Critical Review of all Research Topics

CP4022 Research Topics in Networks and Distributed Systems.
Assessment 3

By Stacey Greenaway

Contents

1. Introduction

Computer science research is the process of creating algorithms or developing existing algorithms or mathematical techniques to provide solutions to a specific problem. Of the seven research areas presented, including Bandwidth measurement in IP networks, Internet priority scheme performance, Middleware for ad-hoc networks, Denial of service attack prevention, Managing trust in peer-to-peer networks, Dependability in wireless sensor networks and Approaches to context awareness in mobile networks, some key themes can be highlighted that connect each research area. Mostly, each presentation concentrated on a different problem involved with decentralised networks rather than client server networks. Suggested solutions to issues concerning security, anonymity and performance of these networks have been proposed through algorithmic based strategies.

2. Decentralised Networks

Ad Hoc, Peer to Peer and wireless sensor networks share one major similarity and that is that they are decentralised. They are not controlled by one central authority and each node in the network acts as both client and server. Instead of bandwidth being provided by a central ISP, the resources of each node in the network are shared to power the network. For the most part nodes in the network preserve anonymity, meaning, details such as type of device, location, even IP address remain undisclosed. Context awareness research aims to determine the device connecting to the network, its location and its connectivity. Whilst this is a threat to anonymity, it is an important development for selecting the best node in a network.

Selection of the best node can further be determined through research into Bandwidth measurement, potentially if the bandwidth between each node of the network can be measured at the point of connection then a choice can be made of which node to connect to. Of course the problem with this research is how much bandwidth is consumed making the calculation and how this will effect the speed of connection. This would be of benefit in P2P file sharing networks for instance, where higher bandwidth would be required to quickly download high quality files. However, it is hard to measure bandwidth on P2P, Ad Hoc and Wireless sensor networks because the connection is not active long enough and potentially not repeated. Without bandwidth measurement of these networks it is hard to take proposed strategies out of simulated networks into real networks as they might be too greedy in bandwidth consumption. The connections are not alive long enough to test a systems effectiveness adequately.

With this in mind prioritising connections is important research to work out which activities get what share of the bandwidth. When linked to context awareness research, priority could be given to a certain device, or a device in a location that is near by, so data has less distance to travel making the network more efficient. Equally priority schemes linked with bandwidth measurement research can give priority to nodes in the network with greater bandwidth, these nodes could be identified as more important nodes.

3. Choice

Certain difficulties arise in selecting the best available node, measuring user preference and performance bottlenecks. Whilst it is beneficial to offer a user more choice, it creates new problems, how can user opinion be measured and what impact does it have on system performance? In client server networks users make choices over which ISP to use, they may base this on price and connection speed or reliability. Similar choices can be expected for decentralised networks with the addition of the type of device to connect to be it phone, pda or laptop and whether the node in the network is trustworthy. Similarly in peer to peer networks bandwidth and trust are important in interactions. Research into Bandwidth Measurement, Context Awareness, Priority Schemes and Trust and Reputation systems all factor in potentially providing more choice to a user in a mobile, ad hoc or p2p network.

Context awareness research aims to determine the device connecting to the network, its location, its connectivity. This information, if delivered to other nodes in the network will allow for choice. creating more choice for users of the network by potentially allowing a user to select a device to connect to and the speed at which to connect. Alternatively if devices (nodes) in the network received this contextual information they could select the best connection in a network automatically, selecting the best path to send information from one node to another, this is especially useful in wireless sensor networks where information is passed through several nodes as opposed to one on one interactions in peer to peer or ad hoc networks, where user preference has more prevalence. Through knowing the type of device and location of each node a user could be offered a choice of connection accounting for various preferences, a user may only wish to connect to other mobile phones in a network and only phones in a local vicinity, if for instance they are entering a chat room or swapping ring tones, this may speed up the performance of the network.

By using bandwidth measurement strategies on decentralised networks, the potential performance of a connection could be delivered back to the user, providing a choice for the user of which node to connect to. A problem of performance bottleneck arises by knowing the bandwidth performance capabilities of all nodes in the network, the highest performing node will always be selected until its bandwidth is shared over too many nodes so they are no longer getting good connectivity. A solution to Performance Bottleneck needs to be found in order to successfully allow a user to select which node in a network to connect to. Equally if nodes know all the available bandwidth of all the other nodes in the network, the best performing node could be automatically selected at the point of connection, again creating a performance bottleneck. Threshold limits and priority queues could help to prevent this.

Determining which activity gets priority on a decentralised network, be it ftp, http, or p2p file sharing is very much a user preference, each user is different and will have different priorities on different days. File sharing happens mostly in the background whilst other tasks are undertaken that more than likely require an internet connection. It cannot be assumed that although it is a background activity, a user would not give file sharing priority over surfing the web. Similarly, when trying to measure trust and reputation in p2p networks, measuring a human opinion of bandwidth allocation in order to prioritise activities across decentralised networks is equally hard to determine as no user will hold exactly the same opinion.

These measures will impact on anonymity which again is a user preference as to whether they would rather remain anonymous in a network. An anonymous user may not necessarily be malicious, but worried about malicious nodes having access to there location, device and IP address.

4. Security

The very nature of decentralised networks makes security essential but also hard to enforce. The anonymity of each connection means that there is no distinction between a malicious and a trustworthy node. Security issues involve not just preventing DoS attacks or viruses but protecting data transmitted through the networks.

Certain malicious activity can be prevented by protecting the information travelling across the network, encrypting it so it cannot be intercepted by malicious users. Public Keys and Hash Spaces offer a solution to protecting data within a decentralised network, there is however a concern on how much strain security systems place on the network resources and how they impact on anonymity, which is one of the appealing aspects of decentralised networks now that the internet is so corporate and well policed. Unfortunately malicious users see the anonymous nature of decentralised networks as their way to spread viruses and bring down the networks using Denial of Service attacks.

This decentralised connectivity is also a problem for preventing DoS attacks, as there is no central authority, there is no control over the connection or content being transferred over the network, so a malicious user can easily gain access to the network and subvert it. The key area of research in Trust and Reputation systems for P2P networks, dependability in wireless sensor networks and preventing DoS is being able to recognise a trustworthy node in the decentralised network and being able to identify and remove malicious users somehow.

Equally, QoS is hard to police in a decentralised network. Each node on the network is responsible for its own activities. There is no central server that can ban a user if they misbehave.

5. Conclusion

To allow for a user to know the type of device, location of device, its bandwidth and a trust rating will all take up significant resources upon connection, but will allow for increased security of decentralised networks. This could lead the way for standards to be introduced and make decentralised networks a more mainstream technology. With every positive about developments for decentralised networks there are negatives which will make widespread implementation of proposed systems difficult.