Self-Adjusting Transmission Range Control of Mobile Hosts in Ad Hoc Wireless Networks for Stable Communication

Krishna Paul[1], S. Bandyopadhyay[2]

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

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

Abstract. There has been a growing interest in mobile, multi-hop wireless networks in recent years. One of the major concerns in this context is to design a communication protocol that provides QoS guarantee. Because of mobility, a node involved in the communication process may move out of the fixed transmission range of the sender, thus disturbing the communication process. In this paper, a mechanism is proposed based on self-adjusting variable transmission range of mobile hosts, which will not allow this to happen during a communication process. At the same time, variable transmission range of mobile hosts will allow us to control the congestion of control packets in a dynamic setting which would in turn reduce the end-to-end delay in data communication.

1. Introduction

There has been a growing interest in mobile, multi-hop wireless networks in recent years. Such a network can be envisioned as a collection of routers, equipped with wireless transceiver, which are free to move about arbitrarily. These networks are also termed as ad-hoc network [1,2,3,4,5] where the network 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 operating without any base-station or any centralized control. 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 may be able to communicate in multiple hops, if other nodes in the network are willing to forward packets from them. However, the successful operation of an ad-hoc network will be disturbed, if an intermediate node, participating in a communication between two other nodes, moves out of range in between message transfer. The situation is worse, if no other path exists between the source and destination nodes.

Thus, an important concern is to design a communication protocol that provides QoS guarantee in this context.

To achieve this objective, we propose a communication protocol, which will allow a path to be retained during a data communication along that path. Because of mobility, a node involved in the communication process may move out of the fixed transmission range of the sender, thus disturbing the communication process. Our mechanism is based on self-adjusting variable transmission range of mobile hosts, which will not allow this to happen during a communication process. At the same time, variable transmission range of mobile hosts will allow us to control the congestion of control packets in a dynamic setting. It has been observed that a low transmission range will not guarantee proper connectivity among mobile hosts to ensure effective communication. On the other hand, if the transmission range is high, it will ensure connectivity but will increase collision and congestion of control packets, which will increase the end-to-end delay significantly. For a fixed number of nodes uniformly distributed over an operating area, an optimal transmission range can be worked out. But in an ad hoc network environment, the number of nodes as well as the concentration of node in different area of the operating zone varies. Hence, a protocol based on variable transmission range would be highly effective in such a dynamic environment.

The protocol is based on a neighborhood agreement/denial scheme through periodic beacon exchange among the neighboring nodes only. The basic assumption is that, even if a node is within the transmission range of another node, it will not be considered as its neighbor unless both of them agrees to be the neighbor of each other. On the other hand, a node can increase its transmission range to include someone as its neighbor. A node will vary its transmission range so that the number of its registered neighbor is six. It has been pointed out earlier [8,9] that if the number of neighbor is six or more, it will guarantee the broadcast percolation throughout the network. At the same time, by adjusting the transmission range, a node-pair will try to maintain their neighborhood relationship i.e. protect the link between them, if that link is involved in a communication process at that instant of time.

2. Related Work

The existing routing protocols in ad hoc networks can be classified either as proactive or as reactive [1]. In proactive protocols, the routing information within the network is always known beforehand through continuous route updates. The distance vector and link state protocols are examples of proactive scheme. An example of proactive routing methods in ad hoc network environment is [6]. However, these methods require to know the topology of the entire network and this information needs to be propagated through the network. In a highly dynamic environment, these schemes are less efficient.

Reactive protocols, on the other hand, invoke a route discovery procedure on demand only. The family of classical flooding algorithms belongs to this group. Examples of reactive protocols in the context of ad hoc networks are [2,3,4,5]. 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, consequently the actual data transmission is delayed until the route is determined. The associated problems and requirements in the context of routing in ad-hoc network has been illustrated in [7].

However, most of these algorithms do not take into account the stability factor of a path. Routing optimality (i.e. selecting a shortest path) is of less important in the context of ad-hoc network. Whatever may be the routing scheme, frequent interruption in a selected route would degrade the performance in terms of quality of service. The idea of selecting stable routes within a dynamic network has been proposed in [4,5]. However, in these methods, stability is not explicitly evaluated in order to predict the life-span of a link in a specific context.

Thus, all the existing routing schemes proposed in the context of ad hoc networks suffer from three major limitations:

- First, because of the mobility of intermediate node(s), there is a need for route maintenance during data communication from a source to a destination. In case of high mobility, these schemes cannot avoid frequent interruption in service that would degrade the performance.
- Second, all of the schemes assume that the transmission range is fixed and is a given parameter. It has been observed that a low transmission range will not guarantee proper connectivity among mobile hosts to ensure effective communication. On the other hand, if the transmission range is high, it will ensure connectivity but will increase collision and congestion of control packets, which will increase the end-to-end delay significantly. Hence, for a fixed transmission range, if the node density is low, the network would be partitioned into disjoint components and proper network connectivity cannot be ensured. On the other hand, if the node density is high, the congestion and collision due to control packets propagation will increase.
- Third, the routing schemes based on fixed transmission range cannot optimize connectivity and congestion control and, therefore, cannot ensure balanced consumption of battery power of the mobile hosts.

The communication protocol proposed in this paper addresses these three limitations and uses a mechanism based on self-adjusting transmission range control of mobile nodes. The usefulness of transmission range control in the context of packet radio network has been proposed earlier [10]. However, there was no complete proposal on the communication protocol in order to achieve any of the above objectives. Moreover, they focussed on transmission range control based on nearest neighbor only that will not guarantee proper connectivity of the network.

3. System Description

The network is modelled 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. In a wireless environment, each node n has a wireless transmitter range

R_n . If a node m is within the transmission range of n, then n and m are assumed to be connected by a unidirectional links $l_{nm} \in L$, such that whenever n broadcasts a message, it will be received by m via l_{nm}. Similarly, If n is within the transmission range of m, then m and n are assumed to be connected by a unidirectional links $l_{mn} \in L$, such that whenever m broadcasts a message, it will be received by n via l_{mn}

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.

We define the strength of relationship between two nodes over a period of time as *affinity*. *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. Thus, the stability of connectivity between n and m depends on a_{nm}. To find out the affinity a_{nm} , node m samples the strength of signals received from node n periodically. Since the signal strength of n as perceived by m is is a function $f(R_n, d_{nm})$ where R_n is the transmission range of n, and d_{nm} is the current distance between n and m, we can predict the current distance d_{nm} at time t between n and m. If V is the average velocity of the nodes, the worst-case affinity a_{nm} at time t is $(R_n-d_{nm})/V$, assuming that at time t, the node m has started moving outwards with an average velocity V. For example, If the transmission range of n is 300 meters, the average velocity is 10m/sec and current distance between n and m is 100 meters, the life-span of link l_{nm} (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 from any node i to another node m as p = (i, j, k, …, l, m), the *stability of path p* 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, $\eta^p_{sd,}$ is given by
$\eta^p_{sd} = \min [_{\forall i,j} a^p_{ij}]$.

We define a node m as a *neighbor of n* and vice versa if and only if both n and m are within the transmission range of each other and there is a neighborhood agreement (to be discussed later) between n and m.

4. A Protocol Based on Self-Adjusting Transmission Range

4.1 Transmission Range Control Protocol (TRCP)

The main features of TRCP are i) to maintain the number of registered neighbors for each node as six; and, ii) to protect a neighborhood relationship, if required, during data communication.

A node having less than six neighbors will increase its transmission range in steps of 20 and sends a neighborhood request to other nodes. If they respond, then the requesting node selects some/all of them and thus establishes neighborhood agreements with them. A node having more than six neighbor will retain its six ‘closest’ neighbor, adjust its transmission range and de-registers others as its neighbor. However, before de-registering, it will check whether that node is

currently involved in communication. If yes, it will not exclude it as its neighbor until the communication is over.

Each node will use the following format to send messages:

Sender_id	Message_Type (REQ/ACK)	Target_Node	Trans.Range of Sender

If the message_Type is REQ, the Target_Node field will be null, since REQ is for all the nodes within the transmission range of the sender.

Each node maintains two tables: A Message_table to accumulate messages received from other nodes; and, a Neighborhood_Table (NT) that contains the updated neighborhood status. The routing algorithm for data communication (to be discussed later) uses NT to get the neighborhood information in order to forward data/control packets.

Whenever a node receives a message, it appends it in MT. Periodically (say, every 500 ms.) the node will process MT, update NT accordingly, adjust its transmission range and sends messages to other nodes.

The structure of MT is same as the format of the messages. The structure of NT in node i is given below :

Neighbor_id	Distance from i	Flag	Status	Whether Protected (True/False)		
				True for Comm_id 1	… ..	True for Comm_id n

MT has two components : the first four fields are used to maintain the neighborhood information; the last field indicates whether the link between i and neighbor_id needs to be protected due to data communication. The same link may be used in multiple data communication simultaneously. If this link is selected for a data communication with a communication id , the Start_data_comm packet will set that flag true. End_data_comm packet will set it to false. This is discussed in section 4.3.

Each node periodically sends the following messages to establish, retain or deny a neighborhood relationships with other nodes:

Neighborhood Establishment: If a node i wishes to have more neighbor, it increases its transmission range in steps of 20 and sends a REQ message to all the nodes within its transmission range. If a receiving node j wishes to respond to this request, it sends a ACK message to i. If i is not within the transmission range of j and if j still wishes to respond, it adjusts its transmission range to include i and sends a ACK message to i. If a node having six neighbors receives requests for neighborhood from other nodes, it will accept only one request (request from the "closest" node) and de-register one existing neighbor (the furthest neighbor that is not involved in a communication process at that instant of time).

Neighborhood Retention: If a node i wishes to retain its neighbor j, it sends a ACK message to j. If j is not within the transmission range of i and if i still wishes to retain j, it adjusts its transmission range to include j before sending a ACK message.

Neighborhood Denial: If a node i wishes to de-register its neighbor j, it stops sending ACK message to j. If j does not receive ACK from i for two consecutive cycle (the field *flag* in NT is used to track this), it will de-register i as its neighbor.

4.2 Path Finding Protocol (PFP)

In this scheme, a source initiates a route discovery request when it needs to send data to a destination. The source broadcasts a route request packet. All the nodes within the transmission range of the source will receive this. 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 n which is decrement at each hop as it propagates. When n=0, the search process terminates. The count n thus limits the number of intermediate nodes (hop-count) in a path.

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

1. If the receiving node is not a registered neighbor of the node generating the packet, discard the route request packet.
2. If the node is the destination node, return a route reply packet to the source along the selected route, as given in the route record that now contains the complete path information between source and destination.
3. Otherwise, if n=0, discard the route request packet.
4. Otherwise, if this node id is already listed in the route record in the request, discard the route request packet (to avoid looping).
5. Otherwise, decrement n by 1, 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 of its up-link and down-link and propagates the packet to the next node listed in the route record to reach the source node.

4.3 Path Evaluation and Data Communication Protocol (DCP)

As discussed earlier, quality of service in 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 and a new path needs to be searched. Our mechanism is based on self-adjusting variable transmission range of mobile hosts, which will not allow this to happen during a communication process. By adjusting the transmission range, a node-pair will try to maintain their neighborhood relationship i.e. protect the link between them, if that link is involved in a communication process at that instant of time. In the worst case, if two nodes are moving away from each other, both of them have to progressively increase their transmission range in order to protect the link between them. In order to protect a path during data communication, all of the node-pairs in the path have to protect their links by adjusting their transmission range.

Let us assume that a source s wants to send NUM number of packets to a destination d. The source s initiates a route discovery request and it waits for the route reply until timeout. After timeout, the source evaluates all the paths in order to evaluate the "best" path for data communication. The best path is a path where the path protection mechanism during data communication will consume the least battery power during the adjustment of their transmission range.

Suppose that source s and destination d are connected by two intermediate nodes j and k. The current transmission range of s, j, k and d are R_s, R_j, R_k and R_d and the current distances between nodes are d_{sj}, d_{jk} and d_{kd}. The following steps are performed :

- Compute the stability required : If NUM number of packets need to be communicated from s to d, then the stability
  η = number of hops * $(\sum_{k=1}^{NUM} t_p) / f$, where t_p is the average hop-delay and f is the correction factor to take care of congestion (typically, f=0.7 to 0.9, depending on traffic volume).

- Compute the affinity required for each link ; affinity required for each link should be at least equal to η. So, the final transmission range of each node should be sufficient to deliver this affinity value.
- Compute the final transmission range required by each node to achieve the affinity :
  If v is the average velocity, then
  $NewR_s = \eta * v + d_{sj}$
  $NewR_j = \max((\eta * v + d_{sj}), (\eta * v + d_{jk}))$
  $NewR_k = \max((\eta * v + d_{jk}), (\eta * v + d_{kd}))$
  $NewR_d = \eta * v + d_{kd}$
  If any one of ($NewR_s$, $NewR_j$, $NewR_k$, $NewR_d$) > Maximum transmission range R_{max}, then reject the path and go to the next path.
- For all selected paths, Compute the sum of deviations from R_{max} and average :
  $\Delta R_p = ((R_{max} - NewR_s)+(R_{max} - NewR_j)+(R_{max} - NewR_k)+(R_{max} - NewR_d))/4$
- The best path is the path with $\max(\Delta R_p)$.

The data communication from source to destination starts with a Start_data_comm packet. The purpose of this packet is to set *protect* field in the NTs of intermediate nodes including s and d with a communication_id. On receiving the acknowledgment from designation, the data communication will start. If no acknowledgment is received within a specified time-out period, the *protect* field in NTs will be reset and the source starts the same procedure with the second best path. On completion of the data communication, an End_data_comm packet will reset the *protect* field, thus releasing the path.

5. Conclusion

We are in the process of evaluating the performance of the proposed scheme on a simulated environment under a variety of conditions. The routing algorithms proposed here are implemented to study a large range of cases by varying a set of

parameters, including: number of nodes, transmission range, pattern and speed of individual node movement, session length, number of nodes initiating communication in a given time-interval, volume of data to be transferred between a given source/destination pair. The preliminary results indicate three distinct advantages over existing routing protocols proposed in the context of ad-hoc networks. First, the proposed scheme eliminates the need for route maintenance during data communication, even if we want to send large volume of data from a source to a destination. Second, self-adjusting transmission range is adaptive to increase or decrease of number of nodes and this will help us to ensure network connectivity on one hand and to control the congestion due to control packets propagation on the other. Third, adaptive transmission range will ensure balanced consumption of battery power of the mobile hosts.

References

1. Z. J. Haas, Milcom'97 Panel on Ad-hoc Networks, http://www.ee.cornell.edu/~haas/milcom_panel.html
2. 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.
3. 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.
4. C-K Toh, A novel distributed routing protocol to support ad-hoc mobile computing, IEEE International Phoenix Conference on Computer & Communications (IPCCC'96).
5. R. Dube, C.D. Rais, K. Wang and S.K. Tripathi, Signal stability based adaptive routing for ad hoc mobile networks, Technical Report CS-TR-3646, UMIACS-TR-96-34, Institute for Advanced Computer Studies, Department of Computer Science, University of Maryland, College Park, MD 20742, USA, August, 1996.
6. C. Perkins and P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing for mobile computers, Proc. of the ACM SIGCOMM, October 1994.
7. S. Corson, J. Macker and S. Batsell, Architectural considerations for mobile mesh networking, Internet Draft RFC Version 2, May 1996.
8. H.Takagi and L.Kleinrock, Optimal transmission ranges for randomly distributed packet radio terminals, IEEE Trans. Commun. vol COM-32, pp246-257, Mar.1984.
9. Y.C.Cheng and T.G.Robertazzi, Critical connectivity phenomena in multihop radio network, IEEE Trans. Commun. , 37(1989), pp 770-777.
10. T.C.Hou and V.O.K.Li, Transmission range control in multihop packet radio network, IEEE Trans. Commun. 34 (1986), pp 38-44.