

Ad Hoc Networks

Introduction

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required.

Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile ad-hoc network. Nodes rely on each other to established communication, thus each node acts as a router. Therefore, in a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes.

In a wireless world, dominated by Wi-Fi, architectures which mix mesh networking and ad-hoc connections are the beginning of a technology revolution based on their simplicity.

Ad hoc networks date back to the Seventies. They were developed by the Defense Forces, to comply with a military framework. The aim was to rapidly deploy a robust, mobile and reactive network, under any circumstances. These networks then proved useful in commercial and industrial fields, first aid operations and exploration missions. Ad hoc networks, also called peer-to-peer networks, still have a long way to go in order to be fully functional and commercial, as it has its defects such as security and routing which we will discuss further.

Routing Protocols

Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later.

Discussed below are three categories that existing ad-hoc network routing protocols fall into:

1. Table Driven Protocols
2. On Demand Protocols
3. Hybrid Protocols

Ad-hoc Mobile Routing Protocols



Diagram 1

1. Table Driven Routing Protocols, also known as Proactive Protocols, work out routes in the background independent of traffic demands. Each node uses routing information to store the location information of other nodes in the network and this information is then used to move data among different nodes in the network. This type of protocol is slow to converge and may be prone to routing loops. These protocols keep a constant overview of the network and this can be a disadvantage as they may react to change in the network topology even if no traffic is affected by the topology modification which could create unnecessary overhead. Even in a network

with little data traffic, Table Driven Protocols will use limited resources such as power and link bandwidth therefore they might not be considered an effective routing solution for Ad-hoc Networks. Fisheye State Routing is an example of a Table Driven Protocol.

2. On Demand Routing Protocols, also known as Reactive Protocols, establish routes between nodes only when they are required to route data packets. There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. When a route is required by a source node to a destination for which it does not have route information, it starts a route discovery process which goes from one node to the other until it arrives at the destination or a node in-between has a route to the destination. On Demand protocols are generally considered efficient when the route discovery is less frequent than the data transfer because the network traffic caused by the route discovery step is low compared to the total communication bandwidth. This makes On Demand Protocols more suited to large networks with light traffic and low mobility. An example of an On Demand Protocol is Dynamic Source Routing.[\[9\]](#)

3. Hybrid Routing Protocols combine Table Based Routing Protocols with On Demand Routing Protocols. They use distance-vectors for more precise metrics to establish the best paths to destination networks, and report routing information only when there is a change in the topology of the network. Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone. Zone Routing Protocol (ZRP) is an example of a Hybrid routing protocol.[\[10\]](#)

Security

Ad-hoc networks are highly vulnerable to security attacks and dealing with this is one of the main challenges of developers of these networks today. The main reasons for this difficulty are;

"Shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability." [\[1\]](#)

Generally, when considering the security of a network, we examine it under the headings; availability, confidentiality, authentication, integrity and non-repudiation. Availability refers to the fact that the network must remain operational at all times despite denial of service attacks. Confidentiality ensures that certain information is never disclosed to certain users. Authentication is the ability of a node to identify the node with which it is communicating. Integrity guarantees that a message is never corrupted when transferred. Non-repudiation states that the sender of the message cannot deny having sent it. An ad-hoc network has extra security requirements caused by its lack of proper infrastructure and the dynamic relationship between the nodes in the network. Because of the lack of infrastructure, accountability is very difficult to determine as there is

"no central authority which can be referenced when it comes to making trust decisions about other parties in the network." [\[2\]](#)

The dynamic relationship between the nodes leaves very little opportunity for the nodes to form trust relationships with each other. In an ad-hoc network, nodes must act as both terminals and routers for other nodes. Because there are no dedicated nodes, a secure routing protocol is needed. Multi hop routing protocols are usually employed. These can lead to problems due to non-cooperating nodes and denial of service attacks.

Denial of Service Attacks

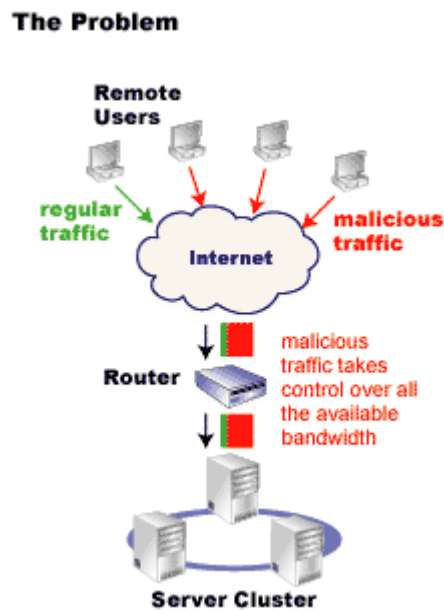


Diagram 2: reference [\[3\]](#)

These problems are not easily solved and routing protocols for ad-hoc networks are still under active research.

Confidentiality is also a major issue in ad-hoc networks but it is one that can be solved more easily. Cryptography is one of the most common and reliable means to ensure confidentiality.

"It is the study of the principles, techniques, and algorithms by which information is transformed into a disguised version which no unauthorized person can read, but which can be recovered in its original form by an intended recipient." [\[4\]](#)

Another issue to be considered is protecting the information that is actually stored on the device as the more portable the device, the easier it is to tamper with in general. We must also attempt to retain confidentiality of identity and location which will become more important in the ubiquitous computing environment. Ad-hoc networks require a high level of security, but because of the nature of these networks,

this can often be difficult to provide. Therefore, it is an issue which requires a lot more research if these networks are to continue to thrive.

The future of ad hoc networks

Mobile ad hoc networks are the future of wireless networks. Why? Because they're practical, versatile, simple, easy to use and inexpensive! We will be living in a world where our network instantly updates and reconfigures itself to keep us connected anywhere we go.

These networks provide a new approach for wireless communication and by operating in a license free frequency band prove to be relatively inexpensive.

With the current trend of society's demand for information at our fingertips, we will see our future living environments requiring communication networks between the many devices we use in day to day living, allowing them to talk to each other.

For example devices like personal digital assistants and mobile phones being able to receive instant messages from a home device. Such as a refrigerator sending a message to a PDA to update its shopping list; notifying that it's run out of milk. Or washing machines and ovens sending a report to say the clothes are finished or the chicken's cooked.

Like wise, in education ad hoc networks may be deployed for student laptops interacting with the lecturer during classes. [\[5\]](#)

Also wireless public access for dense urban areas (Nokia RoofTopT): A wireless broadband solution for residential markets, based on a multi-hop Ad-Hoc (mesh) networking. [\[5\]](#) *See diagram below*

Or similarly, ad hoc networks for cars, sending instant traffic reports and other information. Sensors and robots forming multimedia network that allows remote visualization and control, multiple airborne routers (from tiny robots to blimps) automatically providing connectivity and capacity where needed (e.g., at a football game); an ad hoc network of spacecrafts around and in transit between the Earth and Mars. [\[6\]](#)

Science fiction? Only time will tell.

Nokia RoofTopT Wireless Routing

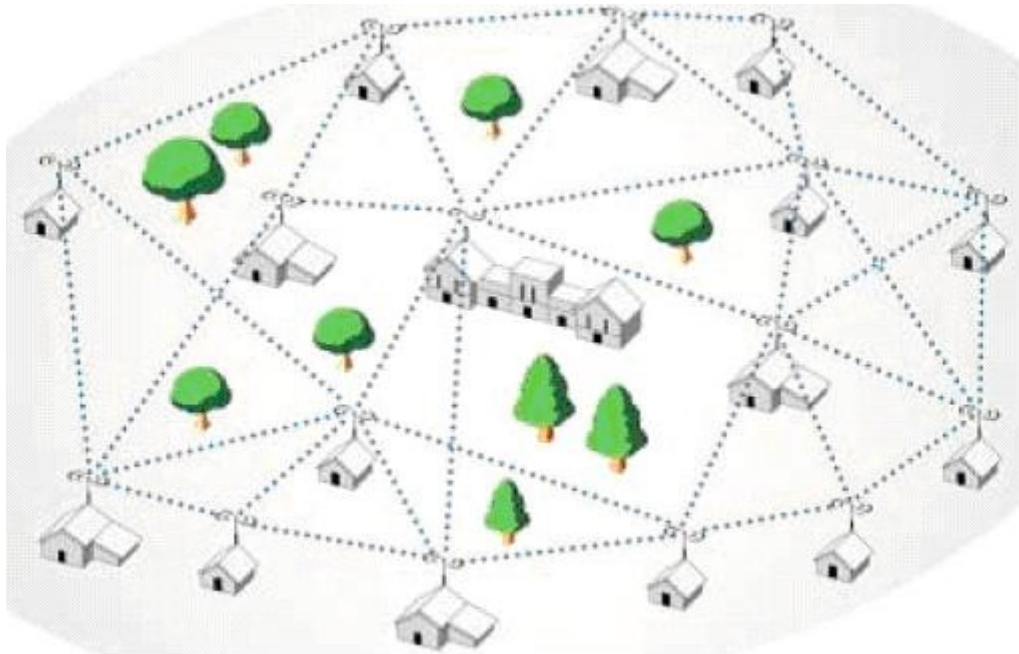


Diagram 3: reference [\[5\]](#)

WAND

Closer to home, in Trinity College Dublin itself, the WAND venture, Wireless Ad hoc Network for Dublin, is underway. WAND, is a project that is currently in progress to aid research in the area of ad-hoc networks. The project is run by the Distributed Systems Group of Trinity College, in collaboration with Media Lab Europe.

WAND is arranged as a large scale test bed for ad-hoc networks protocols and applications, covering a 2km route from Trinity to Media Lab Europe. *See diagram below*

This route will be routed with custom-built wireless-enabled embedded PCs. Along this stretch, the embedded PCs will be placed in apartments, shops, on traffic lights and in phone booths providing a minimum level of connectivity.

The PCs form a sparse population of wireless network nodes. This sparse coverage is

constantly available and the embedded PCs can be configured to create a variety of network models.

Other devices with wireless connectivity may also connect to the network via the implementation of mobile nodes. [7]

2km route from Trinity to MLE

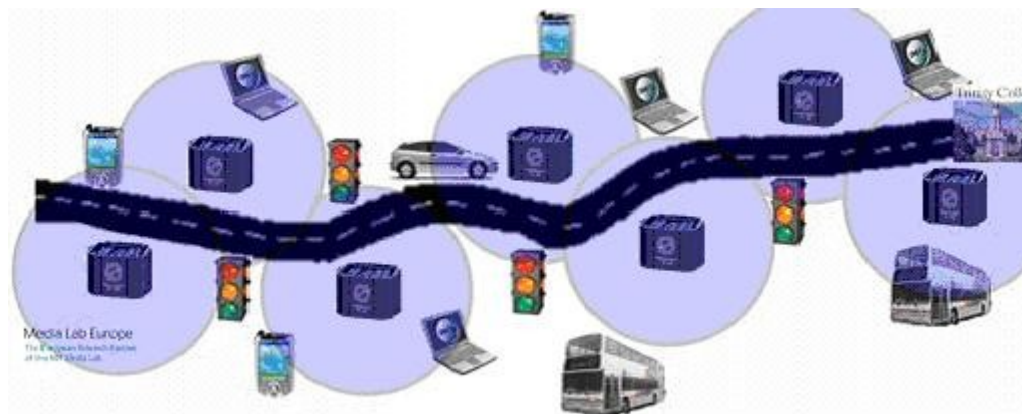


Diagram 4: reference [8]

Many factors lead us to believe that ad-hoc is the wireless network of the future. Due to the network not requiring any base station makes them indispensable in disaster relief situations or military war zones. Also energy issues have moved us from using a single long wireless link (as in cellular) to a mesh of short links (as in ad hoc networks). [6]

To sum up, ad-hoc networks will be the future of our wireless networks.

Conclusion

After researching Ad-hoc networks in depth, we believe that they will be the future of wireless networking. It is true that performance suffers as the number of devices grows and large ad-hoc networks become difficult to route and manage. However, much time is being devoted to achieving routing stability, and a few technical issues need to be solved before they become common place. The area of ad

hoc networks is a very fast growing area, and due to the vast research in them, we are seeing these problems disappear and they are coming into a world of their own.

References:

- [1] <http://www.phptr.com/articles/article.asp?p=361984>
- [2] http://www.pampas.eu.org/Position_Papers/Ericsson.pdf
- [3] <http://www.sysmaster.com/imgs/dos>
- [4] <http://www.phptr.com/articles/article.asp?p=361984&seqNum=11>
- [5] http://dessr2m.adm-eu.uvsq.fr/portes2003/Ad-Hoc_presentation.pdf
- [6] <http://ieeexplore.ieee.org/iel5/35/21724/01006968.pdf?arnumber=1006968>
- [7] http://www.dsg.cs.tcd.ie/dynamic/?category_id=-2WAND
- [8] <http://www.medialabeurope.org>
- [9] <http://www.cs.tcd.ie/courses/baict/bass/4ict>
- [10] <http://www.computingunplugged.com/issues/issue200407/00001326002.html>
- [11] <http://www.wikipedia.org>