

State of the Art: Ad Hoc Networking

John Paul O Grady/ Aidan McDonald
Adaptive Wireless Systems Group
Cork Institute of Technology

1 Introduction

Ad Hoc networks are multi-hop wireless networks where nodes may be mobile. These types of networks are used in situations where temporary network connectivity is needed. Ad hoc networks are formed on a dynamic basis, i.e. a number of users may wish to exchange information and services between each other on an ad hoc basis, in order to do this they will need to form an Ad Hoc network. An example of this may be found in a disaster relief situation. Here an Ad Hoc network could enable emergency services to co-ordinate emergency services more effectively or enable medics in the field to retrieve patient history from hospital databases (assuming that one or more of the nodes in the Ad Hoc network has connectivity to the Internet).

Smart spaces are defined as environments that allow people to perform tasks efficiently by offering unprecedented levels of access to information and assistance from computers. Ad Hoc networks will play a significant part in these environments, allowing people to exchange information and services; for example, people at a meeting could create an Ad Hoc network using their PDA's or Laptops and exchange information relevant to the meeting. Indeed there are endless examples of where their use could be found.

2 Overview

The two areas of Ad Hoc networking that we mainly researched were IP routing and dynamic configuration of IP addresses in Ad Hoc networks. Routing in Ad Hoc environment is different compared to normal wired networks. This is mainly due to two factors

- The bandwidth restriction due to the use of wireless connections
- Rapid change in network topology due to node movements

In our analysis of IP routing we present the advantages and disadvantages of the various types of IP routing protocols proposed for Ad Hoc networks.

Most of the research conducted in the area of Ad Hoc networking to date has focused on solving the routing problem, however the problem of dynamic configuration of IP addresses has yet to be addressed.

Two methods can be used to configure an IP addresses, manual configuration and dynamic configuration. Since an Ad Hoc network is highly dynamic by nature, manual configuration can't be used, as it would take away from the dynamic nature of the network. This means that dynamic configuration is required; in wired networking dynamic configuration is achieved using Dynamic Host Configuration Protocol (DHCP). DHCP however can't be used in Ad Hoc networks, in our analysis of

the area we present the reasons why as well as investigating the various protocols proposed for dynamic configuration of IP addresses in Ad Hoc networks.

3 Analysis

3.1 *IP Routing in Ad Hoc Networks*

An Ad Hoc network (also called a Mobile Ad Hoc Network MANET) consists of wireless hosts that move around, i.e. they have no permanent physical location. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes before the exchange of IP data packets. Below is a brief overview of IP routing in an Ad Hoc environment. There are many papers dealing with routing in Ad Hoc networks. If a more detailed review is required we have a summary of Ad Hoc routing protocols written by Susan Rea who is a PhD candidate student and a member of the Adaptive Wireless Systems Research Group at CIT.

The routing protocols in Ad Hoc wireless networks are generally categorised as

3.1.1 Proactive

These protocols require each node to maintain one or more tables to store up to date routing information and to propagate updates throughout the network. These protocols try and maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronise the tables.

Some examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) [1], Optimized Link State Routing Protocol (OLSR) [2] and Fisheye State Routing Protocol (FSR) [3]. These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

The problem with these protocols is the overhead; the protocols propagate and maintain routing information, regardless of whether or not it is needed.

3.1.2 Reactive

These protocols create routes only when desired by a source node, therefore a route discovery process is required within the network. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible or until the route isn't needed any longer.

Some examples of source initiated ad hoc routing protocols include the Dynamic Source Routing Protocol (DSR) [4], Ad Hoc On Demand Distance Vector Routing Protocol (AODV) [5], and Temporally-Ordered Routing Algorithm (TORA) [6]. No periodic updates are required for these protocols but routing information is only available when needed.

3.1.3 Hybrid

These protocols try to incorporate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; routing in general can be either flat or hierarchical

In a flat approach, the nodes communicate directly with each other. The problem with this is that it does not scale well, it also does not allow for route aggregation of updates

In a hierarchical approach, the nodes are grouped into clusters, within each cluster there is a cluster head, this acts as a gateway to other clusters, it serves as a sort of default route.

The advantage of a hierarchical structure is that within a cluster, an on demand routing protocol could be used which is more efficient in small-scale networks. For inter cluster communication then a table driven protocol could be used which, would allow the network to scale better. An example of such a hybrid routing protocol is the Zone Routing Protocol (ZRP) [7].

In figure 1.0 below we have two clusters, with one laptop representing the cluster head in each cluster.

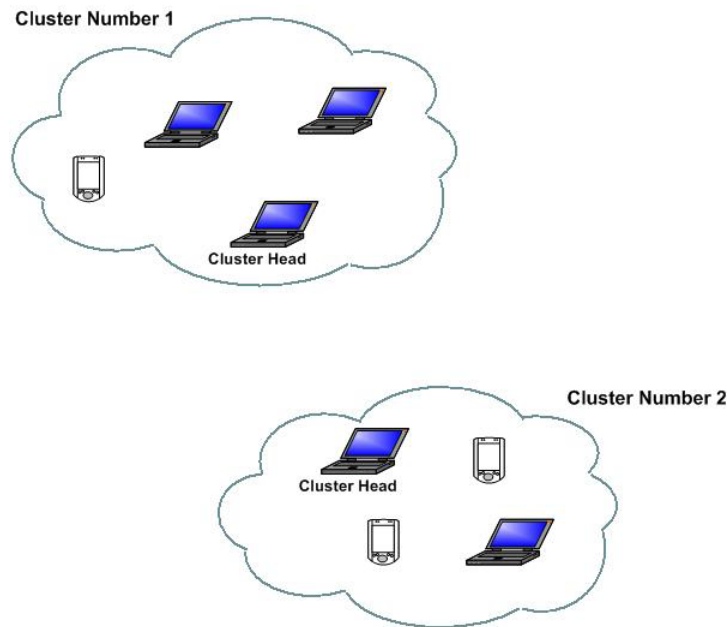


Figure 1.0

3.1.4 Other Types of Routing Protocols

There are many other types of ad hoc routing protocols; one for example LANMAR [8] uses location info, obtained using the Global Positioning System (GPS). By knowing the precise location of a node you can limit the search to a smaller “request zone” of the network.

3.2 Dynamic Configuration of IP Addresses

In order to communicate nodes need IP addresses. Since Ad Hoc networks lack any centralised administration these addresses can't be manually configured, and so must be configured dynamically. In a wired network dynamic configuration is achieved using the Dynamic Host Configuration Protocol (DHCP) [9], however this requires the presence of a centralised DHCP server, which maintains the configuration information of all nodes in the network. Since an Ad Hoc network is devoid of any fixed infrastructure such as a central server, this approach can't be used.

There are a number of issues to consider:

- As regards the auto-configuration, the process is simpler in IPv6 compared to IPv4. It is easier to create globally unique addresses in IPv6; because IPv6 addresses are 128-bit addresses compared to IPv4's 32-bit. The MAC (48-bit) address or some other unique identifier for example could be embedded into the address to ensure the address is unique.
- In IPv6 there is also a process called [10] "IPv6 Stateless Address Auto Configuration" this is a process used to create unique link local addresses in the absence of a DHCP server. This process has to be modified for use in ad hoc networks, since ad hoc addresses need network wide uniqueness. A number of papers "Wireless Multi-hop Internet access: Gateway Discovery, Routing, and Addressing" [11], "IPv6 Auto Configuration in Large Scale Mobile Ad Hoc Networks" [12], "Stateless Address Auto Configuration in Mobile Ad hoc Networks using Site local Addresses" [13] propose a modification of the above technique as a method for dynamic IP address allocation. The problem with these solutions is that they are only applicable to IPv6 and so can't be used in IPv4; this in turn limits the use of these proposals.
- The use of Mobile IP "IP Mobility Support for IPv4" [14], "Mobility Support in IPv6" [15] is also proposed for use in ad hoc networks. In Mobile IP a node has two addresses, its home address and its care of address, when a node is away from its "home address" it obtains a "care of address" and registers that address with its home address. When packets are sent to the nodes home address they are forwarded to its "care of address". A foreign agent is used to assign the care of addresses.
- In order to connect to the Internet, there needs to be a gateway node that has access to the Internet. The other nodes need to discover this node if they want to access the Internet. There are a number of possible ways to discover the gateway, a multicast address could be used, or the gateway could advertise itself. This process could be done proactively or reactively depending on the routing protocol in use. One proposed solution to this problem is outlined in [16] "Global Connectivity for IPv6 Mobile Ad Hoc Networks". Two methods for Internet gateway discovery are proposed here, one method periodically disseminates gateway advertisements to all nodes in the MANET (Mobile Ad Hoc Network); the other utilizes solicitation and advertisement signalling between the MANET node and the gateway. This solution however is only applicable to IPv6, as it utilizes the [10] "IPv6 Stateless Address Auto Configuration" process.

The problem in regard to Internet connectivity for IPv4, is that most of the proposals for dynamic address allocation assumes the use of private addresses, due to the difficulty in obtaining global addresses. There is an issue here in regard to connectivity to the Internet, as some sort of network address translation (NAT) process will be required, this is a process that converts a private address into a unique global address. In the wired environment NAT is achieved using "Traditional Network Translation (NAT)" [17], this is a process that converts a non-unique IP address to a unique IP address. A solution is proposed in "Connectivity for IPv4 Mobile Ad Hoc Networks" [18] however it assumes that each node in the MANET (Mobile Ad Hoc Network) is using Mobile IP and as a result already has a globally unique home address. It assumes that a Foreign Agent assigns "care of addresses" to nodes as they arrive into the network and acts as a gateway for them when they want to connect to the Internet.

- When a node leaves the network, it needs to give up its allocated IP address. A node may leave the network gracefully or it may leave very suddenly, the nodes must recognise that a node has left the network and recover its IP address. Different proposals use different techniques to recognise that a node has left the network. We will outline these techniques in detail later.
- Another problem is the merger of networks. Say you have two networks, both using the same private address (e.g. 10.0.0.0). If these two networks merge, a process must detect this, as there is the possibility that a node in each of the two networks may share the same IP address. If this problem is not addressed routings errors can occur.

If two networks merge, each with different network addresses (e.g. 10.0.0.0 and 157.190.0.0), there will not be a problem in regard to having duplicate addresses. This is because different address spaces are used in each network, and so normal Ad Hoc routing will allow the nodes to communicate with each other. However still the merger of the networks may need to be identified, for example in-service discovery it may be beneficial to know that another network is nearby.

The partition is different, here the network may splits in two, and the allocation scheme must cope with this. It must for example recover any IP addresses that are not being used currently in the network.

3.2.1 Dynamic Allocation Proposals

When a node is assigned an address, it needs to find out whether or not the address it chooses is unique within its network. In order to determine this, a process known as duplicate address detection (DAD) is performed, it is basically a process that determines whether or not a chosen IP address is unique within a chosen network. An overview of different DAD techniques is presented in [19]. Generally the different proposals differ in the technique they use to perform DAD. The proposals fall into two different categories.

Hierarchical Approach

In a hierarchical approach, a clustering technique is used with one node (cluster head) assuming the responsibility for the allocation of addresses to new nodes as they arrive, basically when a new node arrives, he registers with the cluster head, who then allocates a new addresses and coordinates a duplicate address (DAD) process in order to determine whether or not the address chosen is unique within the ad hoc network. The following paper is based on this approach

- Sanet Nesargi, Ravi Prakash. 2002 “MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network” in Proceedings of Infocom 2002. [20]

This paper presents a hierarchical approach to the IP address allocation problem. This paper proposes the use of IPv4 private addresses although IPv6 address could also be used. It does however only consider a stand alone MANET (Mobile Ad Hoc Network) which has no connection to the Internet. Below is an outline of the basic idea.

A new node entering the network, hereafter called the “requester”, chooses a reachable node as the “initiator”, which performs address allocation on its behalf. All other nodes know the route

to the initiator and can forward their responses to it. The initiator chooses an address it perceives as unallocated and attempts to acquire permission from all other nodes in the network to assign the address to the requester. Nodes perceiving this address as unallocated mark the requested address as allocation in progress and reply in affirmative to the initiator. This allocation is made permanent by a second message, which is sent by the initiator if the initiator receives an affirmative response from all nodes in the network. Therefore the IP address allocation is similar to a two-phase commit.

Nodes, which no longer wish to be part of the system, relinquish their address by broadcasting a message to the effect before leaving the network. If a node abruptly leaves the network, i.e. goes down without relinquishing its address, it would fail to respond to the address allocation request by some initiator the next time a requester enters the network. In this case the address of the departed node is cleaned up by the initiator awaiting a reply from the departed node.

This paper also deals with network partitions and mergers. Partitioning of the network is easy to handle, all the nodes in one partition conclude that all the nodes in other partitions have departed abruptly and so reclaim their addresses.

Merging works differently, here a unique partition ID is used. When two nodes come into contact and exchange their partition ID's, they realise that they are different partitions and so merge. To do this they exchange partition ID's as well as the table, which shows all IP addresses that have been allocated. If it is found that nodes in the partitions have the same IP address, then one node gives up its IP address and requests another one.

One issue with this paper is that networks merge even if they have no reason to do so. Also the problem of security has not been addressed.

Flat Topology Approach

In a flat topology approach there is no cluster head, which assumes responsibility for the allocation. Here when a node joins the network and wants an IP address, it chooses an address at random and then performs a duplicate address procedure in order to determine whether or not that address is unique. The papers below present solutions based on this approach

- Perkins et al. Nov 2001. Internet Draft "IP Address Auto-configuration for Ad Hoc Networks, Technical Report. Internet Engineering Task Force, MANET Working Group. [21]

This is the proposal from the IETF MANET (Mobile Ad Hoc Network) working group. The process differs slightly depending on whether you are using IPv4 or IPv6

The process is based on a proactive routing protocol e.g. Ad Hoc On Demand Distance Vector Routing (AODV) [5] and uses a flat structure. In a proactive routing protocol routing is done on an on demand basis, in order to route to a destination a AREQ message is sent out looking for the destination. When the destination is found an AREP message is sent back indicating that the destination is reachable.

A node performing the auto-configuration process picks two addresses, a temporary address and the actual address to use. The former is used only once in the uniqueness check to minimise the possibility for it to be non unique. The unique check is based on sending an address request (AREQ) and expecting an address reply (AREP) back in case the address is not unique. In case no AREP is received, the uniqueness check is passed.

The process differs slightly when using IPv4 or IPv6

IPv4

In this case, a node attempts to select a random address on the network 169.254/16. For IPv4, the messages are Internet Control Message Protocol (ICMP) packets.

IPv6

For IPv6, on the other hand, the AREQ is a modified neighbour solicitation and AREP is a modified neighbour advertisement as specified in the “Neighbour Discovery Protocol for IPv6”[22]

The process for the auto-configuration of IPv6 addresses is based on the “IPv6 Stateless Address Auto-configuration” [10], but with a number of changes. The IPv6 Stateless Address Auto-configuration process specifies a process that can be used to create link local unique addresses in the absence of a DHCP server. Ad hoc networks can't use link local address due to the fact that the addresses are valid over a multiple hop distance, not only to the immediate neighbours, changes need to be made to the process to ensure the addresses are unique within the network.

Internet Connectivity

This process allows for a node to obtain a globally unique IPv6 Address, however obtaining a globally unique IPv4 address is out of its scope. In order to connect to the Internet a gateway node needs to be available. If a gateway node is available a node should be able to connect to the Internet through the “Global Connectivity for IPv6 Mobile Ad Hoc Networks” [16] process.

Problems

The major problem with this proposal is that it does not consider the possibility of merging and partitioning.

- Mansoor Mohsin, Ravi Prakash. 2002 “IP Address Assignment in a Mobile Ad Hoc Network” in Proceedings of Milicom 2002. [23]

This paper uses the concept of binary split in order to perform dynamic configuration. It uses a flat structure; every node can assign an IP address to a new node without consulting any other node in the network.

The paper only considers a stand alone MANET (Mobile Ad Hoc Network), i.e. the network does not have access to the Internet. Below is an outline of the basic idea.

In the beginning, there is only one node in the network that has the entire pool of addresses. When an un-configured node A, wishes to join the network, it requests the nearest configured node, B, for an IP address. Node B assigns the requesting node A an IP address from its pool of IP addresses. It also divides the set of IP addresses into two and gives one half to the requesting node A (keeping the other half for itself)

A node can leave the network either gracefully or abruptly. When node A leaves a network gracefully, it gives its pool of IP addresses to any node B nearby. Node B then has the responsibility for handling this set of addresses. On the other hand, when node A leaves the network abruptly it leads to IP address leak (because there is some IP address that is neither assigned to any node nor available for assignment to an un-configured node). This situation is handled through synchronization. Nodes synchronise from time to time to keep track of the IP addresses assigned and detect any leaks in the available pool of IP addresses.

This paper also addresses the problem of network partitioning and merging through the use of a partition ID. When a new network is formed a new partition ID is created and this ID is passed to new nodes as they join the network. When a node detects that it has been partitioned from the main network through the synchronisation process it assigns itself a new ID.

When two partitions merge there may be a problem as two different nodes in the two partitions may share the same IP address. This paper presents an algorithm which they believe will solve this problem, its details are similar to the “Manetconf: configuration of hosts in mobile ad hoc networks” [20].

One issue with this paper is that networks merge even if they have no reason to do so. Also the problem of security has not been addressed.

- Subir Das, Anthony McAuley, Archan Misra. 2001 “Auto-configuration, registration, and Mobility Management for Pervasive Computing” in IEEE Personal Communications August 2001, pp. 24-31. [24]

Focusing only on the auto-configuration part of this paper only, the paper proposes the Dynamic Registration and Configuration Protocol (DRCP), which tries to extend Dynamic Host Configuration Protocol (DHCP) [9] to a stateless auto-configuration protocol for wired and wireless networks. Basically it presents a distributed DHCP architecture. Each node represents a DRCP client and server and owns an IPv4 address pool. The Dynamic Address Allocation Protocol (DAAP) is responsible for the distribution of the address pools. Each node requesting a pool obtains half of the pool of a neighbouring node. This may lead to a lot of unassigned addresses in the already scarce IPv4 private address space, and subsequently to scalability problems.

The major problem with this proposal is that the problems of network merging, partitioning or Internet connectivity are not considered.

4 Future Directions

Our future research will focus on the dynamic IP address assignment problem associated with Ad Hoc Networking; there are a number of problem areas, which could be further researched.

- **Merging of Networks**
In most of the papers we have seen, the partitioning and merging of networks has not been addressed in detail. One potential area of research here is in the service discovery, if two networks are to merge together there will presumably be a reason to do so, for example one network may offer printing facilities to another network, issues of service discovery are important here. Other potential areas here include methods for detecting partitioning and merging of networks.
- **Security in the auto configuration process** has not been addressed, denial of service attacks are one possible security flaw, one node for example may request all the potential IP addresses available.
- **Internet Connectivity**
This problem is closely related to the routing problem, and the problem differs depending on whether you are using IPv4 or IPv6.
- **The applicability of Mobile IP in Ad Hoc networks?**
- **Routing**
Could the IP address assignment process be optimised for different IP address assignment protocols? For example if a hierarchical routing protocol is used, which utilizes clusters and cluster heads. Would it be more efficient for a hierarchical IP address assignment protocol to use the clusters and cluster heads identified by the routing protocol or to create its own. Also could routing information be used in the address assignment protocol, for example, if a node finds that it cant route information to a particular node, can it assume that that node has left the network? This kind of information could be useful for the IP address assignment protocol as it may allow nodes to identify the departure of a node more quickly.
- **IPv4 vs. IPv6**
Should the IP address assignment solution be independent of IP version in use, i.e. will one solution work for IPv4 and IPv6 or will two different solutions be needed?

5 References

- [1] P. Bhagwat ,C. E. Perkins, 1994 “Highly Dynamic Destination –Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, Proceedings of ACM SIGCOMM’94.
- [2] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, 2002 “Optimized Link State Routing Protocol”, Work in Progress, Internet Draft, MANET Working Group
- [3] M. Gerla, X. Hong, G. Pei, 2001 “Fisheye State Routing Protocol (FSR) for Ad Hoc Networks”, Work in Progress, Internet Draft, MANET Working Group
- [4] Y-C. Hu, J. G. Jetcheva , D. B. Johnson, D. A. Maltz, 2000 “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)” Work in Progress, Internet Draft, MANET Working Group
- [5] C. E. Perkins, E. M. Belding-Royer, S. R. Das, 2001 “Ad Hoc On Demand Distance Vector (AODV) Routing, Work in Progress, Internet Draft, MANET Working Group
- [6] S. Coran V. Park, 2001 “Temporally-Ordered Routing Algorithm (TORA) Version 1 Fundamental Specification”, Work in Progress, Internet Draft, MANET Working Group
- [7] Z. Haas, M. Pearlman, 1997 “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, Work in Progress, Internet Draft, MANET Working Group
- [8] I. Cardei, 2002 “LANMAR: Landmark Routing for Ad Hoc Wireless Networks”, Wireless Networking Seminar, University of Minnesota, February 2002.
- [9] R. Droms 1997 “Dynamic Host Configuration Protocol”. Network Working Group, (Draft Standard) 2131.
- [10] S. Thomson and T.Narten 1998 “IPv6 Stateless Address Auto Configuration” (Draft Standard) 2462. Internet Engineering Task Force.
- [11] Christian Bettstetter and Jin Xi. 2002 “Wireless Multihop Internet access: Gateway Discovery, Routing, and Addressing” in Proceeding of International Conference on Third Generation Wireless and Beyond (2002)
- [12] Kilian Weniger, Martina Zitterbart. 2002 “IPv6 Auto Configuration in Large Scale Mobile Ad Hoc Networks” in Proceedings of European Wireless 2002
- [13] Jung-Soo Park, Yong-Jin Kim, Sung-Woo Park. 2001 “Stateless Address Auto Configuration in Mobile Ad hoc Networks using Site local Addresses”. Internet Draft.
- [14] C. Perkins 2002 “IP Mobility Support for IPv4”, Network Working Group, (Draft Standard) 3344

- [15] J. Arkko, D. Johnson, C. Perkins 2002 “Mobility Support in IPv6”, IETF Internet Draft (Work in Progress)
- [16] C. Perkins, J.Malinen, A. Nilsson, A. Tuominen, R.Wakikawa. 2002 “Connectivity for IPv6 Mobile Ad Hoc Networks”. IETF Internet Draft (Work in Progress)
- [17] K. Egevang, P.Srisuresh “Traditional Network Translation (NAT)”, Network Working Group, RFC 3022
- [18] E. Belding-Royer, Y.Sun. 2001, “Connectivity for IPv4 Mobile Ad Hoc Networks”. IETF Internet Draft (Work in Progress)
- [19] Nitin N. Vaidya. 2002 “Weak Duplicate Address Detection in Mobile Ad hoc Networks” in Proceedings of Mobicom 2002
- [20] Sanet Nesargi, Ravi Prakash. 2002 “MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network” in Proceedings of Infocom 2002.
- [21] Perkins et al. (Nov 2001) Internet Draft “IP Address Auto-configuration for Ad Hoc Networks, Technical Report. Internet Engineering Task Force, MANET Working Group.
- [22] T.Narten, E. Nordmark and W. Simpson. 1998 “Neighbour Discovery Protocol for IPv6”. (Draft Standard) 2461. Internet Engineering Task Force.
- [23] Mansoor Mohsin, Ravi Prakash. (2002) “IP Address Assignment in a Mobile Ad Hoc Network” in Proceedings of Milicom 2002.
- [24] Subir Das, Anthony McAuley, Archan Misra. 2001 “Auto-configuration, registration, and Mobility Management for Pervasive Computing” in IEEE Personal Communications August 2001, pp. 24-31