Wireless Mesh Networks: Traditional Uses and Video-Surveillance Applications

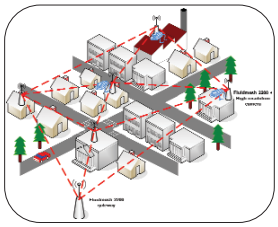
Umberto Malescim, president and co-founder
Fluidmesh Networks, Inc.

Wireless mesh networks have undergone much academic research over the past twenty years. The Defense Advanced Research Projects Agency (DARPA) funded research of mesh networks because of their inherent reliability and flexibility, in the hope of applying them to military applications. Mobile and nomadic communication in the battlefield or in hostile environments was the original optimum application of mesh networks.

The absence of any single point of failure makes mesh architecture the ideal network topology where many-to-many communications are possible but one doesn't want to rely on layered and stellar architecture. Every node is a peer node in a mesh network, and there is no higher layer or controlling node that can be destroyed to bring down the entire network. The unmatched reliability and flexibility that a mesh-capable transmitter offers, compared to traditional wireless devices, are making wireless mesh the preferred network architecture for high-end wireless video-surveillance, condition-monitoring and wireless SCADA systems.

Self-Forming and Self-Healing Mesh Networks

Nodes in a wireless mesh network are powerful devices that run advanced mesh routing algorithms designed to evaluate and select the optimal path for every transmitted packet in real time. The dynamic mesh routing algorithm allows the routing of packets and video streams around obstacles, sources of interference or low-quality links, increasing reliability and flexibility at the same time.



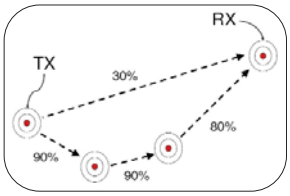
Wireless mesh and video surveillance used in an urban environment.

Wireless mesh devices are completely auto-configurable, the routing protocol finds other mesh devices nearby and the location of the base units attached to the wired network. If a link goes down, the nodes in the network will immediately notice the failure and change their preferred path to avoid the failed link.

Routing of Packets in a Wireless Mesh Network

Routing in a wireless environment is conceptually similar to routing over the Internet, but is different in terms of evaluating the quality of a particular path. While Internet routing is based on minimal hop count, the quality of wireless links in a mesh network is crucially important. Researchers at the Massachusetts Institute of Technology (MIT) recently discovered that minimum hop count is not effective for wireless routing. Rather, a metric involving link-quality measurement is needed to create reliable wireless mesh networks. This discovery broke most of the layered abstractions developed by the "inventors" of the Internet in the 80's and 90's and established new ways of thinking about wireless routing.

It's easy to see the importance of link quality in a wireless environment. Wireless links tend to have high packet-loss rate and the transmitter needs to resend the lost packets multiple times, wasting valuable bandwidth. Consequently, it's often preferable in a mesh network to take a longer yet more reliable path rather than the unreliable direct route to the end point. Often the shortest path would require multiple retransmissions per packet, wasting bandwidth and increasing delays.



In a wireless mesh network, the shortest path may have a low success probability (30 percent success rate) than a longer path (90 percent/90 percent/80 percent = 65 percent success rate).

By continuously probing the different wireless links, every mesh node builds and updates statistics regarding every link available. These link-quality tables are then used by the routing protocol to compare every possible path and pick the optimal one at any given time.

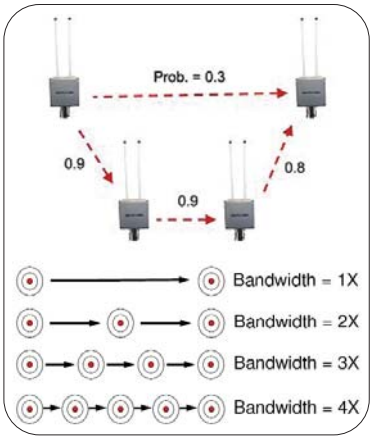
Origin of Wireless Mesh Networks and Their Traditional Uses

Many defense-related applications of mesh networks involved highly mobile and battery-powered units, creating challenging technical problems whose solutions are still in their infancy. However, mesh networks for data transmission, video-streaming or temporary communications in case of natural disasters are a reality today, with several different products focused on different types of applications.

Challenges in Streaming Video Over Wireless Mesh Networks

Video-streaming and video-surveillance have been one of the latest additions to the list of possible applications for mesh technology. However, high-resolution video-streaming over a mesh network presents several technical challenges: bandwidth is always scarce when dealing with high resolution video and a multi-hop transmission may decrease usable bandwidth and increase delay. For example, a video packet that goes through three hops absorbs three times the bandwidth compared to a video packet that is only one hop away from its destination.

Advanced mesh products solve these challenges by operating multiple radios simultaneously. In this way, the video stream can use many different channels to create high-bandwidth and low-delay paths. Operating multiple radios increases the bandwidth by spreading the transmissions on multiple non-overlapping channels while decreasing the delay of the network. At every hop the packets go through, the mesh transmitter can choose the best frequency to reach the following node, therefore optimizing not only the path but the frequency spectrum usage, as well.



In a single-radio mesh network, adding a hop decreases the total available bandwidth by half because every packets needs to be transmitted twice.

Routing in a multi-hop, multi-radio mesh network requires, however, advanced routing algorithms and powerful processors embedded in the transmitter. The optimization work is computationally expensive and the processor needs to continuously crunch and solve complex optimization problems in real time.

Advantages of Using Wireless Mesh Networks for Video-Surveillance Applications

Mesh architecture is the solution to several problems faced by security system integrators when they work on wireless video-surveillance systems. Mesh devices are completely auto-configurable and capable of deciding how to transmit packets based on the present conditions of the channels rather than on pre-determined configuration values.

Reliability and flexibility are intrinsic benefits of mesh architecture. Unpredictable sources of interference do not need to be anticipated as the network will identify the position of the source of interference and start routing packets around low-quality links. Airports and seaports are typical locations where mesh architecture solves several problems at once.

Airplanes taxiing on the ground are often unpredictable and moveable sources of interference. During the design and the installation of a mesh-based CCTV system, it's not necessary to identify every possible position where an airplane can be interfering in the video streaming quality. The mesh network itself will find alternative paths in case some of the links are not usable due to interference. Similarly, using traditional wireless technology in commercial seaports is also very challenging because loaded container ships are almost moving buildings, making the design of a traditional static wireless network almost impossible. However, using a mesh-based architecture, video-streams will change their path in case a container ship docks in the middle of a wireless link impeding transmission through that particular path. The transmitter will always have an alternative to reach the base station.

Using traditional point-to-point solutions large obstacle like hills, buildings or forests require the installation of high towers or poles to create line-of-sight between the antennas. Video-streams don't have to overcome these obstacles when taking a mesh-based approach but can simply be routed around them. Line-of-sight is not required from the camera directly to the base station, it's only needed for the next node in the mesh network that will then relay the stream to the following one and so on until the packets reach the base station.

Automatic Solution for Exogenous Interferences

Large industrial areas are often characterized by a high density of RF devices, and the problems related to exogenous interferences deriving from other transmitters are rather frequent.

The types of interferences that may occur are due mainly to:

- Other transmitters operating on frequencies close to or coinciding with those used (e.g., Wi-Fi networks, Hiperlan data networks, and analog radio links for various purposes including video-security);
- Different devices whose operation creates interferences in the bands affected by the transmission (e.g., radars or microwave ovens).

Conversely, low-frequency (UHF, VHF) radio equipment or cellular towers are not sources of interference for most 2.4 GHz and 5 GHz radio equipment. Only extreme physical proximity of the antennas could result in reduced transmission performance.

Interference is one of the most complex phenomena that need to be tackled in the area of radio transmission. It must be addressed simultaneously at different levels using the least busy channels, while also introducing redundancy into the system so that it can assist with automatic adjustment in case of unexpected interferences.

During preliminary inspections and installation, it's important to be able to evaluate any possible interferences caused by other wireless networks existing in the area. (A Wi-Fi device in listening mode or a spectrum analyzer may be used to identify them.) It's also always advisable to ask the customer about the existence of other radio devices in the area, their carrying frequency, their bandwidth and power. Careful planning can solve a large percentage of problems relative to interferences.

When operating on license-free bands, keep in mind that the absence of a wireless network on the day of testing doesn't mean that one cannot be installed in the near future. Consequently, it's important to introduce redundancy into the network and use dynamic equipment that's able to identify new interferences and respond to minimize their effects. This approach usually requires the use of smart radio equipment, often of the mesh type, set to perform constant transmission channel analysis and to select in real time the best pathway within the network and/or channel most free of interference.

Smart radio equipment can help users avoid interference in thier wireless mesh surveillance application.

Conclusion

Mesh topology is undoubtedly a step forward in wireless networking applied to video-surveillance applications. Reliability and flexibility unmatched by any other wireless solution are intrinsic in this innovative architecture, where every node in the network is an "intelligent" router capable of forwarding packets received from nearby units and deciding in real time the optimal path based on the channel and network conditions.

Mesh networks also enable the installation of wireless CCTV and SCADA systems where other wireless solutions fail, such as in the presence of moveable obstacles or sources of interference. Mesh networks are also allowing the design and installation of condition-monitoring and security systems with the reliability of a wired network but a higher flexibility than any point-to-point or point-to-multipoint wireless system.

About the Author:

Umberto Malesci

President and co-founder of Fluidmesh Networks, Umberto Malesci is one of the leading designers and developers behind Videomesh technology and architecture. He has extensive experience in academic research in the field of wireless networking, working as a researcher at MIT CSAIL (Computer Science and Artificial Intelligence Laboratory), at the Media Lab in Cambridge, MA and at IMSC in Los Angeles.

Mr. Malesci received a Bachelor of Science in Electrical Engineering and Computer Science as well as a Master of Engineering in Electrical Engineering and Computer Science, both from the Massachusetts Institute of Technology (MIT) in Cambridge, MA (USA).

Fluidmesh Networks is the global leader in wireless systems for security and mission-critical applications based on mesh networking technology. The company is focused on the development of superior quality wireless products for a wide array of video surveillance applications.

Founded by a team of researchers and engineers from the Massachusetts Institute of Technology (MIT) in Cambridge, MA and the Politecnico of Milan in Italy, Fluidmesh Networks serves its customers worldwide from its headquarters in Boston and its European office in Milan, Italy. For more information please vist www.fluidmesh.com or call 866-58-1522.

Hear Fluidmesh Speak at the Remote 2008 Conference and Expo!
Session Title:Wireless Mesh for Industrial and Security Applications
www.RemoteExpo.com