Ryan Sims
11-2-15

An Overview of Wireless Mesh Networks

Wireless networks are ubiquitous in modern society. Nearly everywhere you go in major cities, you are within range of some wireless network. People have come to expect fast, reliable access to the internet. Many communication systems rely on wireless connections, so when network access drops out, it can cause many problems. This is why people are starting to use wireless mesh networks (WMNs), in order to build robust wireless networks. WMNs are very reliable, scalable, and are deployed easily. These networks are self-healing, easy to configure, and offer redundancy between wireless connections, which makes the network much more reliable. They enable networks to extend their range much further than previously possible. Slowly, WMNs are becoming popular all over the world for their many benefits over traditional network infrastructures.

What is a Wireless Mesh Network?

A wireless mesh network is a type of communication network made up of individual nodes organized into a highly interconnected mesh topology. In a mesh network, the nodes relay data to other nodes, distributing the data across the network. The nodes in a Wireless Mesh Network (WMN) are typically laptops, phones, routers, or other devices that communicate wirelessly. These nodes can serve several roles; they can function as mesh clients, mesh routers, gateways, or any combination of the three. In a WMN, the same device can act as a client, a router, and a gateway to another network (i.e. the Internet). Since the network is wireless, the range in which devices are able to connect is very important to how the infrastructure of the network is configured. Depending on the network's configuration, devices can be mobile, and can physically move around and maintain network connectivity.

Mesh networks have many advantages over other types of network topologies. They are self-discovering, meaning that when new nodes are added to the network, the network can start using that node for routing. When nodes are removed from the network, the network can heal itself, and redistribute the data accordingly. Nodes can connect to multiple nodes at a time, so when one node drops out, there is redundancy to ensure the network stays connected.

A device in a Wireless Mesh Network can have many roles. The first and most obvious role is that a node can be a mesh client. A client node is able to send and receive data from other devices that it is connected to. Clients communicate with other clients and distribute network coverage, and can communicate to mesh routers. Mesh routers are devices which connect to a WMN and are able to send and receive data on the network, either serving data to clients, or connecting other routers to one another. The differentiation between client and router is fairly vague in a WMN, since both devices have similar functionality. The differentiation is mostly made to indicate which device is able to connect to a gateway, and to indicate differences in hardware in the system; however, this depends entirely on the protocol you are using for your network. Lastly, nodes can be gateways. Gateways are the nodes in a WMN which are able to communicate to other networks, most commonly the internet. Gateways can allow clients to connect to the internet, and act as a device which controls network traffic. Computational overhead may be distributed across the network, and gateways typically are the point where internet traffic and intranet traffic is processed and distributed.

Most wireless mesh networks are Multihop wireless networks. A multihop network is any network that sends data between at least two nodes before reaching its destination. Mesh networks can relay data between a large number of nodes before reaching the terminal node. The path that the data takes is decided by the routing protocol that the network uses. Depending on the routing protocol, the data can be distributed between multiple routes, or can be sent down just the most efficient route calculated. Since all the nodes in the network are indirectly connected to one another, one node can flood out data across the network to every

node connected. This can be used to change state across the system, or as a means of determining where the terminal nodes are.

Why Wireless Mesh Networks?

Wireless Mesh Networks offer many advantages over other types of network topology. The biggest advantage that WMNs offer is the increased reliability compared to traditional network models. It is easy to improve the quality of the network too; the range, speed, and reliability of the network increases by adding more nodes. The equipment costs are very low when building the network. WMN are self-configuring, self-healing, and self-discovering, which makes configuring and expanding the network easy.

One of the most common uses of wireless mesh networks is for extending low bandwidth networks over a wide range. Many commercial operations rely on WMNs to connect a single hard wired internet gateway to a network of wireless routers, extending the wireless network range much further than otherwise possible; this is common in malls, airports, and sometimes schools. By creating a mesh using a large number of wireless routers, you can extend the network as far as needed. Building such a robust wired network is very expensive; this is one of the reasons why WMNs are so appealing. With the cost of installing wires completely eliminated, the savings are already huge. Ad hoc WMNs, networks which use pre-existing hardware, are essentially free to deploy. The hardware just needs slight modification before it can be used in a WMN. Another advantage of WMNs is how servers can be ran on each node. FTP, chat, and other applications may utilize these servers, which can be especially useful when used in developing countries.

Despite all the advantages, WMNs are not perfect. The biggest disadvantage is the low bandwidth connections. This makes it impractical for many personal and business networks. Not only are the connections low bandwidth, they are also high latency. Since they are multi hop networks, the amount of time spent deciding each route adds to the total latency; the further you

are from the gateway node, the higher your latency becomes. VOIP, online gaming, and video-streaming become very difficult, if not impossible. Another disadvantage is that it does require some special knowledge to initially setup. All networking requires some technical knowledge, but unless you invest in a plug and play WMN, the initial setup can be difficult. WMNs are an incredible solution for any low bandwidth, low cost, and long range network.

Properties of Wireless Mesh Networks

In the last decade, WMNs have become much more popular. This is mainly due to the decreasing cost in wireless equipment. WMNs can utilize cheap 40 dollar routers, and turn them into powerful tools. The recent open-source hardware movement has helped fuel to development of these networks. Cheap open source hardware, like an Arduino or Raspberry Pi, can be connected to modular wireless units, which can be used to allow all devices to communicate with one another. One wireless unit, the NRF24L01, is a 2 dollar radio transceiver. This device is popular for connecting small devices to one another using WiFi. The Internet of Things (IOT) is a concept which has been gaining a lot of attention lately. In the IOT, small devices can all communicate with one another wirelessly. These devices can then interact with one another, and can change their state according to the states of other devices. While seemingly impractical now, IOT is only going to become more popular in the next decade.

In regards to the OSI model (Open Systems Interconnection model), WMNs use layer 2 (the data link layer), sometimes use layer 3 (network layer), and technically use layer 1(physical layer). The majority of the logic used by wireless mesh networks is in layer 3, the network layer. The network layer is responsible for packet forwarding and routing. Depending on which routing protocol is used, this logic will be different. The data link layer, layer 2, is responsible for sending the data between the different nodes on the network. This is usually handled by 802.11s, which is the most common WMN protocol in layer 2; others exist, but 802.11s became the standard in 2006, so most WMN protocols are built on top of this. 802.11s provides the logic

for layer 2, but the higher logic of layer 3 is handled by the routing protocol. Technically layer 1 is used, but it is very complex compared to the other layers. Layer 1 is responsible for physically sending data in between the different nodes, however this setup no different than your average wireless network setup.

Turning a wireless router into a mesh network router is incredibly easy. First, you must modify the software on the router to support wireless mesh networking. Depending on which protocols you plan on using, the setup will be different. Once this is completed, you can then power on your device, and it will connect to other nodes in the network.

The concept of Ad hoc wireless networks helps contribute to making mesh networks so powerful. A wireless ad hoc network is a decentralized network that does not use pre-existing infrastructure. A good example is the use of smart phone ad hoc networks; these networks use smart phones to transmit data, and can establish routes to connect clients to the internet. Smart phones are able to send data back and forth to each other using their own hardware. When paired into a mesh network, bandwidth can easily be distributed across the network. Clients can be mobile, and the network can heal when any clients drop in or out. Building a network without using an existing infrastructure is incredibly useful.

Different Ways to Communicate

There are many different protocols and physical mediums which WMNs can use to communicate. The first and most obvious one is WiFi. The 802.11s protocol dictates behavior for wireless mesh networks, albeit fairly simple, it is the common standard used in most commercial networks. WMNs are not limited to just WiFi however, and can utilize other forms of radio communication, and virtually any kind of wireless technology. Bluetooth is a common standard for short range mesh networks, like wireless sensor technologies or in-home automation. Different frequencies may be used as well, as a means of communicating with more devices. The most commonly used bands are 2.4GHz radio (WiFi, Bluetooth), 5GHz, and

900MHz. The adaptability to different bandwidths is useful when dealing with wireless sensor networks, and networks which use many different types of hardware.

Self-Healing, Self-Configuring, and Self-Discovering

Network resilience is one of the most important aspects of WMNs. WMNs are self-healing, meaning that when a node drops out, the network will adapt and still be able to send data to the rest of the network. How this is specifically done depends on the protocol used. Before any packets are sent through the network, the protocol tries to make a connection between the requesting node and the terminal node. For this to happen, the network must be aware of all the nodes currently connected. If a node drops out, this is the point where the network can check and adjust routing accordingly. WMNs are self-discovering, meaning that new nodes are discovered automatically. The network checks for the presence of new nodes by sending out requests to each node, which then send out messages trying to connect to all other local nodes. When this action is performed, any new nodes are automatically connected to the network. When a node drops out, it can reconnect easily and gracefully.

Many WMNs are self-configuring, meaning that the node can be added into the network without any special adjustments by administrators. Properties of that node's connection, like signal strength and reliability, can be incorporated into how the routing protocol optimizes the network. If the hardware is set up with the right software, then connecting an additional node can be as simple as just powering the device on. This is especially useful for smart phone WMNs, where the users typically don't have knowledge of setting up networks.

Bottlenecks and Points of Failure

Wireless mesh networks inherently have weak points. These weak spots can take the form of either bottlenecks or points of failure. Bottlenecks are nodes in the network that cannot keep up with the number of requests the network is giving them. Say there are several nodes

upstream from a bottleneck, and they all request data simultaneously. If all the data has to go through this one route, then the individual node may not be able to process all the requests fast enough. The node will process what data has been requested first, and make the other requests wait. This is a bottleneck, which is very common in wireless mesh networks. The physical location of routers in the network is what dictates where the bottlenecks will be. If a node is added which can help distribute the data, and alleviate the number of requests the node is expected to handle, then the network ideally will speed up to those nodes downstream of the bottleneck.

Reliability is one of the biggest advantages that wireless mesh networks offer, and with a poorly configured network, some of your nodes may not be very reliable. Sometimes one node may be the only thing connecting two large clusters of nodes. This is called a point of failure. If this one node were to drop out, then suddenly there is a portion of the network which cannot communicate to the rest of the network. By adding in an extra node in an optimal location, you can help distribute load, and add redundancy to make the network more reliable.

Routing Protocols

Wireless mesh networks must be able to coordinate how to send one packet from a requesting node to a terminal node. How the path is determined depends on which routing protocol is used. Different routing protocols optimize different things, like network latency, load-balancing, and reliability.

There are many different kinds of routing protocols, but there are two main types, reactive protocols and proactive protocols. Reactive protocols generate routes when a node needs to send data. These are good for networks that don't send much data, networks that consist of mobile routers, or networks where nodes aren't very reliable. Many reactive protocols use routing tables at each node to determine which node to send the data to next. Routing tables are tables that indicate which nodes are connected to one another. For reactive

networks, tables are generated when the node attempts to send data. Proactive protocols generate routes periodically, even when no requests are being made. This is useful when you need low latency connections, and when low packet loss isn't critical. Proactive protocols are by nature a little less reliable, and they require extra bandwidth and CPU utilization to calculate optimal routes.

One class of proactive protocols are the link-state based protocols. These rely on the nodes knowing the state of the network topology prior to sending data. One class of reactive protocols are the distance vector protocols. Distance vector protocols work by just informing neighboring nodes of changes in topology. This makes the packet calculate its route at every node, but is computationally less complex than with link-state protocol.

AODV - Routing Protocol

Ad hoc On-demand Distance Vector Routing, or AODV, is a routing protocol commonly used by wireless mesh networks. It is specifically designed for mobile ad hoc networks. Each mobile node in an AODV network is a specialized router. It is a reactive protocol, meaning that every time a route is needed, a new route is calculated. This means that network latency is higher, but it gives an advantage towards easy network discovery and routing using mobile ad hoc networks. Since there is no reliance on periodic advertisements, the network uses less overhead bandwidth.

Network discovery for AODV is fairly simple. When sending data to other nodes, a node first sends out a routing request to determine if there is an available route. If a route can established, then the original node sends the message it intended to send. To make a request, a node checks the routing table to see if a connection to the terminal node is available. If no immediate routes are available, the requesting node broadcasts out a route request to all connected nodes. These nodes then check for a route, and if none are available, the process is repeated until a route to the terminal node is discovered. The broadcasted message contains

variables which help the nodes determine the route to take. The source address and destination address are used to determine the devices which will be used to communicate. The source sequence number is used to determine ‘freshness’ in regards to finding a new route back to the source once the destination is found. A broadcast ID is given to distinguish between other broadcasts on the network, and a hop count variables keeps track of the number of hops. Once a route has been established, a lifetime variable is added. This is to ensure that if the message doesn't reach its destination, it is deleted. Since AODV uses routing tables at each hop, the packet itself stays small, since it doesn't have to record each source route; this is helpful on larger networks that require many hops. Once the terminal node is hit, it sends back a route response. Since each node received and stored information regarding that broadcast, when the response reaches a new node, it knows the ID of the previous node in the route, and sends the response accordingly. As this happens, each node sets up a forward pointer to create a route between the requesting node and the terminal node; also, the node updates its routing table with the nodes it is connected to. After all of this, the route is then established, and the data packet is then transferred.

OLSR - Routing Protocol

Optimized Link State Routing Protocol (OLSR) is another routing protocol used for mobile ad hoc networks. OLSR is a proactive link-state protocol, meaning that it checks the networks topography periodically. There are several unique features to OLSR which give it an advantage over your average link-state protocol when used with mobile ad hoc networks.

Since OLSR is a link-state protocol, it floods the network periodically with topology information. This information is fairly reliable, but it does not account for cases when nodes lose connection in between checks. The nodes may not be synchronized, which can cause errors. When OLSR floods the network with data, it picks a central node to distribute data from, and floods it from that node. This is unique to OLSR, and reduces some of the redundancies from

typical flooding. However, this lack of redundancies makes it more likely for a node to be unsynchronized.

OLSR has low latency compared to many other protocols. As the network grows in size, the routing overhead does not increase, due to the nature of link-state routing protocols. Since OLSR periodically updates the network with information, it is not ideal for sensor networks which stay quiet most of the time, or when your device is running on battery power. OLSR is very useful for certain applications, but several factors must be considered before going with OLSR. It is very CPU intensive, and uses a lot of bandwidth; for cell powered networks and battery-powered sensor networks it is not ideal. For mobile ad hoc networks, OLSR isn't as reliable as many other protocols. It is best used for ad hoc networks which need low latency, and where power and CPU usage are not a concern.

BATMAN - Routing Protocol

The Better Approach to Mobile Ad hoc Networking (BATMAN) is a mobile ad hoc network protocol which aims to replace OLSR. BATMAN is very different from other WMN protocols. The topology information is distributed across nearby nodes; this way, no single node could ever determine the path on its own. This decentralization of network knowledge helps in making the network more balanced, efficient, reliable, and secure.

BATMAN employs some unique methods for determining the optimal routes. Periodically, each node broadcasts an originator message that informs all neighboring nodes of its existence. This information is then relayed to other nodes, flooding the network until every node in the network is informed. The optimal route is determined by counting the speed and reliability of the route. First, it counts the number of originator messages that each node received; this is done so the node can determine the quality of the route. This information is added to a routing table controlled by BATMAN, which is used to determine route reliability. The originator messages contain a broadcast identifier, so that the node knows it is counting the

same message only once. The node which sent the originator message to any specific node first is seen as the fastest connection between those nodes.

Each node only stores information regarding the immediately connected nodes, and requires packets to determine their route at each node. This adds a level of security, and distributes the computational overhead across the network. This also makes it so each packet can be routed dynamically; the packet can be en-route to the destination, and if the network topology changes during transmission, the routing will change accordingly.

BATMAN is much less scalable than OLSR. Since there is a need to count and record all the originator messages for each node, as the network scales up it becomes slightly less efficient. On smaller mobile ad hoc networks, it has many advantages. Since the route is calculated at each node, the workload is distributed across each node. It is good for smart phone WMNs, where battery usage has to be kept to a minimum. BATMAN automatically handles gateway detection; if a device can also connect to the internet, the protocol automatically designates it as a gateway connection. It also determines the bandwidth and connection speed of the internet connection the gateway has, since these factors can help distribute the network more efficiently.

Mesh Network Uses

During the Hong Kong protests of 2014, many of the cell networks were becoming so overused, that people weren't able to connect to the internet at all. The cell towers were acting as bottlenecks, and there was no way to respond to all the requests being made. An app, called Firechat, started to gain popularity for its ability to turn regular smart phones into wireless mesh clients. Upon downloading the app, if you have a source of internet connection, your device would be treated as a mesh gateway and a mesh client. If other people in the mesh network are connected to you, but not to the internet, they can utilize your internet connection. This allowed users who could connect to specific WiFi access points to distribute the connection to those

without internet access. This helped alleviate the strain on the cellular networks, and gave protesters the ability to connect to the internet.

Since WMNs are so cheap, they are becoming increasingly common for networks in developing countries. Using cheap routers, people have been building networks in rural villages. These networks can be coupled with long range directional WiFi antenna, and can connect different villages together. Spreading the internet to these communities gives them the chance to learn, and communicate with one another. WMNs allow for community ownership of the network. One Laptop per Child (OLPC) is a program which distributes laptops to children in developing countries all around the world. OLPC successfully experimented with wireless mesh networks as a means of distributing internet and VOIP services to its users.

During certain emergency situations, communication networks may go down. If there is a severe natural disaster, like a hurricane, establishing communication networks is critical. WMNs can be deployed using routers via hot air balloons or drones. These networks can be deployed in less than a few hours after the disaster. This is a very cheap and novel solution to reestablish communications.

Agriculture is another emerging market for WMNs. Farms are slowly being fitted with large sensor networks, able to read information about the land that farmers otherwise wouldn't be able to quantify. Nutrient content, soil moisture levels, and sap flow are very useful metrics to farmers. In order to get the data quickly and reliably, a mesh network which can communicate to all the sensors in the field must be deployed. Connecting to each sensor in the network with wires is nearly impossible; tractors can catch loose wires, and some wires could have to be several miles long, which is very impractical. With WMNs, the sensors can wirelessly send data between nodes, and ultimately get the information to a gateway node which can upload everything online.

Conclusion

Today, wireless networks are all around us. The majority of people carry devices on them on a daily basis which can connect to various wireless networks. By utilizing WMNs, we can introduce much more reliable, scalable, and autonomous networks than ever before. If we take advantage of the tools and hardware we have, we can build much more robust wireless networks than we have implemented today. People have come to expect fast, reliable connections for their wireless devices; WMNs provide advantages which help make networks more efficient. WMNs are increasing in popularity all around the globe, and will only continue to do so as hardware prices decrease.

Works Cited

Ardagna, Claudio A., Sushil Jajodia, Pierangela Samarati, and Angelos Stavrou. "Providing Mobile Users' Anonymity in Hybrid Networks." *Computer Security – ESORICS 2010 Lecture Notes in Computer Science*: 540-57. Print.

Braunstein, Brian et al. "Feasibility of Using Distributed Wireless Mesh Networks for Medical Emergency Response." *AMIA Annual Symposium Proceedings* 2006 (2006): 86–90. Web. <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1839719/>

Coulson, Geoff, et al. "Flexible Experimentation in Wireless Sensor Networks." *Commun. ACM* 55, 1 (January 2012), 82-90. Print.

Hu, Elise. "How Hong Kong Protesters Are Connecting, Without Cell Or Wi-Fi Networks." *NPR*. NPR, 29 September 2014. Web. 10 October, 2015. <http://www.npr.org/sections/alltechconsidered/2014/09/29/352476454/how-hong-kong-protesters-are-connecting-without-cell-or-wi-fi-networks>

Martignon, Fabio, Stefano Paris, Ilario Filippini, and Antonio Capone. "Efficient Bandwidth Allocation in Wireless Community Networks." *2011 IFIP Wireless Days* (2011). Print.

Perkins, C., E. Belding-Royer, and S. Das. "Ad Hoc On-Demand Distance Vector (AODV) Routing." Web. <https://www.cs.cornell.edu/people/egs/615/aodv.pdf>

Sanchez-Iborra, Ramon, and Maria-Dolores Cano. "Qoe-based Performance Evaluation of Video Transmission Using the BATMAN Routing Protocol." *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks - Q2SWinet '14* (2014). Print.

Thompson, Michael S., Allen B. Mackenzie, and Luiz A. Dasilva. "A Method of Proactive MANET Routing Protocol Evaluation Applied to the OLSR Protocol." *Proceedings of the 6th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization - WiNTECH '11* (2011). Print.

Vijayalayan, Kanthaiah Sivapragasam, Aaron Harwood, and Shanika Karunasekera. "Distributed Scheduling Schemes for Wireless Mesh Networks." *CSUR ACM Comput. Surv. ACM Computing Surveys* (2013): 1-34. Print.