SURVIVABILITY ANALYSIS OF AD HOC WIRELESS NETWORK ARCHITECTURE

Krishna Paul[1], Romit RoyChoudhuri[2], S. Bandyopadhyay[3]

[1] Cognizant Technology Solutions, Sector V, Saltlake
Calcutta 700 091 India
{PKrishna2@cal.cts-corp.com}

[2] Department of Computer Sc and Engg
Haldia Institute of Technology
Haldia, West Bengal, India

[2] PricewaterhouseCoopers, Saltlake Technology Center
Sector V, Calcutta 700 091, India
{somprakash.bandyopadhyay@in.pwcglobal.com}

Abstract. Mobile ad hoc wireless networks are generating novel interests in mobile computing. The dynamism in network topology has thrown up multifarious issues, requiring a fresh look into the aspects of system design and networking protocols. As a direct consequence of injecting mobility into a static network, the formal relationships between several governing parameters have undergone changes. In this paper we have assayed the behavior of the ad hoc network as a whole and analyzed trends in the inter-parameter dependencies, with the objective of addressing to the survivability issues. We have finally drawn out an operating region of survivability for mobile ad hoc wireless networks in terms of user declared specifications. Our own simulator has been operative through the work. We have derived our survivability constraints from several runs of the network simulator.

1. Introduction

An ad hoc network [1] can be envisioned as a collection of mobile routers, each equipped with a wireless transceiver, which are free to move about arbitrarily. The mobility of the routers and the variability of other connecting factors results in a network with a potentially rapid and unpredictable changing topology. These networks may or may not be connected with the infrastructure such as internet, but still be available for use by a group of wireless mobile hosts that operates without any base-station or any centralized control. Applications of ad hoc networks include military tactical communication, emergency relief operations, commercial and educational use in remote areas, etc. where the networking is mission-oriented and / or community-based.

There has been a growing interest in ad hoc networks in recent years [1,2,3,4,5]. The basic assumption in an ad-hoc network is that, two nodes willing to

communicate may be outside the wireless transmission range of each other but still be able to communicate if other nodes in the network are willing to forward packets from them. However, the successful operation of an ad-hoc network will be hampered, if an intermediate node, participating in a communication between two nodes, moves out of range suddenly or switches itself off in between message transfer. The situation is worse, if there is no other path between those two nodes. An important problem associated with this is to find a stable path satisfying multiple constraints to ensure certain level of QoS guarantee during communication.

Lot of research has been done on ad hoc network routing protocols in order to solve the problem of routing packets. However, there is no complete proposal available to assess the survivability issues in ad hoc network in order to provide a network specification to support effective communication in such a dynamic environment. Survivability analysis [6], in this context, can be defined as network specifications and management procedures to minimize the impact of system dynamics on the network services . For example, assume an area 1000 x 1000 sq.meter where 20 nodes are moving around with an average velocity of 10m/sec. The transmission range for each node is, say, 350 meter. Under a given traffic pattern, will this network be able to provide the required service guarantee to its users in spite of the dynamic change in topology due to mobility? If the answer is yes, let us further assume that some of the users decide to switch-off or to leave the field or to increase their mobility. Will the network still survive? On the other extreme, let us assume that 20 new nodes join the system, making the node count to 40. The transmission range that is optimal for 20 nodes may be too high for 40 nodes, as this will increase collision and congestion of control / data packets. Will the network still be able to provide the required service guarantee to its users ?

So, survivability analysis and drawing up a specification for a survivable ad hoc network is an important issue that we want to address in this paper.

2. Survivable Systems

2.1 Definition and Characteristics of Survivable Systems

Traditionally, survivability in network systems has been defined as the capacity of a system to fulfil its mission, in a timely manner, in the presence of failures [7]. The term mission refers to a set of very high-level requirements or goals. Timeliness is a critical factor that is typically associated with the mission fulfillment. In the context of ad hoc network, mission fulfillment in a timely manner implies that the network should be able to ensure certain level of service guarantee to its user in the presence of system dynamics. Survivability analysis, in this context, can be defined as network specifications and management procedures to minimize the impact of system dynamics on the network services.

Thus, in this study, we are not considering failure due to hardware malfunctions or software errors. However, in an ad hoc network, any node can randomly switches itself off causing an event equivalent to node failure. Similarly, any link between two node can get disconnected anytime because of mobility of the nodes, causing an event equivalent to link failure. Additionally, new nodes can join the system at any

point of time; similarly, new links can be formed between any two nodes, as they come closer to each other due to their mobility.

For survivability, we must achieve system-wide properties that typically do not exist in individual nodes. A survivable system must ensure that desired survivability properties emerge from interactions among the components in the construction of reliable systems from unreliable components [7]. If survivability properties are emergent they are present only when the number of nodes of a system are sufficiently large. If the number or arrangements of nodes falls below a critical threshold, the attendant survivability property fails. For example, we can specify an ad hoc network to operate at a transmission range of, say, 350 with number of nodes between 15 and 20 at a mobility ranging from 5m/s to 20m/s. But, if number of nodes falls below that, the system may not survive i.e. may not be able to ensure certain service guarantee to its users.

2.2 Specifying the Requirements of Survivable Ad hoc Network

Central to the notion of survivability analysis is to identify and ensure the maintenance of certain essential attributes and the operating levels of those attributes that must be associated with the specified level of service guarantee. In the context of ad hoc network , the goal is to maintain the network availability and allow the data packets to be delivered to the intended destination from a source in spite of the changes in network topology due to its dynamic behavior. Survivability analysis consists of determining whether service objectives can be maintained during all operational modes.

Thus, network service in the context of ad hoc network is primarily pivotal to two fundamental requirements:

1. establishing a connection between any two nodes in the network at any instant of time.
2. Assuring an uninterrupted connection until a finite volume of data transfer has been accomplished (of course with limited delay in data transfer).

Survivability issues depend entirely on how well these two demands are met with. A network would be called survivable if it meets both the above requirements satisfactorily. Now, in order to declare an ad hoc network survivable we need to first define the user requirements in more formal terms. In other words we require a set of metrics which would inherently take care of all the service demands and finally throw up a numerical values depicting the degree of survivability for a given set of design specifications. Our objective is to design such a set of metrics in terms of the basic network parameters: number of nodes (N), transmission range (R), mobility (M), average volume of data to be communicated from a source to its destination (V) and average number of communication events per minute (C).

3. System Description

The network is modeled as a graph G = (N,L) where N is a finite set of nodes and L is a finite set of unidirectional links. Each node $n \in N$ is having a unique node identifier. Since in a wireless environment, transmission between two nodes does

not necessarily work equally well in both direction [1], we assume unidirectional links. Thus, two nodes n and m are connected by two unidirectional links $l_{nm} \in L$ and $l_{mn} \in L$ such that n can send message to m via l_{nm} and m can send message to n via l_{mn}. However, in this study, we have assumed $l_{nm} = l_{mn}$ for simplicity.

In a wireless environment, each node n has a wireless transmitter range. We define the neighbors of n, $N_n \in N$, to be the set of nodes within the transmission range R of n. It is assumed that when node n transmit a packet, it is broadcast to all of its neighbors in the set N_n. However, in the wireless environment, the strength of connection of all the members of N_n with respect to n are not uniform. For example, a node $m \in N_n$ in the periphery of the transmission range of n is weakly connected to n compared to a node $p \in N_n$ which is more closer to n. Thus, the chance of m going out of the transmission range of n due to outward mobility of either m or n is more than that of p.

Each link l_{nm} is associated with a signal strength S_{nm} which is a measurable indicator of the strength of connection from n to m at any instant of time. Due to the mobility of the nodes, the signal strengths associated with the links changes with time. When the signal strength S_{nm} associated with l_{nm} goes below a certain threshold S_t, we assume that the link l_{nm} is disconnected.

Affinity a_{nm}, associated with a link l_{nm}, is a prediction about the span of life of the link l_{nm} in a particular context [5]. For simplicity, we assume a_{nm} to be equal to a_{mn} and the transmission range R for all the nodes are equal. To find out the affinity a_{nm} , node n sends a periodic beacon and node m samples the strength of signals received from node n periodically. Since the signal strength is roughly proportional to $1/R^2$, we can predict the current distance d at time t between n and m. If M is the average velocity of the nodes, the worst-case affinity a_{nm} at time t is (R-d)/M, assuming that at time t, the node m has started moving outwards with an average velocity M. For example, If the transmission range is 300 meters, the average velocity is 10m/sec and current distance between n and m is 100 meters, the life-span of connectivity between n and m (worst-case) is 20 seconds, assuming that the node m is moving away from n in a direction obtained by joining n and m..

Given any path p = (i, j, k, …, l, m), the **stability of path p** [5] at a given instant of time will be determined by the lowest-affinity link (since that is the bottleneck for the path) and is defined as $\min[a_{ij}, a_{jk}, \ldots, a_{lm}]$. In other words, stability of path p between source s and destination d, η^p_{sd}, is given by

$$\eta^p_{sd} = \min_{\forall i,j} a^p_{ij}$$

However, the notion of stability of a path is dynamic and context-sensitive. As indicated earlier, stability of a path is the span of life of that path from a given instant of time. But stability has to be seen in the context of providing a service. A path between a source and destination would be stable if its span of life is sufficient to complete a required volume of data transfer from source to destination. Hence, a given path may be sufficiently stable to transfer a small volume of data between source and destination; but the same path may be unstable in a context where a large volume of data needs to be transferred.

4. Route Discovery and Data Communication Mechanism in Ad hoc Network

The existing routing protocol can be classified either as proactive or as reactive [3]. In proactive protocols, the routing information within the network is always known beforehand through continuous route updates. The family of distance vector and link state protocols is examples of proactive scheme. Reactive protocols, on the other hand, invoke a route discovery procedure on demand only. The family of classical flooding algorithms belongs to this group. It has been pointed out that proactive protocols are not suitable for highly mobile ad hoc network, since they consume large portion of network capacity for continuously updating route information. On the other hand, on-demand search procedure in reactive protocols generate large volume of control traffic and the actual data transmission is delayed until the route is determined.

Whatever may be the routing scheme, frequent interruption in a selected route would degrade the performance in terms of quality of service. In [5], we have attempted to minimize route maintenance by selecting stable routes, rather than shortest route, which is illustrated below.

4.1 Path finding mechanism

A source initiates a route discovery request when it needs to send data to a destination. The source broadcast a route request packet to all neighboring nodes. Each route request packet contains source id, destination id, a request id, a route record to accumulate the sequence of hops through which the request is propagated during the route discovery, and a count max_hop which is decremented at each hop as it propagates. When max_hop=0, the search process terminates. The count max_hop thus limits the number of intermediate nodes (hop-count) in a path.

When any node receives a route request packet, it decrements max-hop by 1 and performs the following steps:

1. If the node is the destination node, a route reply packet is returned to the source along the selected route, as given in the route record which now contains the complete path information between source and destination.
2. Otherwise, if max_hop=0, discard the route request packet.
3. Otherwise, if this node id is already listed in the route record in the request, discard the route request packet (to avoid looping).
4. Otherwise, append the node id to the route record in the route request packet and re-broadcast the request.

When any node receives a route reply packet, it performs the following steps:

1. If the node is the source node, it records the path to destination.
2. If it is an intermediate node, it appends the value of affinity and propagates to the next node listed in the route record to reach the source node.

4.2 Sending the data from source to destination

When a source initiates a route discovery request, it waits for the route reply until time-out. If it receives a path, it computes its stability $\eta^p_{sd.}$ If V_{sd} is the volume of data to be send to destination and if B is the bandwidth for transmitting data, V_{sd} / B is the one-hop delay to transmit the data, ignoring all other delay factors. If H is the number of hops from source to destination, H* V_{sd} / B will be the time taken to complete the data transfer. If η^p_{sd} is sufficient to carry this data, the path is selected. Otherwise, the source checks the next path, if available, for sufficient stability. In order to check the sufficiency, η^p_{sd} is multiplied with a correction factor f, to be decided dynamically, to take care of estimation error and other delay factors related to traffic characteristics.

The Algorithm:
Step I: p:= 0;
Step II: **wait** for a path **until** timeout;
Step III: **if** a path is available **then**
begin
p:=p+1;
find $\eta^p_{sd} = \min_{\forall i,j} \eta^p_{ij;}$ { find the stability of path k}
if (H* V_{sd} / B) < f * η^p_{sd} {if the path is suffiently stable }
then start sending V_{sd} into p_{th} path
else reject the path and goto step II
end
Step IV: terminate.

5. The Simulation Environment

Existing simulators are not well-equipped to serve our purpose [9,10,11]. Hence, in order to model and study the survivability issues of the proposed framework in the context of ad hoc wireless networks, we have developed a simulator with the capability to model and study the following characteristics:

- Node mobility
- Link stability (*affinity*)
- Affinity- based path search
- Dynamic network topology depending on number of nodes, mobility and transmission range
- Realistic physical and data link layers in wireless environment
- Data communication with different data volume and different frequency of communication events per minute.

The proposed system is evaluated on a simulated environment under a variety of conditions. In the simulation, the environment is assumed to be a closed area of 1000 x 1000 sq. meter in which mobile nodes are distributed randomly. We ran simulations for networks with different number of mobile hosts, operating at different transmission ranges. The bandwidth for transmitting data is assumed to be

1000 packets / sec. The packet size is dependent on the actual bandwidth of the system.

In order to study the delay, throughput and other time-related parameters, every simulated action is associated with a simulated clock. The clock period (time-tick) is assumed to be one millisecond (simulated). For example, if the bandwidth is assumed to be 1000 packets per second and the volume of data to be transmitted from one node to its neighbor is 100 packets, it will be assumed that 100 time-ticks (100 millisecond) would be required to complete the task. The size of both control and data packets are same and one packet per time-tick will be transmitted from a source to its neighbors.

The speed of movement of individual node ranges from 5 m/sec. to 20 m/sec. Each node starts from a home location, selects a random location as its destination and moves with a uniform, predetermined velocity towards the destination. Once it reaches the destination, it waits there for a pre-specified amount of time, selects randomly another location and moves towards that. However, in the present study, we have assumed zero waiting time to analyze worst-case scenario.

6. Analyzing the Impact of Dynamic Topology on survivability

6.1 Related Definitions

To conceive certain trends in network characteristics on the whole, some terms have been used that are defined as follows:

Average Connectivity Efficiency (E): Connectivity Efficiency has been defined as the ratio of total number of connected node-pairs (in single hop or in multiple hops) and the total number of available node pairs at any instant of time. This fraction captures the degree of connectivity among the nodes in any snapshot of the mobile environment. From the survivability point of view, this parameter is an indicator to the success rate of a source node, in attempting to establish a connection with a destination node. The efficiency values obtained over several snapshots (taken at intervals of one second from the simulator) of the dynamic environment have been finally averaged to yield the Average Connectivity Efficiency. A network where all the node-pairs are always connected in single or multiple hops have a Average Connectivity Efficiency of 100%. Thus,

$$\textbf{Average Connectivity Efficiency (\%)} = \frac{\Sigma^{T}_{i=1}\ \textbf{(no. of connected node pairs) * 100}}{\textbf{T * Number of node-pairs}}$$

Average Network Stability (S): From survivability perspectives, the span of time for which two nodes remain connected (given the number of nodes, transmission range and the mobility) need to be analyzed. A parameter, **affinity**, introduced in [5] and explained in section 3 has been used for average worst case analysis. As explained in section 3, the stability of the path (i.e. the span of time for which this path would exist) can be determined by the weakest link in the path.

Two nodes in the ad hoc environment may often be connected with several paths. For data communication between two nodes, the best path should always be chosen i.e. the path assuring greater stability. Thus,
Node to Node Stability = *max* (stability of all the paths between the two nodes).

The **Average Network Stability** has been defined as the average node to node stability over time.

$$\textbf{Average Network Stability} = \frac{\Sigma^{T}_{i=1}\,\Sigma_{\text{all node-pair}}\ \textbf{(Node to Node Stability)}}{\textbf{T * number of node-pairs}}$$

A**verage Number of Neighbors (G):** The study of percolation is an important aspect from the data communication point of view in a mobile computing environment [12]. For a random distribution of nodes in a bounded region, percolation is proportional to the number of neighbors, which in turn is a function of node density and signal strength. Average Number of neighbors has been defined as:

$$\textbf{Average Number of Neighbors} = \frac{\Sigma^{T}_{i=1}\Sigma_{\text{all node}}\ \textbf{(Number of neighbors of each node)}}{\textbf{T * number of node}}$$

6.2 Variation of Average Connectivity Efficiency (E) with N, R and M

It is quite obvious that if the signal strength increases, the probability of connectivity also increases. The variation of connectivity efficiency against signal strength has been shown in the plot in fig.1(a). However this signal strength cannot be allowed to increase indefinitely due to other overheads:

1. Cost (power consumption due to battery usage) increases as the signal strength is raised.
2. Congestion and collision are the inevitable outcome of higher signal strength during data communication, as will be illustrated in the next section.

A larger number of users in a closed area indicate a higher node density. Since E is a measure of connectivity and connectivity is heavily dependent on how close the nodes are with each other, the total number of nodes in a bounded area also contributes to the connectivity efficiency. Thus, the connectivity efficiency bears a composite relation with the number of nodes as well (Fig. 1(b)). From figure 1, it is quite evident that, to achieve a specific threshold of efficiency, there is a lower cut off of the signal strength for a given number of nodes.

E would not depend on the mobility of the nodes. If the node mobility is high, then the probability of nodes moving out of a node's transmission range increases as much as the probability of new nodes coming into the transmission range of the same node. As a result, average value of connectivity taken over a long time remains unaffected at different mobility.

Figure 2 depicts the variation of Average Connectivity Efficiency (E) against Average Number of Neighbors (G). Although G does not reflect the actual dependence of E on N and R, it can be instrumental in deciding the cut off for satisfactory connectivity in the network. Over G=6 the efficiency is always found to

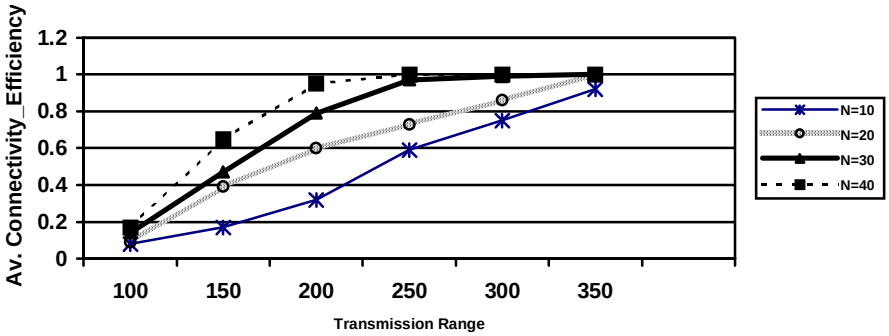


Fig 1(a). Average Connectivity Efficiency vs. Transmission Range for different number of nodes

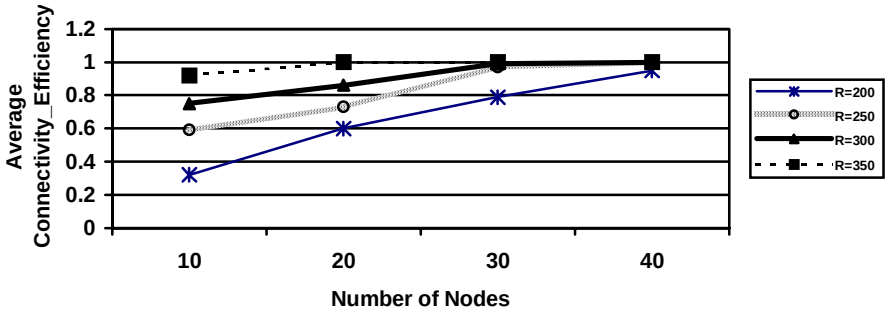


Fig 1(b). Average Connectivity Efficiency vs. Number of Nodes for different Transmission Range

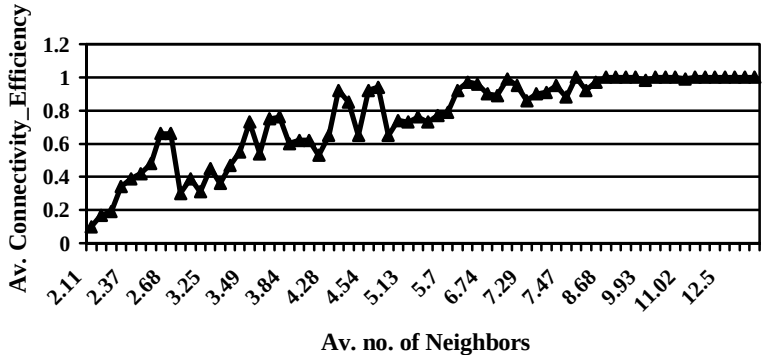


Fig 2. Average Connectivity Efficiency vs. Average Number of Neighbors

be increasing over 0.8. Over a certain threshold of neighbors, the network becomes connected and further increase in G would only hike overhead. The optimal value of G as six to eight has been proposed earlier[12,13] for large number of nodes which has been revalidated here with lower number of nodes with different mobility pattern.

Hence, the conclusion from above is: to ensure a fairly high level of connectivity, the design parameters should be such that the predicted number of neighbors is greater than 6. Assuming uniform distribution, the average node density per unit area is N/A, where N is the number of nodes in area A. Assuming uniform transmission range R, $[(N*\Pi R^2/A) -1]$ will be the average number of neighbors, which should be greater than six to have $E > 0.8$.

6.3 Variation of Average Network Stability against N. R and M

From the perspective of network service, the stability of a path between two arbitrary nodes indicates the volume of data that could be transferred between the two nodes in question (provided none of the intermediate nodes switch off during data transfer). Conversely, it is stability, which would be instrumental in deciding the thresholds of average transferable data volume, thus ensuring survivability.

A high node density in the operating environment essentially indicates that the average distance between two nodes is less in comparison to a model of low node density. Naturally, if two nodes remain in greater proximity, for a given signal strength and mobility, they would remain in contact for a longer period of time. Consequently the average stability of links would be higher and thus the stability of paths. Thus, it can be said that the average stability (S) of a mobile ad hoc wireless network would increase with increase in node density or N (as node density = N / A). At the same time, if the average affinity of links in a network features to be high, the average stability of paths would also be correspondingly higher. From the expression of affinity, we see that affinity of a link increases with increase in transmission range and/or decrease in mobility. Stability can thus be said to be directly proportional to transmission range and inversely proportional to mobility (Figure 3).

7. Analyzing the Impact of Route Discovery and Data Communication on survivability

The above analysis does not take into account the congestion and collision factors that would happen during data communication. We will show that even if a network is well-connected, it may not guarantee successful data communication.

7.1 Related Definitions

Route Discovery Efficiency is defined as the ratio of the average number of route replies obtained per minute and the average number of route request generated per minute. As discussed, the number of route request generated per minute would depend on the number of communication events initiated per minute (C). However,

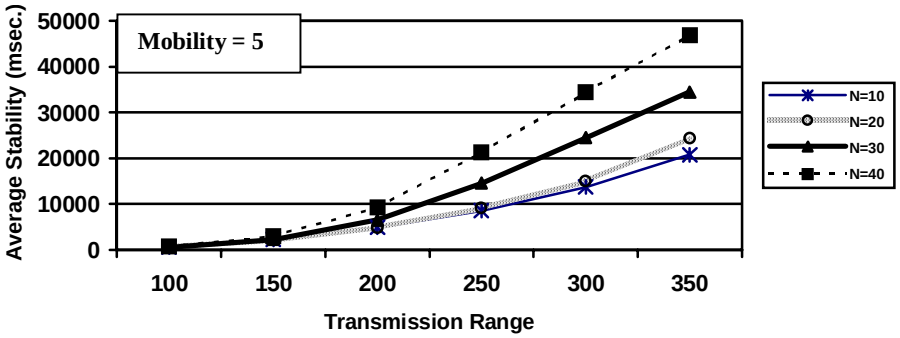


Fig 3(a). Average Network Stability vs. Transmission Range at mobility =5.

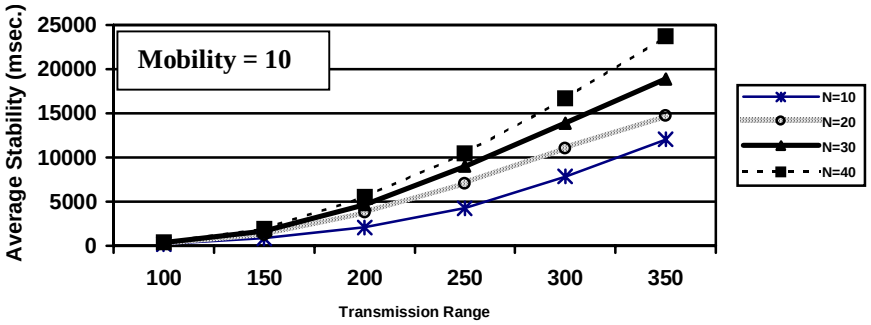


Fig 3(b). Average Network Stability vs. Transmission Range at Mobility = 10.

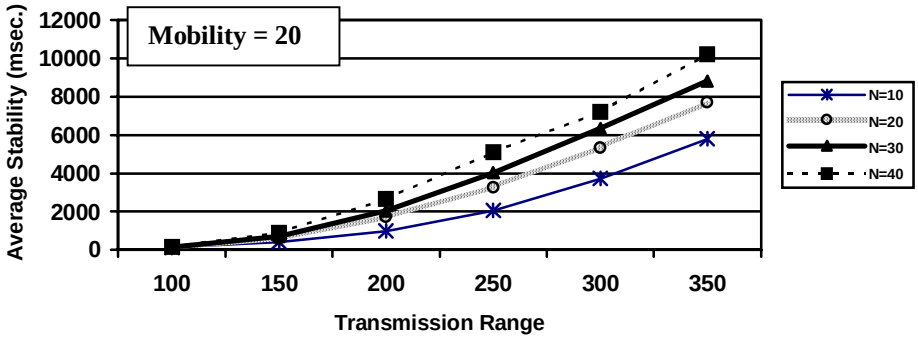


Fig 3(c). Average Network Stability vs. Transmission Range at Mobility =20.

the success of route request i.e. getting a rout reply back within a reasonable period of time (500 msec in our case) would depend on the degree of collision and congestion of the network. This is not only dependent on E but also on the average volume of data communicated from a source to its destination (V) and frequency of communication events per minute (C). If C and / or V increases, the probability of collision and congestion would increase, which in turn will affect the Roure Discovery Efficiency.

Service Efficiency is defined as the ratio of the average number of communication events successful within a reasonable period of time per minute and the average number of route request generated per minute. Service Efficiency depends on four factors : 1) Route request has been generated but route reply has not come back within a reasonable period of time, 2) Route replies have been obtained but the paths are rejected because they are not stable enough to carry out the required volume of data transfer, 3) A path is selected and data communication has started but the path could not be retained throughout the entire period of data communication, and 4) the network delay is too high to complete the data transfer within a reasonable period of time. It has been shown in [5] that the use of stability based routing reduces the probability of (3). However, the prediction of stability would be affected, if the network is heavily congested which will in turn affects the Service Efficiency.

7.2 Variation of Route Discovery Efficiency against N,R and V with C=4 per minute

For a given number of nodes, the number of control packets generated increases drastically beyond a certain transmission range. In a collision-free environment, if G is the average number of neighbors and max_hop =4, then the number of control packet generated will be G^4 per communication event. Therefore, it is obvious that with increase in G, the number of control packets increases drastically.

The congestion due to control packets at high transmission range would affect the Route Discovery Efficiency as shown in Figure 4. The effect would be more pronounced for larger number of nodes and for larger amount of data volume. Here, number of communication event per minute (C) is assumed to be 4. We have also studied this variation with C=10 (not shown) where the large data volume would degrade the Route Discovery Efficiency further. In any case, for a fixed number of N, there is an optimum value of R, R^{Nopt}, which will maximize the route discovery efficiency. Increasing R beyond that point will degrade the performance.

However, R^{Nopt} alone can not maximize route discovery efficiency. We need to consider two more factors : average volume of data to be communicated from a source to its destination (V) and average number of communication events per

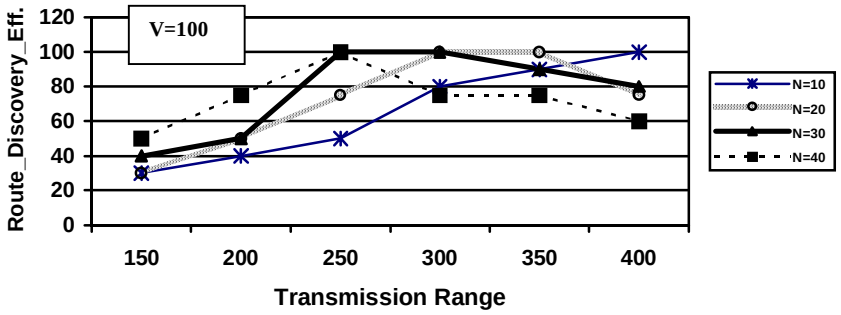


Fig 4(a). Route_Discovery_Efficiency vs. Transmission Range with *Data Volume = 100 packets, Max_Hop=4* and *No of Communication = 4 / min.*

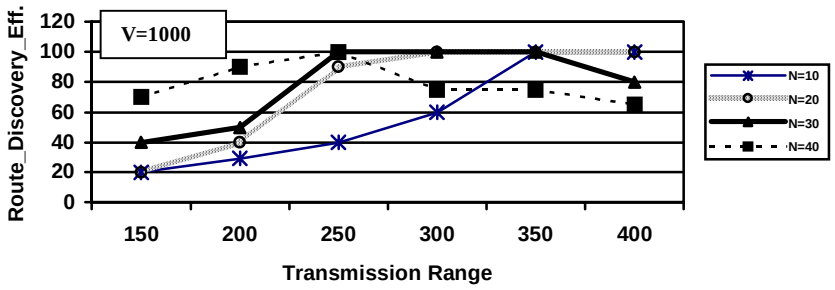


Fig 4(b). Route_Discovery_Efficiency vs. Transmission Range with *Data volume= 1000 packets, Max_Hop=4* and *No of Communication = 4 / min.*

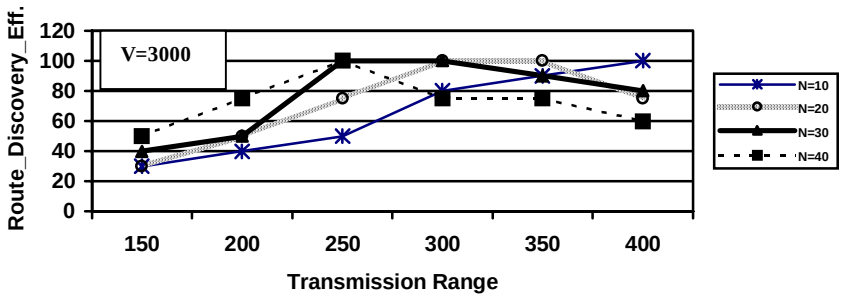


Fig 4(c). Route_Discovery_Efficiency vs. Transmission Range with *Data volume =3000 packets, Max_Hop=4* and *No of Communication = 4 / min.*

minute (C). The system should be capable of absorbing the control and data packets before a new communication event starts.

Depending on R^{Nopt} and the average network stability at that R, we can specify V for an average mobility M. If we increase M or V beyond that, the Service Efficiency will suffer.

7.3 Variation of Service Efficiency with C=4 per minute

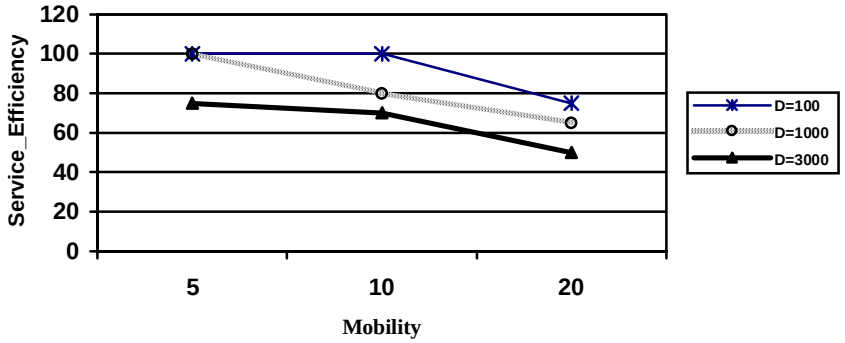
For a given number of node and corresponding R^{Nopt} , the variation of Service Efficiency against M and V is shown in figure 5. It is evident that getting a high Service Efficiency with V=3000 is difficult to obtained in this set up where mobility is varying between 5 to 20. The reason is that we are not getting sufficient stable paths to complete the data transfer. On the other hand, for lower volume of data and low mobility, it is possible to get a Service Efficiency > 80%. With M=20, getting a high Service Efficiency for a data volume > 1000 is difficult, when the number of nodes are more than 20.

8. Survivability Metrics and Specifications for a Survivable Ad hoc Network

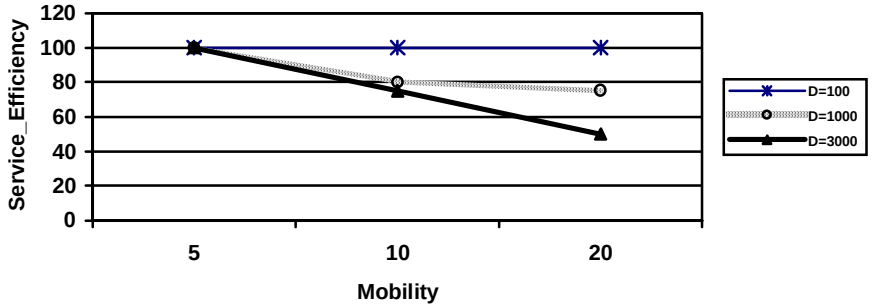
From the above analyses, the following points can be concluded :

- For a fixed number of N, the Average Connectivity Efficiency will be more than 0.8 beyond a certain value of R. If we increase R further, the Connectivity Efficiency will improve and saturate to 1.0. Consequently, the Average Stability will also improve so that a larger volume of data could be sent. But the Route Discovery Efficiency and, consequently, the Service Efficiency will go down because of large number of control packets and / or data packets.
- For a fixed number of N, there is an optimum value of R, R^{Nopt}, which will maximize the route discovery efficiency.
- However, R^{Nopt} alone can not maximize route discovery efficiency. We need to consider two more factors : average volume of data to be communicated from a source to its destination (V) and average number of communication events per minute (C). The system should be capable of absorbing the control and data packets before a new communication event starts.
- Depending on R^{Nopt} and the average mobility M, we can specify average network stability which will in turn determine V. If we increase M or V beyond that, the Service Efficiency will suffer.

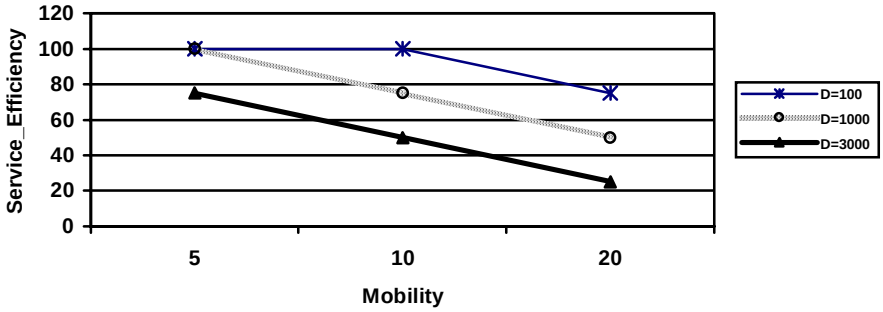
The aim of our entire analysis is to model the survivability region of operation for a mobile ad hoc wireless network. In other words, we need to answer questions like :
What should be the transmission range of operation and the maximum mobility for an ad hoc network with 30 users, if the user require a Service Efficiency of 80% and 1000-Kb average data volume for transfer? The kind of answers we are trying to provide is that, for 30 users with transmission range between 275 m to 325 m, it is possible



5(a). Service_Efficiency vs. Mobility with No. of Comm.=4/min. and *N=20* & *R=350* .



5(b). Service_Efficiency vs. Mobility with No. of Comm.=4/min and *N=30* & *R=300*



5(c). Service_Efficiency vs. Mobility with No. of Comm.=4 / min and *N=40* & *R=250* .

to achieve the required Service Efficiency with V<=1000 and C=4, if the average mobility is less than 10. As another example, suppose we ask that: what is the Service Efficiency achievable if the number of users are 35 to 40, moving with an average velocity between 10 to 20 m/sec and the average data transfer requirement is 4 per minute with an average volume of data = 100 packets ? From the above analyses, we can say that with R=250, we can achieve a Service Efficiency of around 80%.

9. Conclusion

In this analysis, we have not included the impact of the variation of C. We have also not included the per-hop delay and delivery delay under different conditions. However, this preliminary analysis illustrates the basic interdependencies among several governing parameters that would help us in drawing up specifications for survivable ad hoc networks.

Reference

[1] D. B. Johnson and D. Maltz, Dynamic source routing in ad hoc wireless networks, T. Imielinski and H. Korth, eds., *Mobile computing*, Kluwer Academic Publ. 1996.

[2] S. Corson, J. Macker and S. Batsell, Architectural considerations for mobile mesh networking, Internet Draft RFC Version 2, May 1996.

[3] Z.J.Haas, A new routing protocol for the reconfigurable wireless networks, ICUPC'97, San Diego, CA, Oct. 1997.

[4] V. D. Park and M. S. Corson, A highly adaptive distributed routing algorithm for mobile wireless networks, Proc. IEEE INFOCOM '97, Kobe, Japan, April 1997.

[5] K. Paul, S. Bandyopadhyay, D. Saha and A. Mukherjee, Communication-Aware Mobile Hosts in Ad-hoc Wireless Network, Proc. of the IEEE International Conference on Personal Wireless Communication, Jaipur, India, Feb. 1999.

[6] David Tipper, Sreeniwas Ramaswami and Teresa Dahlberg, PCS Networks Survivability, to appear in IEEE WCNC 99, New Orleans, LA, USA

[7] R.J.Ellison D.A. Fisher R.C. Linger H. F. Lipson T. Lonstaff, N. R. Mead, Survivable Network System: An Emerging Discipline, Technical Report CMU/SEI-97-TR-013, Carnegie Mellon University, November, 1997.

[8] D. Medhi, A Unified Approach to Network Survivability for Teletraffic Networks: Models, Algorithms and Analysis, IEEE Transactions on Communications April 1994.

[9] K. Fall, and K. Varadhan. ns Notes and Documentation. The VINT Project, UC Berkeley. http://www-mash.cs.berkeley.edu/ns/,1997.

[10] J. Short, R. Bagrodia and L. Kleinrock. "Mobile Wireless Network System Simulation." *Wireless Network Journal 1*, no. 4, 1995.

[11] Josh Broch,; D.A. Maltz; D.B. Johnson; Y. Hu and J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols." In *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking* (Mobicom'98), Dallas, Texas, Oct. 25-30, 1998.

[12] Y.C.Cheng and T.G.Robertazzi, Critical connectivity phenomena in multihop radio network, IEEE Trans. Commun. , 37(1989), pp 770-777.

[13] H.Takagi and L.Kleinrock, Optimal transmission ranges for randomly distributed packet radio terminals, IEEE Trans. Commun. vol COM-32, pp246-257, Mar.1984.