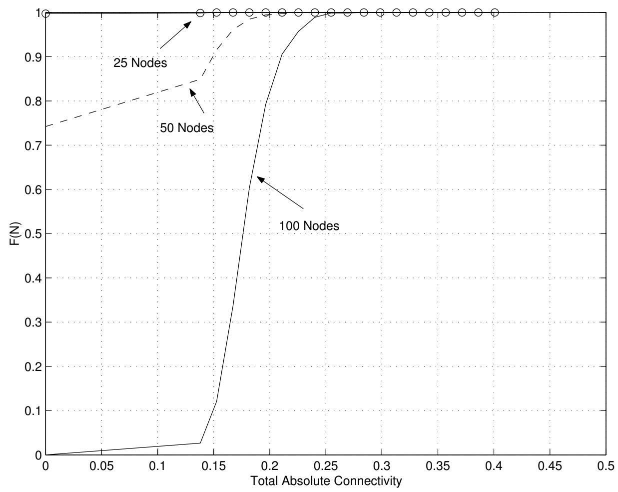

Figure 4.31: Empirical CDF of the Total Absolute Connectivity considering P_{Rx}

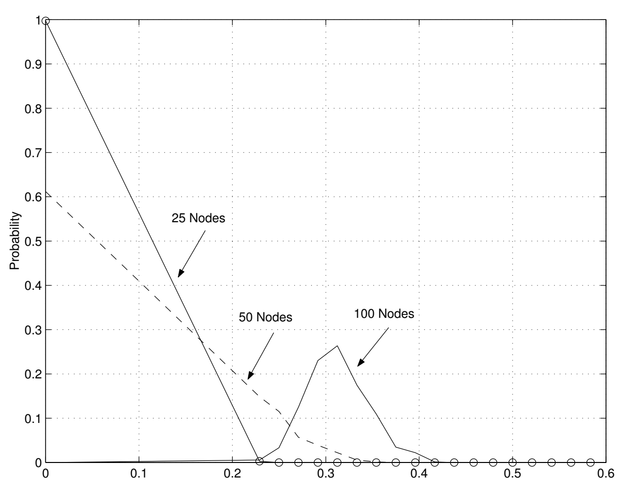

Figure 4.32: Histograms normalized of the Total Absolute Connectivity considering R

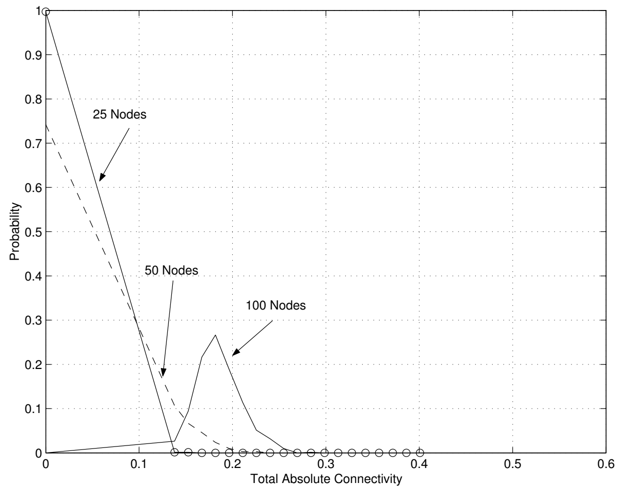

Figure 4.33: Histograms normalized of the Total Absolute Connectivity considering P_{Rx}

Both histograms 4.32 and 4.33 presents us that the maximum probability in order to be connected is 0.27 with approximate with a 20 percent of the network for the case when the power levels received are considered and when the distance is considered, the total absolute connectivity with all network is approximate of a 33 percent. We observe that the probability in order to be connected for both considerations are not increase but the mean value in the histogram considering the distance only is shift to the right.

With a simple inspection we can say that the histograms behavior have a tendency to be Gaussian in function of the node population is greater; in Figures 4.34, 4.35 and 4.36 we compare the samples obtained in the simulation with a Gaussian pdf. In the Figure 4.34 we observed that the some samples follow the Gaussian behavior and some cases the the samples over estimate the Gaussian pdf. In the Figure 4.35 the samples tendency to be Gaussian is greater.

Finally, in Figure 4.36 we can verify the suppose made, in function of the node population.

4.5 Analyzing Fragility

With the idea of analyzing the virtual cluster fragility with different node population in function of node number within coverage area we proposed a new parameter called fragility

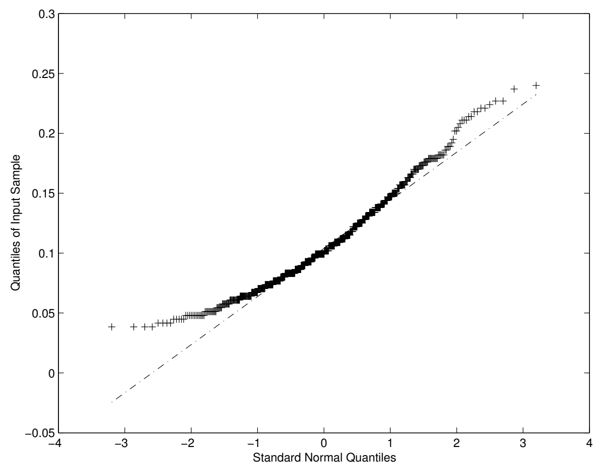

Figure 4.34: Total Absolute Connectivity samples with N_{tot}=25 vs Gaussian pdf

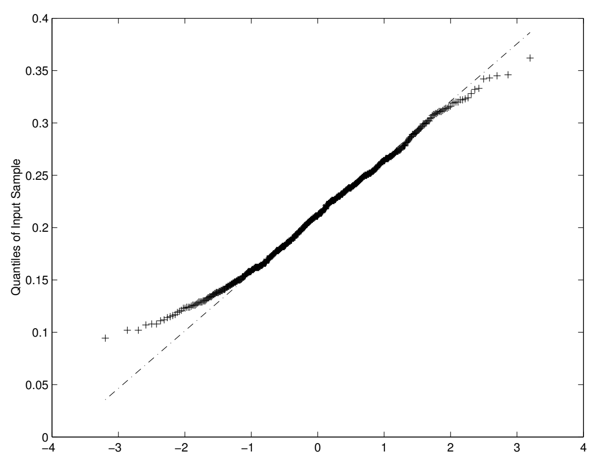

Figure 4.35: Total Absolute Connectivity samples with N_{tot}=50 vs Gaussian pdf

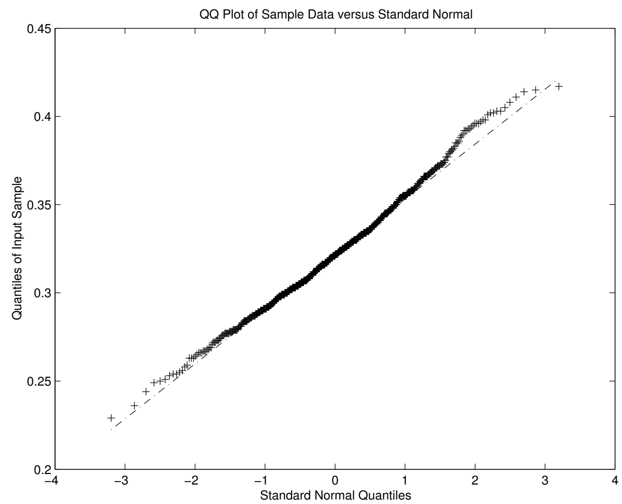

Figure 4.36: Total Absolute Connectivity samples with N_{tot}=100 vs Gaussian pdf

that present a value maximum in 1; when the virtual cluster could be divided with high probability and a value of 0 when the virtual cluster hadn't any link to h-hop (the node is alone in these zone) as shown in Figures 4.37 and 4.38 where the fragility is increase for the case when the power levels received are considering for realize the link; this behavior is presented in Figures 4.39, 4.40, 4.41 and 4.42 too.

In the Figures 4.37 and 4.38 obviously the fragility to 2-hop is generally more low than 3 and 4 hops for case when the node population is equal to 25 nodes but when the node population is increase (second and third scenario) the fragility to 2-hop obviously decrease but for 3 and 4 hops the behavior isn't equal as show in Figures 4.37 and 4.38 now the fragility is similar to the fragility to 2-hop and some case the fragility to 4-hop is the lowest, as show in Figures 4.39, 4.40, 4.41 and 4.42.

The averages of each case are presented in the Table 4.5; and is important explain that in the case with 25 nodes due to exist nodes totally disconnected, we decided that the nodes that totally disconnected do not influence in the averages of fragility.

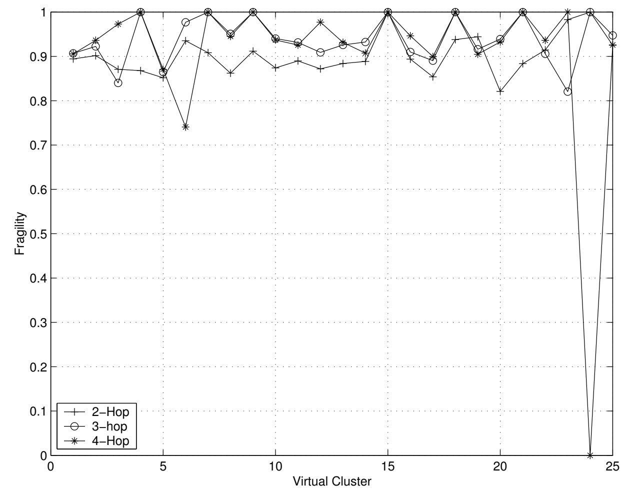

Figure 4.37: Fragility with N_{tot}=25 considering $d_{ij} \leq$R

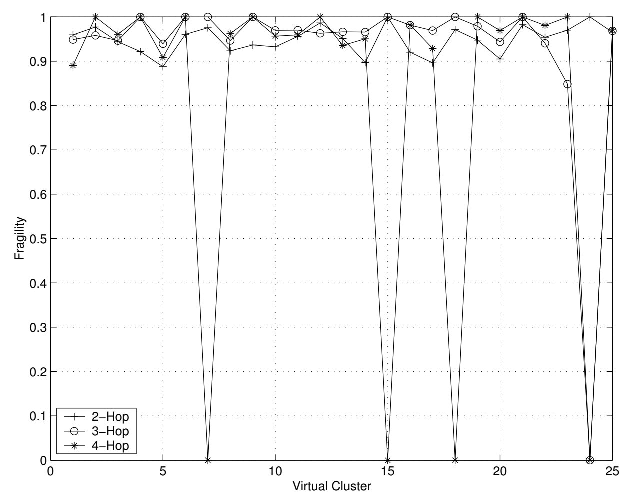

Figure 4.38: Fragility with N_{tot}=25 considering $P_{threshold} \leq P_{Rx}$

Table 4.5: Average of Fragility

Node	$d_{ij} \leq$R			$P_{threshold} \leq P_{Rx}$		
Population	2-hop	3-hop	4-hop	2-hop	3-hop	4-hop
25	0.90	0.93	0.94	0.94	0.96	0.96
50	0.71	0.61	0.73	0.83	0.85	0.85
100	0.55	0.57	0.55	0.70	0.73	0.74

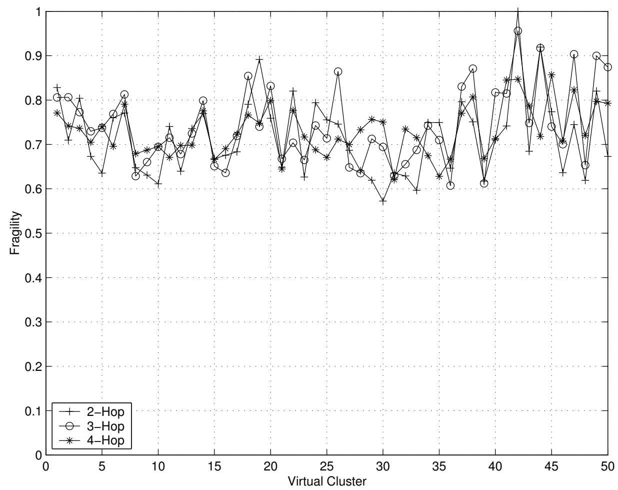

Figure 4.39: Fragility with N_{tot}=50 considering $d_{ij} \leq R$

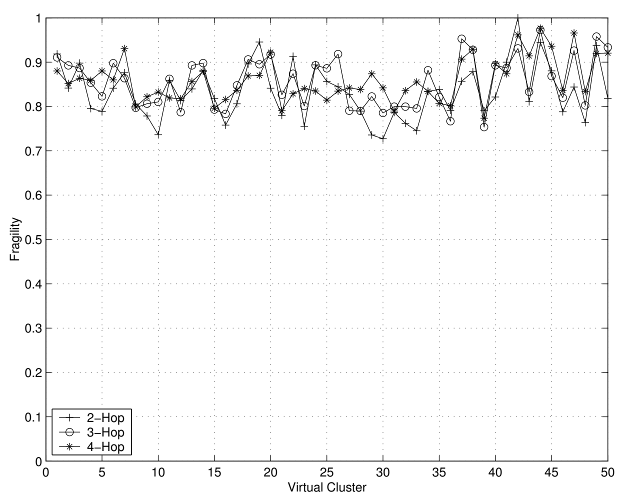

Figure 4.40: Fragility with N_{tot}=50 considering $P_{threshold} \leq P_{Rx}$

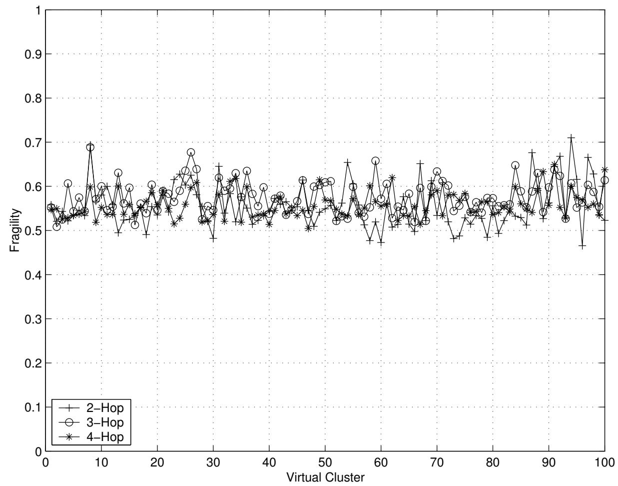

Figure 4.41: Fragility with N_{tot}=100 considering $d_{ij} \leq R$

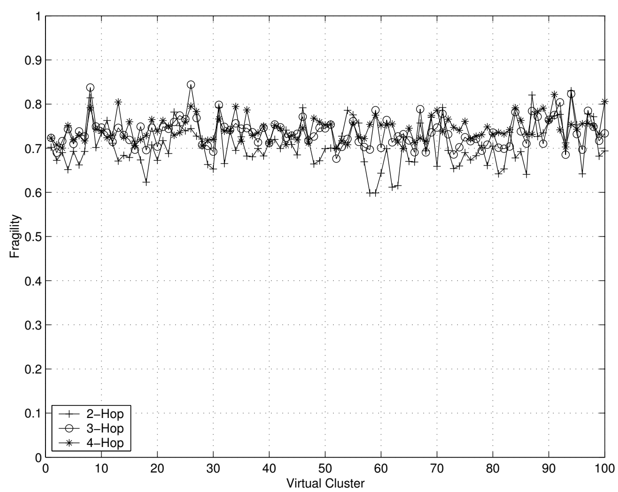

Figure 4.42: Fragility with N_{tot}=100 considering $P_{threshold} \leq P_{Rx}$

Chapter 5

Conclusions

In this chapter we presents the general conclusions of the research. At the end of the chapter, Section 5.2, some research projects are presented which would to fortify this section.

5.1 General Conclusions

In this work we proposed some parameters for analyzing the organization, mobility and connectivity of the nodes with different density within an area bounded; such as the fragility and different types of connectivity both as a function of the nodes connected because we concluded that, in general the node population is an important influence for the network connectivity in ad hoc network. But such influence is more perceptible in the connectivity values within the zone of 3 and 4 hops because this values are increase greatly with respect to the scenario with node population low (25 nodes).

The parameters proposed in this work presents a base for analyze the ad hoc network in general and with different node populations because this parameters are generalized for increment the options of analyze this type of networks and not only the cases proposed in this work.

We could concluded that the new parameters are good analyzing any circumstance of node population and presents results coherent of the behavior of the nodes through of the connectivity values as shown the Figures 4.34, 4.35 and 4.36 where we established that the behavior of the total absolute connectivity of the network has a Gaussian tendency when the node population is increased, and their organization is more complex and is pattern for the fragility values that begin to be decreased.

The network connectivity and the total absolute connectivity for the case where the node population is equal to 100 nodes show us a behavior similar in all graphs where the connectivity values are around of the mean value (the values not change much).

After of observe the graphs and compare results with other works the values obtained for the connectivity to 1-hop for every virtual cluster are between the called "magic numbers", [33]. We concluded that a node is highly connected when the node number linked to 1-hop is between 6 and 8 nodes.

Comparing the considerations made for realized the link with other nodes (distance between nodes and power levels received for every node) the results of the all types of connectivity defined in this work considering the power levels received are generally below of the results obtained considering only the distance between nodes for realized the links. But we consider that the better strategy that show a form more real of evaluate the mobility and organization of an ad hoc network is considering the power levels received in every node because this consideration modelling the environment considering impairments that presents the wireless channel.

5.2 Future Work

This work presents a base for analyze the ad hoc networks in function of their connectivity and fragility, such parameters show us the node mobility and the network organization using complete spatial randomness process to simulate the generation of nodes, but is necessary extend the analyzes using Poisson Cluster Process in the allocation of the node positions because using this process we could consider attractors models within the region.

Other interesting idea, that we propose is analyzing the ad hoc network extending the velocity range of every node and increased the maximum hop numbers with the objective of observe the total absolute connectivity behavior of the network in this case.

Bibliography

[1] Satyabrata Chakrabarti and Amitabh Mishra, "QoS Issues in Ad Hoc Wireless Networks," *IEEE Communications Magazine,* vol.39, no. 2, pp. 142-148, February 2001.

[2] Ting-Chao Hou and Tzu-Jane Tsai, "An Access-Based Clustering Protocol for Multihop Wireless Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications,* vol. 19, no. 7, pp. 1201-1210, July 2001.

[3] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications Magazine,* vol. 6, no. 2, pp. 46-54, April 1999.

[4] A. Bruce McDonald and Taieb F. Znati, "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications,* vol. 17, no. 8, pp. 1466-1487, August 1999.

[5] Dietrich Stoyan, Wilfrid S. Kendall, and Joseph Mecke, *Stochastic Geometry and Its Applications,* Edit. Wiley, Second Edition.

[6] Chai-Keong Toh, *Ad hoc Mobile Wireless Networks Protocols and Systems,* Prentice Hall PTR, 2002.

[7] M. Jiang, J. Li and Y.C. Tay, "Cluster Based Routing Protocol (CBRP) Functional Specification," *submitted for publication IETF internet,* 14 Aug. 1999.

[8] Wendy L. Martinez and Angel R. Martinez, *Computational Statistics Handbook with MATLAB,* Edit Chapman & Hall/CRC, 2002.

[9] John M. Castelloe and Dale L. Zimmerman, "On Maximum Likehood Estimation of a Spatial Poisson Cluster Process," *Technical Report, 312, Department of Statistics and Actuarial Science, University of Iowa* , February 2002.

[10] Leonard E. Miller, "Probability of a Two-Hop Connection in a Random Mobile Network," *Conference on Information Sciences and Systems,* The Johns Hopkins University, March 21-23, 2001.

[11] A. Mawira, "Estimate of Mean C/I and Capacity of Interference Limited Mobile Ad Hoc Network," *IEEE International Zurich Seminar on Broadband Communications,* February 2002.

[12] Paolo Santi and Douglas M. Blough, "An Evaluation of Connectivity in Mobile Wireless Ad Hoc Network," *International Conference on Dependable Systems and Networks (DSN'02),* June 23-26, 2002.

[13] Olivier Dousse, Patrick Thiran and Martin Hasler, "Connectivity in Ad Hoc and Hibryd Networks," *Proceedings of INFOCOM, New York,* June 2002.

[14] Sohjiroh Norita, Masayuki I toh and Akihiro Kajawara, "Ad-hoc Network of Cluster Architecture with Backup Node," *The 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, London UK,* September 2000

[15] Azzedine Boukerche, "A Simulation Based Study of On-Demand Routing Protocols for Ad hoc Wireless Networks," *Proceedings of 34th Annual Simulation Symposium (SS'01),* pp. 85-92, 2001.

[16] Chang Wook Ahn, R.S. Ramakrishna and Chung Gu Kang, "Efficient Clustering-Based Routing Protocol in Mobile Ad-Hoc Networks," *Proceedings of IEEE 56th VTC 2002-Fall,* vol. 3, pp. 1647-1651, 2002.

[17] Wei Lou and Jie Wu, "Efficient Broadcast With Forward Node Set in Clustered Mobile Ad Hoc Networks," *Proceedings of 11th International Conference on Computer Communications and Networks,* pp. 398-403, 2002.

[18] Dimitri Bertsekas and Robert Gallager, *Data Networks,* Prentice Hall, Second Edition, 1992.

[19] C.P.P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers," *Proceedings of ACM SIGCOMM'94,* pp. 234-244, September 1994.

[20] S. Murthy and J.J. Garcia-Luna Aceves, "A Routing Protocol for Packet Radio Networks," *Proceedings of ACM First International Conference on Mobile Computing & Networking (MOBICOM'95),* November 1995.

[21] Jyoti Raju and J.J. Garcia-Luna Aceves, "A Comparison of On-demend and Table-driven Routing for Ad Hoc Wireless Networks," *Proceedings of IEEE ICC,* June 2000.

[22] C.-C. Chiang, H.-K. Wu, W. Liu and M.Gerla, "Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel," *Proceedings of IEEE Singapore International Conference on Networks,* 1997.

[23] C. Perkins and E.Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications,* February 1999.

[24] David B. Johnson and David A. Maltz, *Mobile Computing.* Kluwer Academic Publisher, 1996

[25] V. Park and M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proceedings of IEEE INFOCOM'97,* March 1996.

[26] R. Dube, C. D. Rais, K.-Y. Wang, and S. K. Tripathi, "Signal Stability Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks," *IEEE Personal Communication Magazine,* vol. 4, no. 1, pp. 36-45, February 1997.

[27] Z. Haas and M. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," *IETF MANET Draft,* June 1999.

[28] Z. Haas, M. Pearlman and Prince Samar, "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," *IETF MANET Draft,* July 2002.

[29] Z. Haas, M. Pearlman and Prince Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," *IETF MANET Draft,* July 2002.

[30] Z. Haas, M. Pearlman and Prince Samar, "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks," *IETF MANET Draft,* June 2001.

[31] Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," *Proceedings of ACM SIGCOMM'98,* September 1998.

[32] Theodore S. Rappaport, *Wireless Communications Principles and Practice,* Prentice Hall, Second Edition, 2002

[33] Jian Ni, "Connectivity Properties of Radio Telephone Network," *Mobile and Personal Communications, Conference Publications,* No.387, December 1993.