Concentris systems

A Concentris Systems White Paper

Wireless Mesh Networked Sensors in Security Applications

Advances in sensor technologies and wireless mesh networking offer great promise for military and homeland security applications, including perimeter and facility security. Using a common object-oriented management platform to connect heterogeneous sensors via a wireless mesh network, it is now possible to create rapidly deployed, low-cost security networks that are reliable, flexible, scalable, and easily upgraded.

Introduction

Since 9/11 the federal government has allocated more than two billion dollars to sponsor research to develop technologies such as video cameras, motion detectors, RF sensors, hyper-spectral imaging, and acoustic sensors for purposes of building sensor systems to protect facilities, forces, and other potential targets. Many federally funded research projects have recommended using wireless mesh networks to enable sensors to relay information to one another and to communicate with central command points.

To truly unlock the revolutionary capabilities of wireless mesh networked sensor systems, a common management platform that can seamlessly connect large numbers of heterogeneous sensor types into an integrated system is required. This platform needs to be capable of supporting high-performance data fusion and providing command and control of the sensors themselves.

Advantages of Wireless Mesh-Based Security Networks

Derived from military-funded research into mobile battlefield networks, mesh networking functions without a central controller and, thus, eliminates the reliability and efficiency issues associated with central control. Instead of a central controller, mobile ad hoc mesh networks use peers in the network to transmit data from source to destination by means of multiple hops. Mesh networks use an Internet-like routing scheme to provide high-bandwidth connections that are extremely secure and reliable, and offer the necessary Quality of Service (QoS) characteristics to support data and multimedia traffic, including high-resolution video.

One clear advantage to using mesh technology in a security network is its relative invulnerability to disruption due to physical attack. Because mesh networks are designed to route around points of failure, they are highly resilient. Moreover, mesh sensor networks do not require connecting wires or cables between sensors or large radio antennas, both of which may be vulnerable points in conventional networks.

Eliminating wires and cabling between nodes also dramatically reduces the cost and the time required to deploy a functional network. In addition, wireless mesh networks are extremely flexible and can be easily reconfigured to support additional sensors or the redeployment of existing sensors to areas of greater need. These advantages make wireless mesh networks ideal for emergency or temporary deployments such as special events, flexible perimeters, or ad hoc situations when a particular facility is thought to be a target.

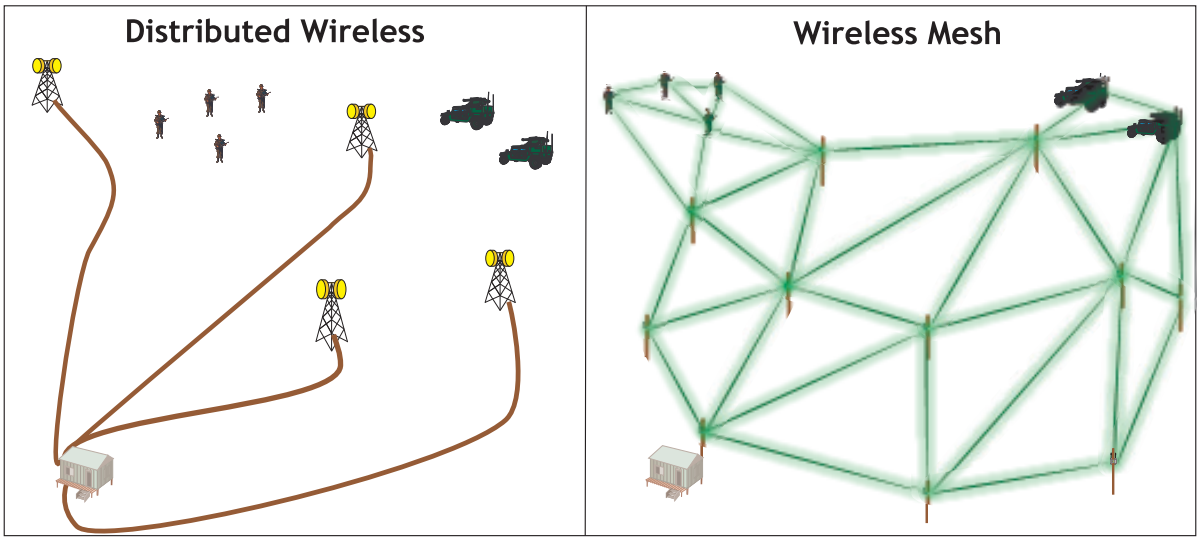

Figure 1: ***A traditional distributed wireless topology requires miles of cable and large fixed antennae, while a mesh topology relies on peer-to-peer communication between low-cost, relatively low power radios. Mobile mesh nodes mounted on vehicles or carried by personnel are instantly integrated into the mesh***

Mesh networks were designed to provide mobility in battlefield environments. Using a mesh network, both the mesh nodes themselves and network devices, such as sensors and monitors, can be mobile. Vehicles and personnel outfitted with sensors and mobile mesh nodes become part of a dynamic network that can instantly respond to threats by relocating mobile sensors and/or adding communication links.

In addition to its resilience in the wake of a physical attack, a mesh network can be made highly resistant to cyber-attack using end-to-end encryption of data and *trusted peer* certificate-based security algorithms. Furthermore, mesh networks are highly scalable, capable of supporting many thousands of network nodes and, theoretically, millions of sensors.

This high degree of scalability offers great potential for security networks. By networking together large numbers of relatively low-powered sensors, researchers have demonstrated exponential improvement in the sensors' ability to blanket large areas as well as enhancement in the quality of information obtained by the sensors. By combining and comparing data obtained from multiple sensor points, sensor arrays augur powerful new capabilities.

For example, Concentris Systems™ is working with researchers at the US Army Armament Research, Development and Engineering Command (ARDEC) to develop a system that will employ a sparse array of low-cost mesh networked acoustic sensors to collect ambient sounds and utilize signal processing methods to extract individual signal sources, determine whether they pose a threat, and, if so, use localization algorithms based on time-difference of arrival (TDOA) between sensors to pinpoint the geographic origin of the threat. This system is designed to allow Warfighters to identify and locate hostile fire. The technology is also applicable to perimeter and facility security, or any situation where potential threats might emit acoustic signatures that differ from the normal acoustic environment.

Sensor Management and Monitoring via Intelligent Mesh Nodes

A mesh network possesses many inherent advantages as a communications platform for sensor networks. Perhaps the most exciting advantage of the mesh-networked approach lies in its ability to distribute computing power throughout the network, turning low-cost commercially-available sensors into controllable and programmable 'smart arrays' and enabling much of the required data-fusion and data-storage to be performed at the network edge.

For example, a single mesh node can tie dozens of low-cost commercially available WiFi-enabled digital video security cameras into a single 'smart array' of sensors operating in unison to provide coverage of a vulnerable area or route of ingress/egress. Rather than flooding the network with data from multiple video streams to a central controller, the video can be aggregated and parsed by the intelligent mesh node, which can then forward useful information to the central controller and other network nodes. These intelligent nodes can also compress and store the video data for retrieval when needed or when the network has excess

Ten Advantages of Mesh Assisted Sensor Networks

1. **Low Cost** – *Using relatively low power, commercially available radios and requiring no cabling or wires, mesh networks provide a low-cost alternative to wired or distributed RF networks.*

2. **High Bandwidth** – *Commercially available 802.11g mesh networks are capable of speeds up to 100 Mbps, and new MIMO technologies promise further speed gains.*

3. **Quality of Service** – *QoS algorithms enable transmission of multimedia traffic and video with little or no loss or latency.*

4. **Flexible** – *Mesh networks support any IP-enabled device or application.*

5. **Scalable** – *Mesh networks can quickly scale to thousands of nodes covering hundreds of miles.*

6. **Quick to Deploy** – *With no wires or cables to string, fully operable mesh networks can be deployed in minutes.*

7. **Reliable** – *Each mesh node is backed up by multiple peers, providing an always-on grid of communication links.*

8. **Resilient** – *Like the Internet, mesh networks are designed to route around points of failure, making a properly designed network immune to single point physical attacks.*

9. **Secure** – *Originally designed for military use, mesh networks can provide military-grade data and information security.*

10. **Mobile** – *Mesh networks support mobility of both mesh nodes and client devices, establishing new links with no user intervention required.*

bandwidth. Research has demonstrated that such an approach, properly executed, would reduce demands on network bandwidth and computing resources while conserving sensor node power.

Five Advantages of Object-Oriented Sensor Fusion

1. Intelligent Sensor Preprocessing *– Distributed processing environment can handle event detection, buffering and prioritization at node level.*

2. Rules Based Permissioning *– Access to sensor data based on authentication and permissioning rules and algorithms. Data can be distributed to multiple recipients via a publish/subscribe framework.*

3. Distributed Retention and Archiving *– Minimizes the consumption of scarce networking capacity and resources.*

4. ***Field Upgradeable*** *– Node-level sensor processing rules and algorithms can be dynamically upgraded to incorporate changing conditions or enhanced functionality at any time.*

5. Ease of Integration *– Each node can intelligently interface with a multitude of sensors from many vendors and present a unified XML based messaging API to higher level applications*

In addition to handling network traffic routing, mesh nodes can also provide command and control capabilities for individual sensors or sets of sensors. In a fully realized system, the mesh nodes provide an open-architecture that enable sensor vendors and third-party developers to port device drivers, software algorithms and downloadable applets to the mesh nodes, which are then able to control sensor behavior based on inputs from sensors, other nodes, end-users, and internal logic.

As the cost of computing power continues to drop, it is easy to envision computation-heavy applications, such as facial recognition, that are currently performed on central servers moving to the network edge. To realize this vision, a flexible architecture that supports seamless integration of new applications and allows distributed nodes and client devices (e.g. sensors and handheld wireless devices) to be easily upgraded is required.

Java™-based Messaging/Management Environment

The required architecture would likely consist of a standard, open-source API linking mesh nodes and sensors together with a Java/XML-based messaging/management platform that would reside on the mesh nodes. Java applets could then be written and downloaded to the mesh nodes, enabling the execution of simple commands or complex programs. These applets could be downloaded on the fly in response to external trigger events (letting the network ‘wake up’ dormant sensors, for example) or set up as virtual arrays of sensors to work in unison when needed and then dismantled when they are no longer needed.

One of the many benefits of a Java-based messaging/management platform is that Java was designed to provide client-side ‘managed execution’ of applets, giving the network protection from malicious or corrupted applications. When combined with the inherent redundancy of mesh topology, this approach limits the extent of network damage that might result from faulty applications or cyber- attack.

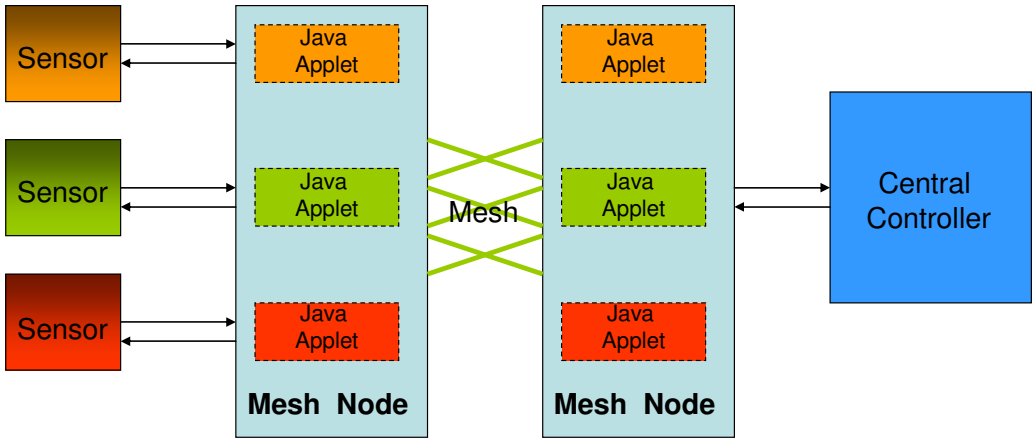

Figure 2: ***An object-oriented, open-systems architecture for a flexible wireless mesh-based sensor system. Intelligent mesh nodes control sensors via downloadable applets and handle the archiving, compression, and routing of sensor data. A central controller distributes applets to govern sensor behavior and requests sensor data on an as-needed basis.***

Among the available alternatives, a Java-based platform is also the most developer-friendly. Sensor equipment manufacturers could draw from a pool of programmers versed in Java and large libraries of customizable applets. In addition, Java's "Write Once, Run Anywhere" architecture would provide a high degree of application portability as new sensors and intelligent nodes are developed.

Conclusion

A Wireless Mesh Assisted Sensor System offers an extremely scalable and flexible platform capable of supporting almost infinite configurations of heterogeneous sensor types. This system allows for experimentation with various combinations of sensors and sensor behaviors to achieve optimization and would be easily adaptable to other facilities and security environments. It would support complex applications as well as low cost commercially available sensors. By eliminating redundant, system-specific communications networks, it would dramatically reduce the costs and resources required to deploy and operate large-scale, state-of-the-art security sensor systems.

About Concentris Systems

Concentris Systems LLC is a minority-owned small business based in Honolulu, Hawaii. Concentris focuses on research and development of wireless mesh networking technology for military, homeland-security and other severe-duty applications.

Concentris' management team pioneered the commercialization of mesh networking technology. Representing the next generation of mesh technology, Concentris' RapidLink™ platform is the only commercially available networking system that uses open standards-based OLSR mesh routing. OLSR is a proactive mesh protocol that enables enhanced network performance while supporting highly scalable mesh networking topologies. Designed to meet military specifications, RapidLink provides high-performance reliable links that function even in harsh radio propagation environments, enabling self-configuring, self-healing networks that can be deployed very quickly. RapidLink products are ruggedized to meet the most demanding environmental conditions, can be configured to support a variety of wireless radio technologies, and are available as both fixed and battery-powered portable nodes.

RapidLink mesh routers enable users to rapidly deploy secure, reliable, and scalable data networks for use in sensor networks, secure perimeter systems, field offices, emergency or temporary venues, and many other applications. Concentris RapidLink networks are deployed faster, cheaper, and easier than any conventional wireless technologies. Quick to deploy and resistant to failure, RapidLink networks are truly *Indestructible Instant Networks ™*. www.concentris-systems.com