

WIRELESS MESH TECHNOLOGY

Connecting the new millennium

What you need to know before you decide if
Mesh is right for you



IJIS Institute

EMERGING TECHNOLOGY WHITE PAPER

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following individuals and their sponsoring companies for their dedication and input on this document:

Matthew A. D'Alessandro, *Motorola* –
Committee Chair



John Crouse, *ACS Government Solutions* –
Committee Co-Chair



Jim Martin, *Datamaxx*



Fred A. Lengerich, *SAIC*



This project was supported by Grant No. 2003-LD-BX-0007 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

WIRELESS MESH TECHNOLOGY

Following the tragic events of September 11, 2001, Congress created the Department of Homeland Security (DHS). The DHS identified two of its highest priorities: 1) Information Sharing, and 2) Interoperability. It is readily recognized that in order to effectively and efficiently share information among local, state, and federal authorities, a secure and reliable method of communications must be implemented.

“The DHS identified two of its highest priorities: Information Sharing and Interoperability.”

To address this need, DHS has taken two approaches. One is to build a network from DHS to strategic information collection and distribution points across the nation, through the Joint Regional Information Exchange System (JRIES) and the Homeland Security Network (HSN).

The other deals specifically with guidelines and/or recommendations relative to the interoperability of communications systems that might support local, tribal, state, and other appropriate entities' needs to become vital information exchange points as it relates to Homeland Security. These guidelines and/or recommendations are set forth in the SAFECOM program of DHS.

This paper addresses an emerging network technology, mesh networking, which may prove to be invaluable in solving many of the obstacles associated with traditional wireless communications networks.

Furthermore, this technology may facilitate a large degree of the interoperability that DHS envisions in the SAFECOM program. Mesh technology may also prove to be cost effective in improving wireless communications within the law enforcement, public safety, first responder, command and control, and integrated justice communities.

What is Mesh Technology?

Mesh network technology is a communications network model that is analogous to the way the wired internet works, since there are at least two possible pathways between each node. Mesh is a network architecture that improves on point-to-point and point-to-multi-point (i.e. centralized hub and spoke) topologies by providing each node multiple possible connection path ways to every other node. Figure 1: Point-to-Point, Figure 2: Point-to-Multi-Point and Figure 3: Mesh Network (Multipoint-to-Multipoint) highlights the differences in topology.

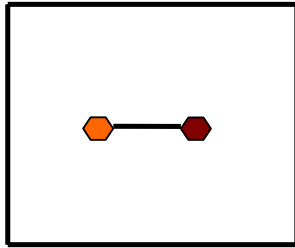


Figure 1: Point-to-Point

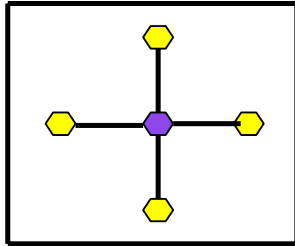


Figure 2: Point-to-Multi-point

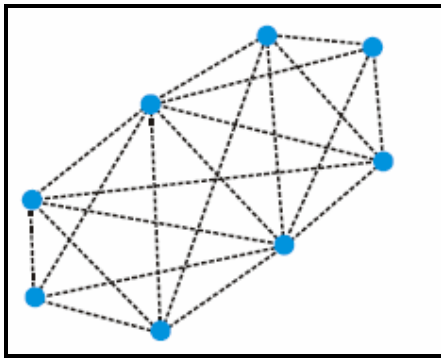


Figure 3: Mesh Network

Why Meshing Makes Wireless Communications More Robust and Cost Effective.

Wireless communication is a vital component of law enforcement and public safety in its fight against crime. Wireless voice and data systems to date have mostly used cellular phone style radio links, that is, use point-to-point or point-to-multipoint transmissions. Backhaul (the connections from the main radio towers or transmitters to the rest of the network) in these wireless

architectures is required at every site and is mainly done with land lines. The cost of using land lines to connect all these hubs is very expensive and time consuming to deploy. In addition, laying land lines is not practical or efficacious in emergency situations where ad-hoc command and control capabilities are required quickly. Connecting wireless hubs via land lines has proven to be very costly to implement and maintain due to their centralized switching model topology, vulnerability to single points of failure, potential for bottlenecks, and high latency. These centralized wireless systems also typically require large tower-based installations, which pose additional deployment issues in terms of cost, zoning approvals, site availability, security, and other location dependant issues.

Recent advances in software and hardware technologies in support of wireless system design allow for the replacement of much of the wired backhaul with wireless links resulting in a mesh network. These new routing technologies enable nodes or access points to communicate with other nodes, without the need to be routed through a central switch or transmitter. This eliminates the potential effect of local node failures and provides self-healing and self-organizing network connections to minimize bottlenecks and deployment issues. This distributed network architecture enables metro (jurisdiction-wide) scale mesh networks to be deployed using shoebox size access points mounted on existing infrastructure such as street lights, traffic signals, and buildings.

Mesh networking techniques, coupled with new high bandwidth radio systems can now offer the same or better reliability and capacities of land line based backhaul for a fraction of the cost. One of the key enablers of a mesh network node is the ability to “hop” its signal though neighboring nodes in the network via peer-to-peer links. The peer-to-peer links in the mesh network enable nodes to act as router/repeaters for

their neighboring nodes, which inherently extends the coverage, capacity, and robustness of the network for no additional cost. In the case where peer-to-peer and multi-hopping capabilities are extended down to the individual user device, ad hoc meshed networks can be set up with “zero infrastructure”. That is, the users themselves “are the network” and can form a broadband mesh among them anytime, anywhere. This enables mesh networks to be highly portable and deployable for first responders at an incident or remote location with each vehicle acting as an access point for other vehicles, something unavailable with traditional tower-based network topologies.

The links of a mesh network reconfigure themselves automatically as necessary to adjust to new users joining the network, node failures, or environmental changes such as interference or local node congestion. Each node identifies routes and pathways other nodes on the network can utilize by dynamically using sophisticated discovery query/response protocols. The better mesh systems available today consume very little network bandwidth, typically 1%-10% of the total to discover and maintain a “mapping” of optimal and back-up pathways through the network. Typically, this dynamic healing capability is not a feature found in centralized or tower based systems.

“Mesh networking techniques, coupled with new high bandwidth radio systems...offer the same or better reliability and capacities of land line based backhaul for a fraction of the cost.”

Intelligence within the nodes measures path information such as received signal strength, throughput, error rate, latency, user mobility, and a host of other parameters ensure optimal packet routing. Based on the link quality, each node then selects the best path to its neighbors, so the optimum quality of service is obtained at any given moment. There is an on-going process of optimization and self-healing constantly taking place between the nodes. This process sets mesh topologies (Figure 3) apart from hub-and-spoke (Figure 2) and point-to-point networks (Figure 1).

NETWORK TOPOLOGIES

Point-to-Point - (Figure 1) is the simplest form of wireless communications enabling two nodes to communicate with each other. Used most often to provide high-performance, dedicated connections, or high speed interconnections. It can be deployed relatively quickly, but is not highly scalable.

Point-to-Multipoint or Multipoint-to-Point - (Figure 2) Multiple nodes link a base station or an uplink node and other nodes. This type of network is easier to deploy than a point-to-point network since adding a new subscriber only requires equipment deployment at the subscriber site, not at the uplink node; however, each remote site must be within range and have a clear line of sight to the base station. This makes this

solution best suited for backhaul operations (e.g., connection to central site).

Mesh or Multipoint-to-Multipoint - (Figure 3) Networks create a routed mesh topology that mirrors the structure of a wired internet. Access routers are deployed throughout the coverage area until a maximum density is achieved. Each access router not only provides access for attached users, but also becomes part of the network infrastructure by routing traffic through the network over multiple hops. This enables any client to join the network at any point in the mesh, even if the clients aren't using a node. Clients can access the entire mesh, whether wireless or wired, making this the best choice for deployment in areas that require larger coverage.

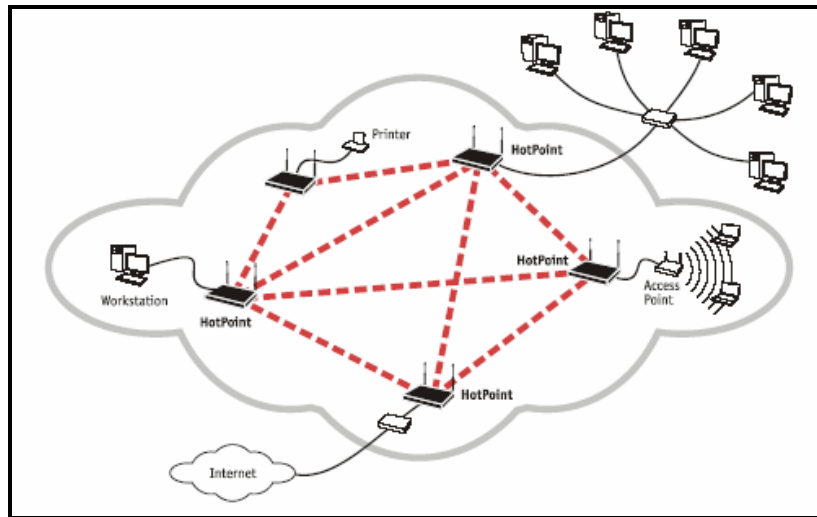


Figure 4: Metropolitan

Metropolitan - (Figure 4) Uses two types of mesh networks and is usually deployed to fulfill the Backhaul and Last Mile requirement. Backhaul is either a Point-to-Point or Point-to-Multipoint topology. The design provides a backbone to the uplink nodes. The prime mission is to bring bandwidth to different parts of the last mile. The uplink nodes in backhaul provide multi-redundant connections to the wired internet and can have capacities exceeding 11 Mbps. Depending on the size of the area covered, numerous backhaul points may be required to cover a large metropolitan area. Figure 4 depicts red lines (dashed) which are the wired backhaul lines that affect higher bandwidths than wireless can provide currently. Each node sees a mesh of wireless devices.

HARDWARE OR SOFTWARE REQUIREMENTS

The specific hardware and software required to implement such a solution varies depending on the specific variety of wireless technology implemented. It can include a PC device with a wireless network card, an 802.11 wireless client that will run in ad hoc mode, a mobile mesh software application, wireless routers, and Intelligent

Access Points (IAPs) that auto-configure requiring minimal additional work to implement. Wireless routers can be placed on light poles or other moderate vertical assets enabling extended coverage to the IAPs which normally are installed on fixed assets like buildings which then provide connectivity to fix wired networks.

ADVANTAGES, DISADVANTAGES, & RISKS

Advantages

Low Cost - When compared to that of comparable, centralized, tower-based systems, the simplified easement, construction, and maintenance considerations of a mesh network leads to much lower deployment and on-going operational costs.

Self Configuring - New nodes are automatically discovered and integrated into the mesh.

Self Tuning - Payload can be automatically balanced across the network via hopping and route optimization. Bandwidth and capital investment is optimized.

Self Healing - If a failure or congestion occurs in the mesh network, it can be isolated and traffic will be automatically routed around the issue.

Self Monitoring - The network, by virtue of the features, detects and reports on itself.

Non-line of sight connectivity - Unlike point-to-point or point-to-multipoint networks, mesh networks can route (i.e. hop) around obstructions and interference.

Interoperability - Modern mesh networks typically support industry standard Internet Protocol (IP). This means that existing internet ready applications, devices, and wired networks will seamlessly integrate and operate with a mesh solution.

Disadvantages

Throughput - For the most part, wireless networks can not match the capacity of end-to-end fiber or copper-based networks today. However, more access points can be added to a mesh network to increase capacity in high usage areas of the wireless network.

Interference - Some unlicensed wireless frequencies such as 2.4 GHz can suffer from interference generated by consumer wireless devices. Other frequencies can be used such as 700 MHz or the newly licensed 4.9 GHz public safety spectrum to minimize or eliminate these problems. There are trade-offs in using these frequencies in terms of spectrum & equipment availability. These issues should be resolved as soon as the market and users gain more experience and visibility with these new wireless solutions.

Training - Technicians need to acquire new skills for deploying, optimizing, and troubleshooting this new technology.

DOMAIN APPLICATION OF TECHNOLOGY

The public safety arena will always have a need to be flexible in meeting the needs of citizens and practitioners. Effective communications capabilities can mean the difference between life and death in a public safety incident first response. Although it is impossible to have a robust cost-effective communications network covering every location, wireless mesh networks are capable of providing a reliable and secure communications capability in many situations. In addition, wireless can be an

alternative to provide ubiquitous coverage over a geographic area such as a city, county, or even a state on an on-going basis. This may become the technology of choice in areas where laying cable and establishing other physical connection methodologies are impractical such as rural areas and those with inaccessible terrain. Finally, as coverage areas expand and terrain becomes too varied the capabilities of this technology can be stressed and more tried and true technologies may be more applicable.

ASSOCIATED STANDARDS

Wireless LAN mesh networks use standards-based IEEE 802.11a/b/g, but they can be extended to any radio-frequency technology. For details on 802.11a/b/g refer to <http://en.wikipedia.org/wiki/802.11a>.

IEEE 802.11 Task Group S – works on developing standards of interoperability for mesh networks.

CURRENT MAINSTREAM OR ALPHA/BETA USERS OF THIS TECHNOLOGY

Metro Scale Wi-Fi for San Mateo, California Police Department

The San Mateo Police Department (SMPD) used mobile data radio systems for years. Their legacy Data Radio Corporation system, while useful for computer-aided dispatch (CAD) and text-only incident information, was slower than dial-up (9.6 Kbps). The lack of true broadband connectivity essentially turned their in-car laptop computers into dumb terminals with practically no processing ability. Without field access to critical, bandwidth-intensive applications, the SMPD officers were forced to travel to headquarters several times (spending as much as 60%) per shift performing vital tasks such as report filing, database access, photo-lineup generation, and other investigative activities. The SMPD set a goal to make important tools and applications available to their officers in the field with a system that was cost-effective to deploy and maintain. Until recently, to get these applications to the officers in the field, San Mateo would have needed to install big pipe broadband systems, previously a cost-prohibitive proposition. The SMPD leveraged the lessons learned by attempts of other police departments and skipped over the 802.11 hot spot technology which requires officers to drive to specific sites for wireless information access which proved too costly and impractical for implementing large coverage areas. The SMPD chose instead a wireless mesh “hotzone” network that allows the police officers to write and file reports remotely and access law enforcement databases from their car laptops anywhere in downtown. Their hotzone is comprised of 17 Wi-Fi cells arranged in a mesh configuration with only two backhaul connections at strategic locations to the city’s fiber ring. With the Wi-Fi cells, the SMPD was able to create a reliable, large scale Wi-Fi network that would have otherwise been economically and logistically unfeasible.

Garland, Texas Police Mesh Network

Garland, Texas covers 57 square miles, has 221,000 residents, and the largest mobile mesh network in the world. Garland developed a communications vision for a fully converged high-speed data, voice, and video network where police, fire, emergency medical personnel, and eventually all city employees will be interconnected in real time. The Garland Texas Police Department’s Cellular Digital Packet Data (CDPD) network was outdated with transfer speeds of 19.2 Kbps, which are at least 20 times slower than current bandwidth technology and could not support the voice, data, and streaming video applications in the communications vision. Garland chose and deployed a wireless broadband network for public safety for several reasons. The deployment and conversion to the new system was simple as the users would maintain the same applications and interfaces, while increasing download speed dramatically. Instead of a traditional wireless network, this solution is a proprietary mesh-based network that does not use the 802.11 standard but instead pushes data, voice over IP, and streaming video through a series of network nodes that serve as repeaters and routers. A Network Operations Center (NOC) monitors the performance of the city's new network. The deployment of the solution is working. It started with the city's 290 police officers, including the mobile data terminals in 80 squad cars, which now receive data at 1.5+ Mbps while traveling at highway speeds in excess of 100 mph. The Garland police officers are using the network for voice, data, and streaming video. Conversion from the Department’s Cellular Digital Packet Data (CDPD) network was made within one week, during which mobile data terminals in the City’s 80 squad cars were outfitted with a new wireless interface and software. City officials started with data on the new network, using it as

part of the Computer Automated Dispatch (CAD) system to transmit 911 calls, alarms, report management, graphics, and mug shots to the mobile units. The city plans to expand the network to fire and emergency medical personnel, and eventually city employees will be interconnected in real time.

Medford, Oregon Gets City-wide Mobile Mesh Network

The City of Medford, which has a population of 70,000, is located on the border with Northern California, and is a fast-growing and progressive municipality. The city was preparing for the transition from a CDPD-based wireless network to one based on General Packet Radio Service (GPRS). While GPRS is faster than CDPD, it would still limit speed and bandwidth to less than a typical dial-up line. The city quickly realized that they needed a better option that would support their current needs and future capabilities. It learned that mesh technology provided a self-monitoring, self-healing, and dynamically expandable network based on the number of devices in the field at any point in time, and that survives natural disasters, physical attacks, and power outages. In addition, the city determined that they would save approximately \$24,000 annually by implementing the technology. Medford, launched the first mobile city-wide mesh network in Oregon. It covers 24 square miles and now provides high-speed communications to city employees in the police and fire departments, public works, and building inspection agencies. Medford is the largest city in Southern Oregon and has approximately 150 police officers and 75 fire personnel. Medford selected two different companies, one for the broadband solution network and another for systems integration, deployment, and project management. The new network handles data at DSL or cable modem-like rates, even while users are moving at highway speeds; provides anytime, anywhere access to mobile voice, video, data, and position location services. The network supports high data rates across both the upstream

and downstream connections; is quick and easy for users to send dashboard video, color photographs, and large reports back to the office or command center; and most importantly supports interoperability between a wide variety of devices, databases, and interagency networks.

North Miami Beach Police Go Wireless

The North Miami Beach Police Department deployed the first metropolitan-scale Wi-Fi network in Florida for law enforcement. They are using network equipment which is based on the 802.11b standard. With the wireless network, officer's log on to state and national databases via Wi-Fi equipped laptops and check drivers' licenses, vehicle registrations, and suspects' photos. Initially, the network covered a several square block area centered near the central police headquarters and plan to expand the network to cover the entire city core of North Miami Beach, an area of over five square miles. The police department chose a Wi-Fi network because the legacy mobile data system they have been using for years is being discontinued by its provider. In their search for a replacement, they discovered that available cellular-based systems require expensive recurring charges and their performance pales in comparison to the broadband speeds offered by a metro-scale Wi-Fi system.

Golden Gate Safety Network (GGSN) Exercise (Wireless Broadband Meshing)

The Golden Gate Safety Network (GGSN) is a San Francisco-based coalition of federal, state, and local public safety agencies. In 2002, 17 agencies developed the Golden Gate Bridge Major Incident Response Plan that detailed the communication challenges and started the history of the project. The mission of the GGSN is to develop a regional public safety communications plan and explore new communications systems that will enable multi-agency, interoperable communications to support day-to-day incidents as well as large-scale emergencies. On February 12, 2004, the GGSN conducted an Interoperable Communications Exercise that instantly enabled thirteen public safety

multi-jurisdictional agencies to communicate seamlessly on a secure, mobile broadband. This Homeland Security exercise simulated a terrorist attack at the Golden Gate Bridge and used a network software solution to meet several project goals including rapid deployment, interoperability, mobility, autonomy, and remote, real-time participation by the California Governor's Office of Emergency Services over 100 miles away using a standard internet connection. The communication system software easily loaded onto 802.11-enabled, standards-based laptops, tablets, and PDAs, allowing every device to send, receive, and route data which eliminated dependence on a fixed infrastructure throughout the rough terrain of the land and over the water of the Golden Gate National Recreation Area. It instantly formed an extended Wi-Fi hot-zone on the fly which can operate with or without access points - known as an autonomous mobile mesh network. This autonomous network is complemented with server-less broadband applications including real-time video, resource tracking, multimedia instant messaging, and white-boarding. For the first time, multi-jurisdictional agencies were able to immediately generate and share media-rich, mission-critical, real-time video and data via networking software and multimedia applications. This system improved the efficiency of first responders in all seven scenarios of the SAFECOM Statement of Requirements and reduced the voice radio communications by as much as 70% during the exercise. This exercise was an important milestone in driving the Golden Gate Safety Network closer to its vision to develop and implement a regional communications system that supports a multi-agency response from local, state, and federal first responders for day-to-day operations and incident management.

Buffalo, Minnesota Gets Mobile Mesh Network

The city is near Minneapolis, has 13,000 residents, and covers nearly 8 square miles. Buffalo's limited resources were being over-taxed and attributed mostly to office-bound,

record-keeping activities. Buffalo's utilities, streets, and parks employees were making several trips to the office each day in order to access maps and drawings, collaborate with other staff members, and to check duty assignments. Police officers needed to go back to the station to look up driving records and file reports. The fire department operated at greater risk as they did not have field access to available structural drawings and known hazardous materials information. Buffalo developed a vision to solve this issue by bringing the office to the field with mobile technology units. Buffalo, Minnesota chose, deployed, and implemented a mobile wireless mesh network to enable remote, mobile high-speed access to public safety and nonpublic safety resources in the field to increase their productivity and save on costs. The public safety applications now available in the field include crash reporting, field incident and citation entry, and access to the states centralized databases including CrimNet and DMV. In addition, nonpublic safety applications include customer service request response, access to city-wide, geofile graphic information, and field reporting entry. Both implementations have saved the city time and money by enabling field personnel to stay in the field longer rather than having to return to their offices to complete record-keeping tasks. Workers in the field can access information stored on the LAN, the email server, and to all web-based applications and databases. Utility, street, and park employees now have real-time, wireless access to the most recent drawings while they are servicing a house meter or locating a fiber optic line and the ability to collaborate calendars or information with colleagues spread across the city. The police officers can search driving records and file reports while still in their squad cars. The fire department can access CAD information on any structure in the community before they enter a building. Their mobile wireless connection enables them to determine the presence of known hazardous materials at a location, as well as the building owner's name and telephone number. The mobile wireless system has

enabled communication along all levels of business and allowed transparent (mobile or office), real-time communications, and is

integrated with the city's wireless internet service.

LINKS TO MORE INFORMATION

As a service, some mesh companies are randomly listed below for consideration.

Motorola, Inc:

www.motorola.com

Boingo Wireless, Inc:

www.boingo.com

Strix Systems:

www.strixsystems.com

Network Solutions:

www.meshnetworks.com

L-3 Communications Nova Engineering:

www.novaroam.com

Cisco Systems Inc.:

www.cisco.com

Firetide, Inc.:

www.firetide.com

Tropos Networks:

www.tropos.com

Nortel Networks:

www.nortelnetworks.com/solutions/wrlsmesh/