Toward an Efficient Solution for Dynamic Ad Hoc Network Interoperability

D. Prince, A.C. Scott and W.D. Shepherd
Distributed Multimedia Research Group
Computing Department
Lancaster University, UK
{d.prince, acs, doug}@comp.lancs.ac.uk

***Abstract* – An *ad hoc* network is formed by an impromptu grouping of network capable nodes. The nodes forming the network have unconstrained mobility, and so provide a dynamic network topology. Current work in this research area has focused on designing routing protocols capable of efficiently forwarding packets in these dynamic network environments. This has led to several designs for ad hoc routing protocols based on various routing algorithms, each suited to specific usage characteristics.**

This paper will discuss issues relating to routing in ad hoc networks. We will describe an active networking based solution that provides dynamic routing protocol interoperability and enables migration of nodes between ad hoc groups. Our design is motivated by a s*quad and base* scenario which consists of two groups wishing to communicate. These groups have contrasting deployment characteristics and so use different routing protocols.

I Introduction

Owning a PDA style computing device is common place in today's society because the price-performance ratio of these devices is continually falling. Increasingly PDAs are being equipped with, or provide functionality to access, wireless LAN interfaces, allowing users to form temporary, but highly dynamic, *ad hoc* networks. Due to these developments the IETF established the Mobile Ad hoc NETwork (MANET) Working Group (WG)[1] to examine the issues relating to network layer connectivity in ad hoc networks with the aim of developing routing protocols and introduce them onto the IETF standards track. The MANET WG describes an Ad hoc network as:

"… an autonomous system of mobile routers (and associated hosts) connected by wireless links—the union of which forms and arbitrary graph."[1]

The work performed by members of the working group has resulted in the development of several drafts for differing routing protocols. Due to the underlying design concepts, these protocols provide different performance characteristics, as shown in simulations carried out in [2,3], but all aim to provide the optimum packet forwarding strategy for an erratic network topology. Due to the differences in characteristics, there is no single panacea ad hoc routing protocol. Instead protocols provide solutions for facets of the overall ad hoc routing problem. The diversity of protocols makes it possible for protocols to be selected based on their characteristics for different ad hoc deployment scenarios. This poses an interesting interoperability issue.

An ad hoc network as an entity is mobile, making it possible for two ad hoc networks, using differing routing protocols, to come into contact with each other. If the two groups wish to communicate, nodes that are physically connected to both groups must perform protocol bridging services. In addition, as the nodes forming the groups are individually mobile, they have the ability to migrate between groups. If a node is to perform bridging services for, or migrates between, networks it must determine, and possibly download and install the new routing protocol.

This paper is organised as follows. Firstly we discuss some of the issues relating to routing in ad hoc networks. We then present a *squad and base* scenario which discusses the problem of two interacting ad hoc groups. We subsequently describe a design for an active network system that solves the problems posed by the *squad and base* scenario. We conclude by discussing the issues involved in designing such a system.

II Overview of Ad Hoc Networking

Ad hoc networks are wireless multi-hop data networks formed in an unorganised manner by a set

of mobile nodes that wish to communicate with each other. Typically there is no core infrastructure, such as wireless base stations or DNS servers, to rely on for network management services which means the network must be both self sufficient and self organising.

In multi-hop networks nodes rely on their neighbours to forward packets on their behalf. In Figure 1 if node A wants to contact any node other than B or C, it must rely on C to forward packets to the destination as only C is common to all nodes.

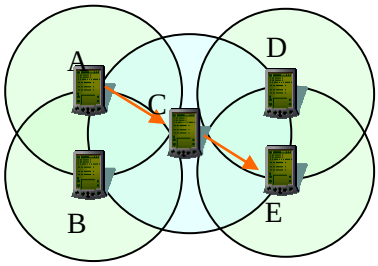

Figure 1 - A Route From A to E Through C.

However, due to the mobility of the nodes in an ad hoc network a global view of the network is unobtainable making it impossible to directly know that node C can connect A to E or D. Ad hoc routing protocols provide mechanisms to discover paths through the multi-hop structure to connect source and destination nodes.

The unrestricted mobility of the nodes forming an ad hoc network means that links in the multi-hop network are constantly being broken and formed as nodes change their positions relative to each other. A simple example of a topology change, caused by node movements, is if node E in Figure 1 is allowed to roam into a position shown in Figure 2.

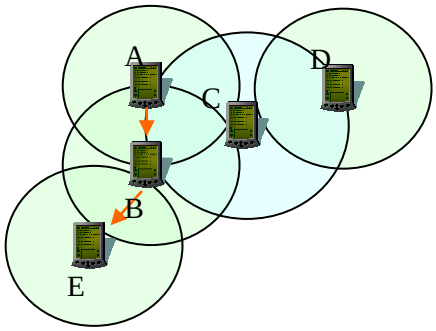

Figure 2 - New Route for A to E Communications after E has Moved.

This movement would result in the route A has for reaching E through C being removed and a new route using B being established. It can be seen from the previous example that any node in an ad hoc network may be called upon to act as a router for another node.

The wireless links connecting the nodes can suffer from signal degradation caused by environmental conditions. Extreme degradation can lead to complete signal loss, causing links to break, or partial loss, causing links to become unidirectional resulting in asymmetric routes. The inconstancy of links, via physical degradation or movement, means that the structure of an ad hoc network is prone to drastic and unpredictable changes with a frequency much greater than seen in the Internet today. A routing protocol designed for use in ad hoc networks must be able to efficiently track the rate of change in the network.

The most commonly cited scenarios that motivate ad hoc network research are military or civil emergencies and business meetings. The simplest type of ad hoc network is represented by a business meeting scenario. In this situation a group of people wish to connect their device forming a temporary network to perform collaborative work. Very little may be known about the nodes taking part in the network or the structure that the network will have before it is instantiated. The emergency scenario is where a data network has to be rapidly deployed and where the majority of the nodes comprising the network are constantly mobile and prone to unpredictable movement due to the volatile nature of the situation that the users find themselves in.

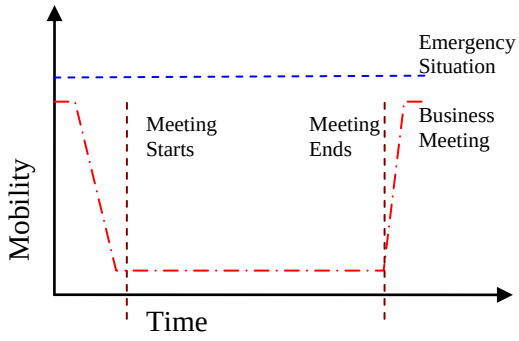

Figure 3 - Temporal Mobility Relationships for Common ad hoc Scenarios

These two scenarios represent two extremes of node mobility. If the level of node mobility is compared to time for each scenario, as shown in Figure 3, the nodes in the emergency situation have relatively constant mobility over the lifetime of the network.

In the business meeting scenario, initially the mobility of the nodes is high as the users organise themselves in a seating arrangement, but as soon as the group of users start to work the level of mobility drops and remains at a low level while the meeting takes place.

There are three classes of routing algorithm which could be considered when developing a routing algorithm, Link State, Distance Vector and Source Routing[4]. Link State routing algorithms attempt to keep a routing table for the complete topology of the network. In an ad hoc network it would be impossible to keep an up to date view of the network topology due to the frequent node movements and so Link State algorithms are not commonly used.

The Distance Vector algorithm is distributed, using a routing table on each routing node in the network containing information about the next hop to a specific destination. A cost metric is associated with each route which is used to calculate the appropriate route to the destination. These estimated costs are broadcast to all of the router's neighbours and so routing information is propagated across the whole network.

Source Routing takes a very different approach to the first two as it uses a source routing header containing a list of nodes through which the packet must pass to reach the destination. In this way the routing information is contained in the packet. However, there is an associated packet overhead for all of the routing information in the packet, which can reduce the space for payload data in large networks. Along with the packet overhead there is still the associated bandwidth overhead for route discovery messages.

Furthermore, protocols can be classified as either Table Driven or On Demand. Table Driven protocols are generally pro-active in trying to maintain routes to all nodes in the network. They actively attempt to update their routing tables regardless of whether the routes are actually being used. On Demand protocols are reactive, waiting for a request to send a packet to the destination and then attempt to discover a route for it.

III Problem Scenario

The motivation for this work is a *squad and base* scenario. The *squad* is a small group of 10 to 30 highly dynamic users. The dynamism of users in the group causes the ad hoc network formed by their computing devices, to be highly erratic. One or more of the nodes in the network may have an interface which provides access to a wide area communications infrastructure, allowing contact with other groups located at a distance. The routes available in this network will be limited due to the small number of nodes comprising the network, and as a result of the unpredictable movement of the nodes, the links are likely to break.

The *base* user group is formed by large numbers of users who are much more static than the squad users. The ad hoc data network formed by the nodes is much more stable than the squads and has a larger number of possible routes between destinations due to its size. The base network may have access to some form of core infrastructure, but would have access to the same wide area communications infrastructure used by the squad networks. The core network provides gateway connections and some management functionality, such as DNS server etc.

When the squads are away from their base they would connect to the base via the wide area network and form subnets from the bases address space. Nodes at the base would form one or more ad hoc networks which hang off the core infrastructure. The squad and base elements provide contrasting operational characteristics and so force the use of routing protocols designed for their specific situations. It also makes it necessary for certain nodes to route between their interfaces to provide connectivity to other groups.

When a squad group returns to the base group it is likely that the users from it will disperse into the base group. In this situation it is possible that the most logical route for a data packet would be through nodes in the base group that may be running a different routing protocol. The nodes in the squad must migrate to the base routing protocol allowing the squad and the base networks to coalesce.

Alternatively a squad may remain at the fringes of the base network but wish to communicate directly with it rather than using the wide area communications infrastructure. In this situation, nodes that can physically contact each network must perform protocol bridging services by disseminating

routes from one protocol to the other and allowing the routes to propagate correctly inside the networks.

IV The System Design

What the authors propose, is a solution comprising a lightweight active networking environment, a routing protocol discovery mechanism, and a protocol manager. Figure 4 shows a simple representation of the system.

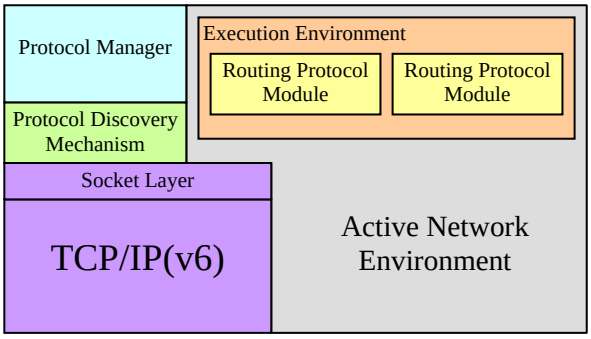

Figure 4 - System Overview

When a mobile node comes into contact with a new ad hoc network, it must determine the routing protocol used by the network and what the characteristics of that protocol are. The Routing Protocol Discovery Mechanism provides the functionality to do this. The mechanism has two phases of operation. Initially it determines whether a new node that has been detected connecting to the physical link, i.e. come into radio range, uses the same routing protocol. This can be done actively or passively. If this process is done actively a messaging scheme is used to establish whether the two nodes wish to interact and if so, whether they are using differing protocols.

The preferred method is the passive mechanism. This method uses any inbuilt link local signalling messages that a routing protocol has to determine whether another node is using the same protocol. Many designs for ad hoc routing protocols specify messages intended to detect the connectivity of another node on the same link. The Ad hoc On-Demand Distance Vector[5] (AODV) routing protocol specifies the use of HELLO messages for this purpose. If neighbouring nodes do not respond to these messages then it is usually assumed that the link to them is broken. If nodes are using different routing protocols then the connection is broken, not at the link layer, but at the network layer. Detection is performed by specifying that implementations of routing protocols that use link local signalling provide event notifications for any messages sent but a response has not returned in the specified limit. Alternatively, ICMP messages can be monitored to see if the other node responds with an indication that there is not a process currently bound to the port that the protocol would normally use.

Once it has been determined that the two nodes are running differing protocols the discovery system exchanges metadata describing the routing protocols that are currently being used. This requires routing code modules to carry accompanying metadata descriptions containing information such as operational parameters and code signatures, or other authentication tokens. This information is used by the Protocol Manager as part of the input into its decision mechanism.

The Protocol Manager decides how the node should interact with the network that has recently been discovered. The protocol manager contains two elements, a profiler and a rule based system. The profiler records the interaction that nodes have with networks. For example, if a node is in an ad hoc network but becomes disconnected from the other members due to the users dispersing into a new group, then the profiler would record this as the networks coalesced due to all of the nodes migrating to the new network. If this type of interaction repeats itself over time it can be predicted that the interaction will happen again if the same network is seen. The rule based system decides what course of interaction the node should take.

The rule based system can produce two different outcomes based on the profiler information, the node should migrate to the new network or, the node should act as a protocol bridge between networks. The node should migrate straight away when not currently in a network or if it is clear from previous interactions with this network that the node would move normally move to the network. The nodes decision to perform protocol bridging is based on the current network situation, i.e. already in an ad hoc network, and on evidence of previous interactions provide by the profiler. It will also temporarily bridge if the network has not been seen before or it is not clear whether to migrate or not, and adopts a *wait and see* state waiting for the final outcome of this interaction. If the node bridges or

migrates, it is necessary to obtain the routing protocol that the new network is using.

The protocol manager uses the active network environment to download and instantiate the new routing protocols. The active network environment provides safe execution environments for code to run allowing two or more routing protocols to run simultaneously so that they can perform protocol bridging using the same address space. The platform provides access to system level functions such as packet queues and sockets, in a secure and safe manner.

V Design Issues

The current design for the system is still in its infancy. However, initial work has identified some key design issues. As mentioned earlier, the profiler records information about the interactions that a node has with networks. The type of information that needs to be recorded must include the networks encountered and the result of that encounter. Identifying a network is problematic as factors such as structure or addresses cannot be relied on to be constant in ad hoc networking. The structure of an ad hoc network is constantly changing and although identifiers such as subnet number and the type of protocol can be used, many ad hoc addressing schemes use site scoped addresses when the group is not connected via a gateway to a globally addressable network. If a network is using site scoped addresses a node may wrongly identifying a network, causing a wrong decision to be made.

Other information on the state of the network that the node is currently in may also be necessary to determine whether the node can use a routing protocol effectively. As the profiler keeps historical data a situation can arise where a node joins a new network and has no prior historical knowledge of the network. A mechanism for distributing this information to new nodes may be necessary so that new nodes can make accurate decisions on the group's behalf.

The selection of the rules for the rule based system of the Protocol Manager is key to successful operation of the system. The rules must effectively choose the correct course of action, with only minimal input from the user, and ensure convergence on a single solution for every node.

In [2] the authors discuss numerous factors that can be measured when comparing two ad hoc routing protocols. These include factors such as, routing packet overhead and MAC overhead for example. These results should be included as part of the metadata describing the protocol optimum operational parameters. Additionally, security information is required to enable the active network environment to authenticate the routing code module. The presentation of the data and what the data has to include is still undecided.

In the squad and base scenario, certain nodes within a squad have interfaces that can access a wide area infrastructure. Handling these multi-interface devices is interesting when the nodes coalesce into one group and one flat network. Essentially a secondary network with different operating parameters is layered on top of another. This concept is shown in Figure 5. In this situation there would be a high bandwidth, high latency (due to hop count), network and another network which has low latency and low bandwidth. It may be possible for the proposed system to capitalise on this secondary network by providing mechanisms to manage the routing table population etc, to provide efficient network load balancing or QoS mechanisms.

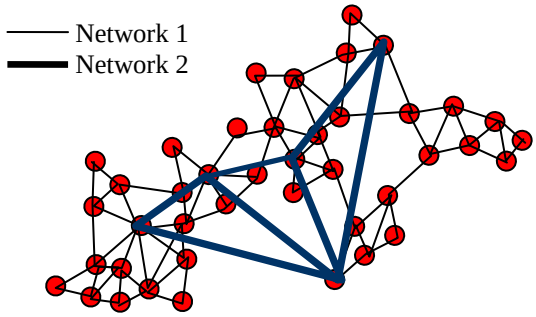

Figure 5 – Two networks, one overlaid on the other.

The LARA++ architecture has been developed at Lancaster University to provide a programmable network node using a component architecture [6].The design of the active network environment will use the same interfaces and code download mechanism as those present by the LARA++ system. This will enable an ad hoc network using the proposed system to download the routing protocol that it is using onto static infrastructure devices, allowing routes from the ad hoc network to propagate. This would enable an ad hoc network to attach to a core infrastructure dynamically and be globally routable.

VI Conclusion

The system presented in this paper provides a low configuration mechanism to allow ad hoc networks to interact even when the networks are running different protocols. The system also facilitates the migration of one or more nodes from one ad hoc network to another using a rule based system taking as inputs historical data about the nodes previous network interactions. The use of active network technologies provides the download and instantiation of new routing protocols dynamically and safe execution environments.

The ability to dynamically install new routing protocols for ad hoc networks as and when they are needed allows a mobile node to be unconstrained at the network interaction level as well as physical mobility level. Through this next generation network users will be able to easily and quickly adapt to new network situations as an when they like.

References:

1. Mobile Ad hoc Networks (MANET) Charter, http://www.ietf.org/html.charters/manet-charter.html, Chairs: J. Macker and S. Corson, 2002.
2. Charles E. Perkins et al., "Performance Comparision of Two On-Demand Routing Protocols for Ad Hoc Networks", IEEE Personal Communications, 2001.
3. J. Broch et al., "A Performance Comparison of Multihop Wireless Ad Hoc Network Routing Protocols", Proc. IEEE/ACM MOBICOM '98, Oct. 1998.
4. Tanenbaum S. "Computer Networks 3rd Edition", Prentice Hall, 1996.
5. C. E. Perkins, E. M. Royer, and S. R. Das, "Ad Hoc on Demand Distance Vector (AODV) Routing, http://www.ietf.org/internet-drafts/draft-ietfmanet-aodv-10.txt, IETF Internet Draft, 2002, work in progress.
6. S. Schmid et al., "Component-Based Active Network Architecture", In Proc. of 6th IEEE Symposium on Computers and Communications, 2001.