Mesh Networking & Net Neutrality

Coen Dekker
s1455966
coen.dekker7@gmail.com

Dirrik Emmen
s1425173
dirrik@gmail.com

Tom Rijntjes
s1405179
tomrijntjes@gmail.com

ABSTRACT

In this paper, the nature of a mesh network topology is investigated. The development is put in a historical context, leading up to present day events and non-military applications. Mesh networking is compared to other networking topologies in terms of strengths and weaknesses. A number of applications is described, including technology that is used to promote net neutrality. Next some basic steps are made to get you started with this technology. Finally, mesh networking is put in a broader perspective of web technology in the context of net neutrality.

1. PURPOSE, CONTEXT AND HISTORY

A mesh network is a network topology of which each node can pass on information. Typical properties of a mesh topology are the lack of centralized routing nodes and ease of deployment in areas without existing communications infrastructure.

Recently mesh networking reached notability in the context of the anti-control movements. Due to its ad hoc nature, mesh networking allows localized, off-the-grid networking without centralized governmental intrusion. For example, the Free Network Foundation [1] deployed their Freedom Towers to supply free, unsupervised network access to the Occupants of Zuccotti Park during the occupy protests.

In this paper, mesh networking is described in the context of conflict and communication. Firstly, the evolution of mesh networking is described. Secondly, the nature of the mesh topology in relation to other topologies is described, followed by the strengths and weaknesses. The practicalities of creating a mesh network will be explored, and lastly the implications of decentralization in the context of net neutrality will be discussed.

Early networking attempts

Early computing in the 1950's employed a mainframe model, using multiple terminals connected to a central processing unit(CPU). The communication consisted of data packets shipped back and forth from the terminal endpoint to the CPU over a longer distance. This technology was soon used for interconnecting remote computers. For military purposes, end to end networking in this manner would not trump existing systems due to the wired nature of the connection and the lack of robustness in case of an attack.

In 1960, J. Licklider famously proposed a global network of computers in his paper Man-Computer Symbiosis [2]. It would take another nine years before the first multi-node network would go live. The main problem concerned representing differing local states in a logically consistent manner across a network. The solution took shape in the form of packet switching, a technology that chunks data into arbitrary packages with routing decisions made on a per-packet basis. This differs from previous approaches based on call routing, which led to suboptimal use of bandwidth and were prone to single point of failure. This means that packet switching responds robustly to failing nodes, in contrast to earlier attempts. ARPAnet, a precursor of the modern internet was developed, this went live in 1969.

Around the same time, a Hawaiian professor Norman Abramson performed a series of experiments with network nodes sharing a radio channel, which became known as ALOHAnet. Based on Abramson's ideas, the first generation of ad hoc networks were developed.

From Packet radio to private MANETS

Based on the multiple access protocol of the the relatively small scale deployment of ALOHAnet, in 1973 DARPA (the technology branch of the department of defense) developed the Packet Radio Network, subsequently abbreviated to PRnet. The network was revolutionary in the sense that it allowed for mobile nodes with ease of deployment and redeployment, attributes that were particularly useful in military applications. However, a disadvantage of sharing the same channel for broadcasting and receiving did not allow nodes to send and receive at the same time. This led to all sorts of limitations with regard to broadcast scheduling: a node could not broadcast when it was receiving a packet, which led to complex networking protocols [3].

Ongoing development led to the DoD-funded Survivable Adaptive Radio Networks (SURAN) project in the early eighties. SURAN improved on PRnet with regard to size, power thriftiness, cost, scalability and resilience to electronic attacks [4]. Other than that, not much is known about the complexities of the technology due to military secrecy.

In the 1990's, two groundbreaking developments regarding mobile ad-hoc networks (MANETs) emerged that caused a shift in military use to private use. These technologies were increasing availability of laptop computers and the emergence of short range wireless connections such as WiFi and Bluetooth. This led to the conception of a range of applications, the most notable will be discussed in later sections.

2. OPERATING PRINCIPLES

"*An alternative physical reality to the magic of the Internet*"
- Isaac Wilder, FFN

When most people are asked to envision the internet, they conjure an image of some sort of magical cloud where web pages reside. However, reality is bound by rules of physics: the internet consists of many physical infrastructural waypoints controlled by governments and businesses. Users connect to an internet service provider (ISP) who will connect to other ISP's or servers in order to find the data we are looking for.

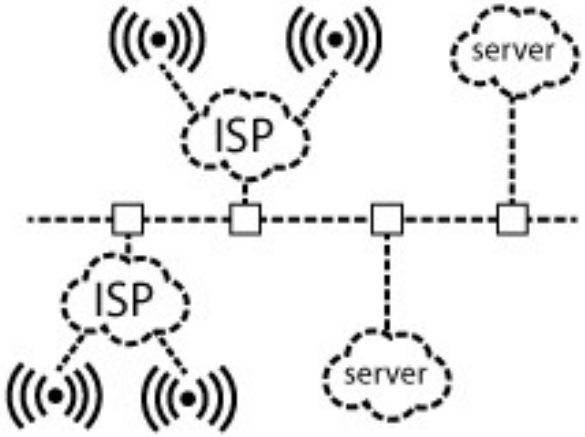

Figure I: The simplified internet

Within networks there are different kind of topologies possible. The internet at large scale can be seen as multiple tree networks connected to a digital highway of sorts. When your ISP is down, you can not connect any longer to other devices on the internet. Connection to your local networking environment is still possible, but internet connection relies on nearby hubs. This is typically the case within tree, ring and star topologies.

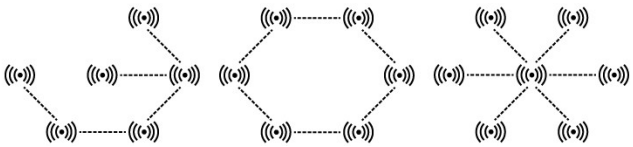

Figure II: From left to right: tree-, ring- and star topologies

In contrary, a mesh network consists out of devices which can function as a hub and endpoint simultaneously. Whenever a device or path between devices fails a mesh network will reconfigure itself, amounting to relatively high robustness in environments where central data distribution is impossible or unwanted.

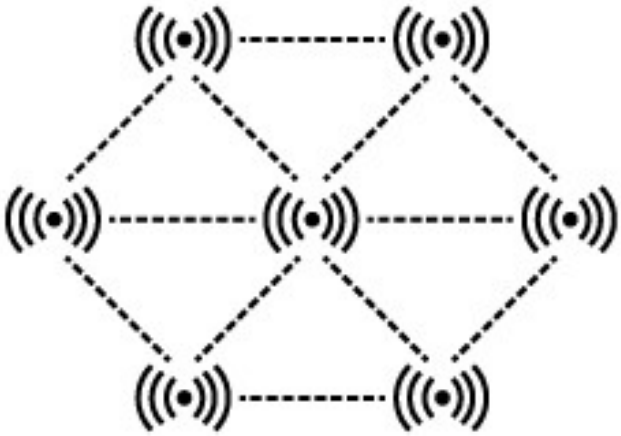

Figure III: Mesh topology

The mesh topology has implications for routing dynamics, which are intrinsically different due to the dual nature of each node as both hub and end-point. A basic approach is flooding, a technique that is agnostic of nodes' relative position. Each receiving node is instructed to broadcast the message to every node it is connected to. Eventually, the packet reaches every node, leading to a shared logical state. Every path is used, including the shortest one. This leads to packet duplications and much redundant traffic, but may suffice for some applications.

A more sophisticated approach relies on routing algorithms such as A*. This algorithm uses a combination of cost functions and geographical heuristics. A side-effect of using A* for routing packets in a mesh network is a linear relation between the amount of nodes and the potential bandwidth. If a route is congested, the cost of that particular route increases and another route becomes more favourable. Adding nodes simply increases the amount of potential routes leading to improved latency and bandwidth since data can travel along multiple routes.

3. STRENGTHS AND WEAKNESSES

Using a mesh topology has a number of potential strengths:
The first advantage of mesh networking is that it can be easily deployed in all kinds of environments, without the need of physical wiring. The setup of a mesh network is like setting up poles within range instead of physical wiring [5]. This decreases the costs and time to set up a network.

Secondly, the self-healing capabilities of a mesh network are really useful in more rough terrain. Each node can give specific values of performance. Nodes of the network could be damaged or even broken, a mesh network allows to trace back the problem, while keeping the network operational [6].

Due the way a mesh network handles its traffic the security and privacy for user to user connectivity is greatly enhanced compared to other forms of networking.

A final advantage of a mesh network is it's ability to adapt to drastic changes. The number of nodes in a network can be easily doubled or halved, without affecting the performance of the network itself. The network uses equal nodes all over, adding or removing nodes will just increase or decrease its size. The on the fly adaptability is only possible using a mesh network.

Although a mobile ad hoc network (MANET) [7] is similar to a mesh network. A notable difference is that a MANET is using one central controller. The controller will receive all the information from the nodes to determine and optimize the routing table. This network architecture makes use of mobile devices that each store the network data to route it's information. A MANET is not related to a fixed position and can easily change overtime. Another version of this network is a vehicular ad hoc network (VANET) [8], which uses vehicles as nodes to form a network, but will mostly work the same as a MANET. Both implementations are used for military uses because of it's flexibility.

Potential weaknesses.

While the feedback might be rich, the management of the network is complex compared to other topologies. Connecting and monitoring each node is quite arduous. Once the network is up and running, it requires constant supervision because of its design, with many redundancies and failures.

Another disadvantage is the fact that while there is a constant flow a data while running the network. This kind of traffic also slows down the actual speed that is possible of the network, even if it is just a little bit.

Why is the internet not meshed?

Popular use of technology usually develops through a combination of forces such as commercial incentives, governmental influence, technological development and coincidence. The complex interplay of these forces is hard to reconstruct, but we can dissect two powers crucial to our argument, which is the role of governmental meddling and commercial interest.

Mesh topology relies on peer to peer routing and communication, which can't be controlled centrally. If a node decides to give certain users paid privileges, it will simply be circumvented by the routing technology. This removes the economic incentive to develop the technology required for reliable networking. Krishnan et al. (2006) describe similar difficulties in peer-to-peer applications, most notably free riding [9].At the present time, demand for decentralized communication is shifting, which may fuel new developments. The current state of the technology can't compete with the Internet. Notable problems are high packet loss rates and low latency. Unless nearby peers start connecting through glass fiber, mesh networking can't beat a fiber optical bus architecture.

There is no reason to believe governmental bodies had a stake in the development of the web in its current architecture. However, the NSA did not fail to recognize the opportunity to leverage centralized communication hubs for their purposes. It can be safely assume that the US government has no interest in changing the current infrastructure.

4. TYPICAL APPLICATIONS

"*ISP's are not saints, and they are certainly responsible for missteps, mismanagement and other follies of failure & greed. Yes. Absolutely."* - jmnugent, reddit commenter

The first typical application for mesh networking would be military purposes [10]. Out in the open, in the wilds or near hard terrain, a group of soldiers in any uncommon landscape can easily set up a mesh network. Enabling them to communicate and share combat intelligence. The network is secure and self-sustaining. If one part of the network is occupied or destroyed the rest will be functioning just fine, informing what happened to the particular node.

One of the largest mesh networks and started in catalonia, it's called guifi.net [11]. Everybody on the network own the network. This network consists out of approximately 25 000 nodes, creating connectivity among people in a large area of spain. Another 11 000 nodes are planned within europe. Per example, this network is being used by students in order to connect to their universities if they can't pay for internet, creating internet connections on places where ISP's don't have coverage, or for video surveillance by companies.

Another great example is the mesh network deployed by Thailand's Royal Irrigation Department [12]. It reaches 372 km along a river and consists out of 64 nodes. This network delivers real-time river data to give flooding warnings to protect the people who lives next to it. The costs of this network was not feasible using wired or fibre technology. This network has a bandwidth of 240 Mbps and they use this bandwidth to monitor 27 HD camera's along the river.

A final example is FireChat, it is available since the first of

march 2014 for Android and iOS, enabling to chat "off-the-grid" without an internet connection [13]. There is no need for messages to go through servers from Google, Facebook or Apple when there are only a few nodes in between you and the recipient. And this where FireChat comes in, it creates a mesh network, enabling people to chat with each other, without using internet providers.

5. POTENTIAL APPLICATIONS

"*The world's urban poor and the illiterate are going to be increasingly disadvantaged and are in danger of being left behind. The web has added a new dimension to the gap between the first world and the developing world. We have to start talking about a human right to connect." - Tim Berners-Lee*

The internet could be seen as a super data highway, mesh networking can be seen as a technology that will bring us off road. It can enable users to share things with each other, or send messages, without an internet connection, even when they are far away from each other. Mesh networking extents the internet to places where there is none, simply by relaying packages, using a device we already have, a smartphone or by using solar powered nodes. Even in many poor areas people might be able to set up a mesh network. A mesh network then creates connectivity without using the internet in developing areas, rural environments, festivals, basements, subways, tunnels or disaster areas where the cell phone towers got knocked down. Mesh networking could eventually even provide free internet for all that uses it. A example for mesh networking in rural environments is the do it yourself guide by wireless Africa [14].

Google already started a project to provide free internet around the world using balloons. It is called Project Loon [15]. Project Loon is in essence a mesh network around the world, using high floating balloons to operate as nodes. The balloon will be floating 20km high, floating through the stratospheric winds around the earth. Here are layers of winds, moving in opposite directions, operating the balloon up and down will give it the ability to navigate. Imagine implementing a lot of balloons like this, a network could be constructed of moving nodes all around the world. On the ground Google plans to use special internet antenna's on the ground to connect with the balloons, thus providing internet.

Another experiment regarding mesh networking is the flexible bus system from the Akita University in Japan, this system can create a demand responsive transit system using ZigBee communication [16]. The busses can only communicate with bus stops and the bus stops are connected to a central control center. A passenger checks in at the busstop and sets its destination, this information is transmitted to the bus when passing a random bus stop. The navigation on the bus then changes the route dynamically based upon the demand. While passing the bus stop, the location of the bus is transmitted, and the expected time of arrival is changed accordingly. All this is done without the need of expensive cellular network communications, the data stays within the network and is sent to the bus by simply using the bus stops.

6. GETTING STARTED

Let's assume the nation is occupied in the nearby future by a currently unknown force. There is a need for communication between like-minded people, but all existing communication infrastructures are compromised. How to proceed?

Firstly, there need to be a physical network layer. This can be any medium that connects to people, including smoke signals, messenger pigeons and people shouting at each other over short distances. Assume that some secrecy is required and that means are limited, something readily available is used: tin cans connected with bits of string. This works well, but due to the fact that the wire has to be tense, the distance between sender and receiver is limited to, say, thirty meters. That's all fine and dandy if you want to talk to your neighbour without anyone listening in, but if you need to reach out to another city, a set of agreements is needed to allow this: a networking protocol.

There are two possible sets of agreements: either each node duplicates and broadcasts the message to every node it's connected to except for the node the messages originated from. For example, Michael needs to be informed, he lives across town, and he should come and have coffee.

The message will always reach the target node eventually, but you can imagine the amount of redundant copies travelling across the network.

A second option is that each node only talks to the nearby node that has the highest chance of reaching the goal node the quickest. Every tin can operator uses a combination of two strategies. The first is their approximation of the general direction of the goal node. Secondly, they incorporate their knowledge about the quality of the connection to each node. For example, a node that is exactly in the direction of the goal, but has a tendency of being absent at that time of the day might not be the best option. If you replace the notion of this tendency with a cost function, this is basically what the A* routing algorithm is. And it is done! The nodes can now talk to every other node without duplicating messages.

To recap, setting up a network with mesh topology is surprisingly simple: all one needs is a physical layer and a routing system to have the essence of a mesh network. It must be noted, however, that this is far from the same as being able to stream Netflix at every node. Mesh networking describes a logical topology, which is a low

level reconfiguration of the web. Toying with the technology in a do-it-yourself setting is challenging due to the scale of a full fledged network. The closest approximation that is not an application level implementation is the XBee module for Arduino, which will be described in more depth in the next section.

Hello World!

Xbee is a wireless data transmitter which runs the ZigBee protocol, the Xbee S2 employs mesh topology, which will be used. We'll describe setting up a basic network.

Requirements:

- Two computers
- Two XBee ZB ZigBee Wireless Modules (Series 2)
- Two XBee Explorer USB Boards
- Two A/B USB cables
- CoolTerm [17]
- X-CTU [18]
- FTDI Drivers [19]

The first thing to do is to connect the XBees to the Explorer Boards and to connect them to the computer. In order for the Explorer Boards to work, you will probably need the FTDI drivers. Now it is time to upload the right firmware to each XBee, using the X-CTU software. After opening X-CTU select the right com port on which the Explorer Board is attached to and press test. In the modem configuration tab we can now select XB24-ZB as a modem in the drop down menu. By using these steps write one XBee as a coordinator and the other XBee as a router. A router will do the mesh relaying to a certain receiver and the coordinator will be your computer interface. Please keep in mind which XBee you set as the coordinator and which one as the router.

On both XBees you will find a 64-bit serial number address. The first part of this address will be the same for both XBees, the high address, the last part will be different, the low address. Remember the low address of the XBees carefully.

Now start up CoolTerm, and hook up your coordinator XBee. Under options choose the serial port the XBee explorer is hooked on to. Be sure the baudrate is set to 9600, the Data Bits to 8, parity none, and stop bits to 1. To see what kind of commands you are going to send to the XBees you need to make sure "Local Echo" is activated in the Terminal options. Press OK to save the setting, press connect and we are up to configuring our first XBee.

Our first command will be "+++" to tell the terminal to go into command mode. Then type the following commands, one at a time, after each command you should get an "OK".

ATID 2001
ATDH 0013A200
ATDL your_low_address
ATWR

Click disconnect and remove your coordinator XBee from the Explorer, and hook up your router XBee. Click connect and go through the options again and send the same commands as before.

Now its time to see what we actually made. Hook up both XBees to their own explorer boards, and plug the explorer boards in a computer. Boot CoolTerm again and connect to the XBees, if everything went correctly you can now send messages between both XBees. The text you type on one computer will be relayed to the other. The range per XBee module is said to be 120m, so just check on your own how much space there can be in between. Now you have a very basic mesh network as illustrated in Figure 1.

Figure IV: A basic MESH network using XBee ZB ZigBee Wireless Modules (Series 2)

When using multiple XBees just set them all to the same ID and to the same low address using the following commands.

ATID 2001
ATDH 0013A200
ATDL FFFF
ATWR

When you type in the broadcasters terminal the message will be relayed to all other modules.

For a deeper understanding of the type of mesh networks you could build with XBees, an overview can be found on Controlanything [20].

7. FINAL THOUGHTS

We live in an era of enhanced awareness of our digital footprint. Landmark events that led to this position were huge successes of data driven enterprises and the revelations by Edward Snowden. These events led to a widely spread understanding of the limitations of the web in terms of privacy, subsequently adding to a demand for alternatives for the internet in its current state. A notable example of a privacy-focused application is Onion Routing, a technology that exploits encryption and random routing paths to cloak packet content and origins.

Onion Routing enabled the genesis of Silk Road, a

notorious online marketplace for trafficking illegal wares and prostitution. Not that we framed the discussion in terms of net neutrality, but it is important to consider the implications of complete freedom of communications. Not every user has benign intentions. Net neutrality proponents point out that criminal activity is not a property of freedom of communications, but a problem in itself. This is a complex discussion and we will leave it at that.

A demand for alternatives led to roughly two groups of net neutrality activists. The first promotes tools to return privacy to the current web infrastructure. The second group has signed up trust in the centralized infrastructure of the internet and suggests alternative infrastructures. The Free Network foundation, the DarkNet project and similar initiatives are part of the latter category.

It's interesting to see that web technology has a central role in a societal problem. In just four decades, the web has evolved from a specialists' tool to a driver of societal change. Take for example the role of Twitter in the events leading up to the Arabian spring.

The development of privacy-centred applications demonstrate that people feel the urgency to protect their freedom of communication. Democracy might be at stake.

REFERENCES

1. Free the Network: Hackers Take Back the Web. (n.d.). *YouTube*. Retrieved May 21, 2014, from https://www.youtube.com/watch?v=Fx93WJPCCGs
2. Licklider, Joseph Carl Robnett. "Man-computer symbiosis." *Human Factors in Electronics, IRE Transactions on* 1 (1960): 4-11.
3. Jubin, J., & Tornow, J. D. (1987). The DARPA packet radio network protocols.*Proceedings of the IEEE*, *75*(1), 21-32.
4. Ramanathan, R., & Redi, J. (2002). A brief overview of ad hoc networks: challenges and directions. *IEEE communications Magazine*, *40*(5), 20-22.
5. Akyildiz, I. F., & Wang, X. (2005). A survey on wireless mesh networks.*Communications Magazine, IEEE*, *43*(9), S23-S30.
6. Mandayam, N. B., Wicker, S. B., Walrand, J., Basar, T., Huang, J., & Palomar, D. P. (2008). Game Theory in Communication Systems [Guest Editorial].*Selected Areas in Communications, IEEE Journal on*, *26*(7), 1042-1046.
7. Shabbir, A., & Kumar, A. S. An Efficient Authentication Protocol for Security in Mobile Ad Hoc Networks.
8. Wang, Y., & Li, F. (2009). Vehicular ad hoc networks. In *Guide to wireless ad hoc networks* (pp. 503-525). Springer London.
9. Krishnan, R., Smith, M. D., & Telang, R. (2006). The economics of peer-to-peer networks. Association for Information Systems.
10. Wireless Mesh Networks for military, defense and public safety applications. (n.d.). *Mesh Dynamics*. Retrieved May 22, 2014, from http://www.meshdynamics.com/military-mesh-networks.html
11. Open, Libre and Neutral Telecommunications Network. (n.d.). *guifi.net - Open, Libre and Neutral Telecommunications Network*. Retrieved May 23, 2014, from http://guifi.net/en/node/38392
12. Firetide Delivers the World's Longest Mesh Network. (n.d.). *Firetide*. Retrieved May 23, 2014, from http://www.firetide.com/121023-firetide-delivers-the-worlds-longest-mesh-network/
13. Firechat. (n.d.). *Open Garden | /firechat*. Retrieved May 23, 2014, from http://opengarden.com/firechat
14. Johnson, D., Matthee, K., Sokoya, D., Mboweni, L., Makan, A., & Kotze, H. (2007). Building a Rural Wireless Mesh Network. *Meraka Institute. African Advanced Institute for Information & Communications Technology*.
15. Project Loon. (n.d.). *Loon for All*. Retrieved May 23, 2014, from http://www.google.com/loon/
16. Iqbal, R., Yukimatsu, K., & Ichikawa, T. (2011, February). The Flexible Bus Systems Using Zigbee as a Communication Medium. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on* (pp. 1-5). IEEE.
17. Roger Meier's. (n.d.). *Roger Meier's Freeware*. Retrieved May 24, 2014, from http://freeware.the-meiers.org
18. XCTU. (n.d.). . Retrieved May 24, 2014, from http://www.digi.com/products/wireless-wired-embedded-solutions/zigbee-rf-modules/xctu
19. FTDI Drivers. (n.d.). *FTDI Drivers*. Retrieved May 24, 2014, from http://www.ftdichip.com/FTDrivers.htm
20. National Control Devices(n.d.). ZB ZigBee Mesh Networking - Introduction to Building Your Own Mesh Network. Retrieved May 24, 2014, from http://www.controlanything.com/Relay/Device/A3001