Echelon Corporation
550 Meridian Avenue
San Jose, CA 95126
Phone: +1-408-938-5200
Web: www.echelon.com

Radio Frequency Control Networking:

Why Poor Reliability Today Hampers What Could Be a Viable Technology in the Future

A Technology Assessment

Abhay Gupta & Michael R. Tennefoss

005-0171-01B

www.echelon.com

Contents

Figures

Tables

Introduction

A control network consists of sensors, actuators, displays, and other electrical devices that exchange information with each other over shared communication media. In order for information to be exchanged reliably, the communication media must be highly robust and able to compensate for sources of interference frequently found in the intended operating environment.

Commonly used communication media include twisted pairs of copper wires (called twisted pair medium), power lines, fiber optic cable, coaxial cable, wireless infrared, and radio frequency (RF). Each medium has different strengths and weaknesses (see Appendix 1); users typically select a medium based on the intended operating environment.

Users often employ two or more different media in control systems for cost and/or reliability reasons. For example, it may be prohibitively expensive to install new twisted pair wiring to reach certain existing devices, so a hybrid twisted pair and power line solution may be best for such an application. Likewise, the presence of metal construction material or wireless data networks could make an all RF-based system unusable or unreliable; a hybrid RF and twisted pair system would overcome these limitations. Having access to a suite of media to create such hybrid solutions can mean the difference between a robust, reliable control network and one that has stability and operational issues.

RF: Everywhere and Nowhere

Much has been made in the popular and technical press about the benefits and capabilities of new RF-based control technologies. Through the use of mesh (repeater-based) networking and new protocols, these technologies are purported to offer the performance of twisted pair solutions but with lower device and installation costs. Among the better known new RF-based technologies are ZigBee©, Z-Wave©, Millennial Net©, and Dust©.

Echelon recently completed a year-long investigation of these technologies, and our findings were very different than we expected. We expected to test high-performance, highly reliable twisted pair replacements, but found just the opposite: the new RF technologies offered very poor robustness against sources of interference, very limited distance operation, mediocre battery performance, and in one case, response times slower than sneaker net.

The underlying RF modems used within these control networks are made by, or the technology is sourced from, a common pool of semiconductor manufacturers. While each RF technology supplier calls its solution unique, the technologies share many common underlying elements — and limitations. For example, all of these systems use mesh networking, in which RF-based devices can also operate as repeaters, to compensate for the poor distance of their radio. Yet even with repeaters enabled, some systems in our tests could not operate reliably in a commercial building or ranch-style U.S. home.

In the following sections, we'll investigate the limitations of the current crop of mesh networking RF networks, and explain why these systems don't deliver on the promise they hold. RF technology could one day become an explosive force in the control networking market, but today it's best relegated to the laboratory so that technologists can finish the development work they started.

Signal Propagation Losses

The strength of an RF signal drops 6dB for every incremental doubling of open field distance with no impairments or obstacles. The presence of typical building construction materials such as gypsum panels, metal-foil wall paper, aluminum wall braces, and office or factory equipment further reduces RF signal strength. An RF signal drops inside a typical building with obstacles/impairments by about 25dB for every incremental doubling of distance. RF mesh network suppliers quote radio signaling distance assuming an open field transmission with no impairments or obstacles between the transmitter and receiver. This scenario is impractical, akin to measuring gas mileage in a car that's driving downhill.

In real-world environments, such as a standard commercial building or a home of roughly 2,700 square feet, the situation proved quite different. None of the RF mesh networks we tested could operate in the presence of metal or stucco walls, metal-foil wall insulation, metal floors, or in L-shaped homes using these construction materials. None of the radios could operate reliably at 30 meters. At distances as short as 10 meters, the radios had insufficient operating margin to work reliably over time. Turning on noise sources dropped the operating distance so low that repeaters would be required every 5 to 8 meters.

Network Traffic in Shared Frequencies

Since RF signaling is regulated by national governments, all of the RF technology suppliers must share their assigned RF frequency spectrum that's in common with other authorized RF-based devices and systems. The devices that share the 868MHz (EU), 915MHz (US), and ISM 2.4GHz bands that unlicensed, mesh network-based control networks operate on include 802.11 (WiFi) routers and network interfaces, cordless phones, Bluetooth devices, audio and video extenders, closed circuit television transmitters, and other control networking devices.

The interference between different wireless devices reduces reliable communication between any two devices. Various RF technologies use different techniques to mitigate interference caused by other devices in their space. For example, WiFi and ZigBee use direct sequence spread spectrum (DSSS) to distribute the information over a wider bandwidth, while Bluetooth uses frequency hopping spread spectrum (FHSS) to randomly move from channel to channel. Cordless phones based on both DSSS and FHSS are available on the market. Interference among multiple DSSS devices operating in adjacent bands poses a problem due to overlapping caused by spectral re-growth of the frequency bands. The net result, compounded by shared use of a limited frequency range, is reduced system performance and reliability.

The growing number of RF devices operating within the shared frequency bands is creating virtual RF traffic jams, and a corresponding degradation in reliability. In our tests, none of the existing mesh networking radios operated reliably in heavily trafficked RF bands: the radios experienced low effective bandwidth in most cases, and a complete loss of communication in extreme cases. Figure 1 on the next page demonstrates how a single WiFi router spreads energy across the frequency bands used by ZigBee to the point where reliable signal reception is not possible.

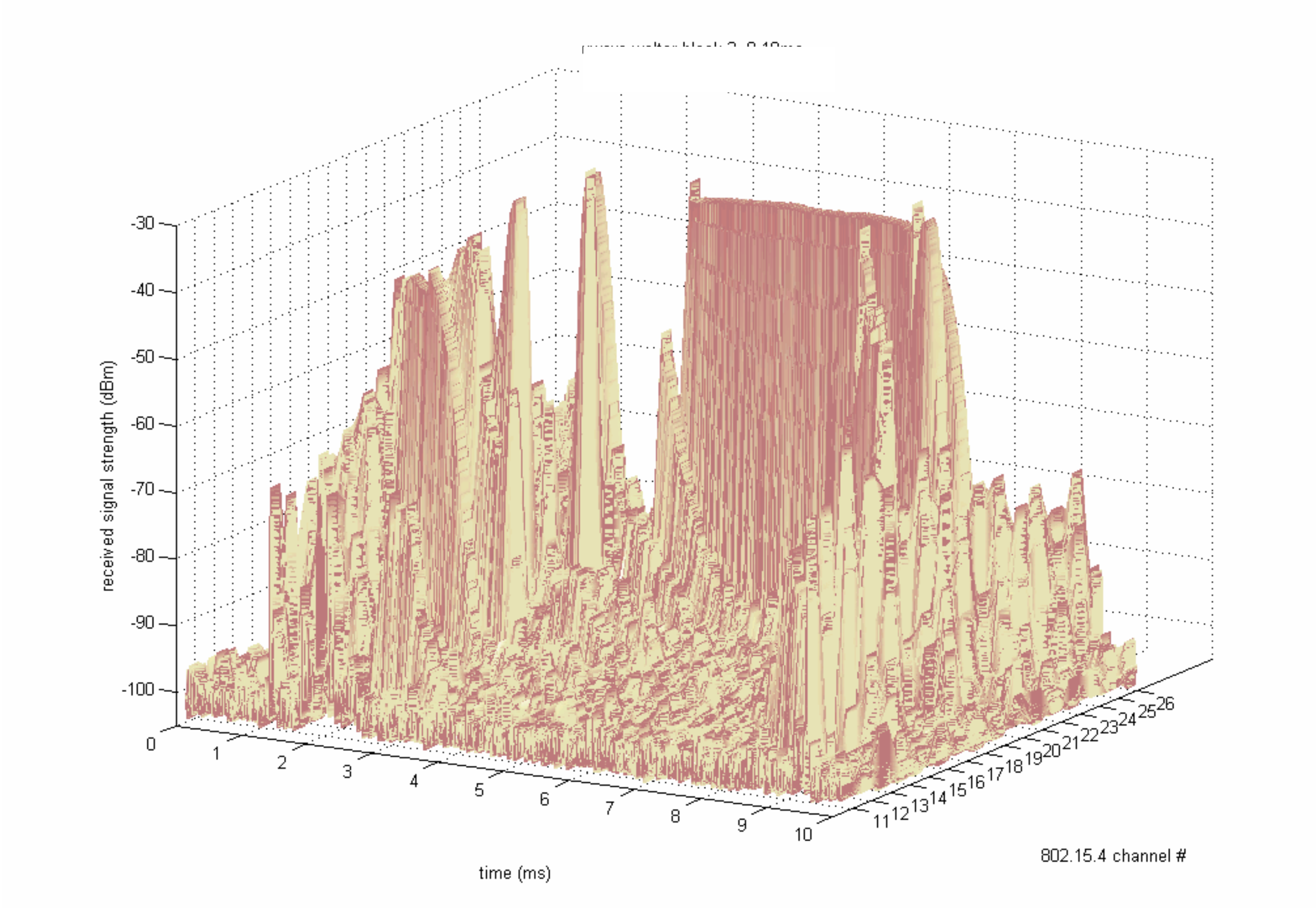

Figure 1. WiFi Router Interference with ZigBee 802.15.4 Radio

The proliferation of WiFi devices, cordless phones, Bluetooth-enabled devices, and similar products in homes, buildings, and factories makes ZigBee-based devices extremely susceptible to interference. As with other impairments, WiFi devices might not be present when an RF mesh network is originally installed but could be added later. Even if a service person is dispatched and can locate the source of interference, it might be impossible to solve the problem due to the location, purpose, and ownership of the interfering device.

RF Multipath and Distortion

Some manufacturers tout the use of DSSS and FHSS military spread spectrum radios as highly effective in preventing jamming, multipath (ghost signals caused by reflections off of certain metal surfaces and materials), and signal distortion. In fact, none of the mesh networking RF technologies have the sophistication and processing power of military radios. The result is erratic RF system operation despite the use of spread spectrum technology.

For example, ZigBee spread spectrum radios have demonstrated susceptibility to multipath interference from metal and metal-foil line surfaces. The multipath signal cancels the original RF signal, resulting in erratic system operation. Other forms of signal distortion cause these spread spectrum radios to lose sensitivity, drastically reducing their operating range.

Since the sources of signal multipath interference and distortion may vary with time and location, they may not be observed when the RF mesh network is originally installed. Changing the location of metal equipment on a factory floor or behind a gypsum wall may also create multipath interference that didn't exist during system installation. Mesh repeaters may not solve this issue when the location of multipath interference source is unknown; their value is primarily in extending signal range and overcoming obstructions such as metal objects.

Multipath interference at 2.4GHz can often be overcome by moving a device a short distance (typically 3cm to 6cm) to avoid the reflected wave. While this is a simple remedy for a mobile phone or cordless headset, it's less so for machines and control devices. Once installed in the field, machines and other control devices face time-varying multipath effects caused by reflections from objects and people moving in and out of their operating range.

Multipath and signal distortion are difficult to troubleshoot since a technician must be present when the problem occurs in order to determine its source and a viable remedy. The net result for product manufacturers? Higher warranty costs compared with a twisted pair or power line solution.

Battery Life

The use of battery-powered wireless technology adds another variable to the operation and maintenance equation. RF mesh technology suppliers have to balance battery life against system latency (delays from the time a signal is triggered until it can be acted upon). Dust networks allows repeaters to be battery powered by powering down the device network and waking it up from time to time to conserve battery life. This technique works with respect to battery life but comes at a very high price — signal latency can exceed 15 seconds from the time a device is triggered until a reaction occurs. Such a long latency rules out the technology for any real-time applications such as security monitoring, lighting, fault alarms, remote controls, or any activity requiring feedback to a user.

Another RF mesh technology, such as that made by Millennial Net, requires that repeaters remain powered at all times. This means that while some devices are battery-powered, others must be mains-powered. Given the poor range of the radios used by Millennial Net, mains-powered repeaters must be located closely to battery-powered devices. This architecture calls into question the purpose of having a battery-powered network in the first place.

Even if batteries are not used within the RF control devices themselves — for example, because they're located in luminaires that already have access to mains power — battery-powered mesh repeaters may still be required. This is because the optimal location of a mesh repeater will be determined not by the availability of mains power but by multipath interference, distortion effects, and proximity to the devices whose signals must be repeated.

The approximate battery life of a control device can be easily calculated. Assume that a simple device (a simple processor and sensor) consumes 20mA at 3V when awake. Add to this the current requirement of a transmitting or receiving radio, typically 20mA. Also, assume that the device wakes up for only 5ms at a regular interval of 2 seconds. Neglecting the energy consumed by the device during sleep, this requires an average current of 40mA * 5ms / 2s = 100μA. With this current consumption, a 1.15AHr alkaline battery would last 1.15AHr / 100uA = 11,500 hours, or approximately 16 months. For large commercial buildings or homes with potentially hundreds of RF devices, the recurring cost of batteries and their replacement would be exorbitant.

Consider the System, Not Just the Radio

Control networks comprise many elements that are just as important as the communication medium. Together, these elements determine how easy a system will be to install, update, maintain, and support. RF mesh technology suppliers make many claims about the suitability of their products for a wide range of control applications. A short list of these claims includes:

- Field-proven technology: None of the RF mesh technology suppliers have fielded millions of units. Indeed, none have even fielded the hundreds of thousands of units needed to statistically validate claims about reliable operation in a wide range of applications. The poor performance results observed in our testing (see Figure 2 for an example) may, in part, be attributed to the lack of understanding of real-world operating environments.

- Open standards: None of the protocols used by the RF mesh technologies has been adopted as an open standard. ZigBee claims to be based on an IEEE standard, but the protocol is proprietary and only the physical layer radio is an IEEE 802.15.4 standard. Why is this relevant? Since ZigBee devices from different vendors don't use an open-standard protocol to share and comprehend messages sent over the network, the door is open to non-interoperable, incompatible derivations of the ZigBee protocol. All of these proprietary implementations of ZigBee will be marketed under the ZigBee umbrella; end users who rightfully expect that all ZigBee devices interoperate will have a rude awakening when they realize they actually purchased a sole-sourced proprietary product.

- Fault tolerance: Mesh networking is claimed to offer fault tolerance, as RF signals can be repeated by multiple devices throughout the mesh. However, ZWave, Millennial Net, and many other RF mesh networks depend on a controller within the network to coordinate the mesh repeaters. This controller must be functional for the mesh to operate correctly; if the controller fails, the mesh degrades or fails completely (see ZWave comparison below). The dependence of these RF mesh networks on one controller makes them susceptible to a single point of failure, and represents a major flaw in the system architecture.

To illustrate the need to consider the system as a whole, Table 1 includes a list of critical items that we believe a control network must demonstrate. In the next two columns we compare a power line-based solution from Echelon with ZWave RF mesh technology, using a commercially available ZWave system that we purchased as the basis for comparison.

There are striking differences between the Echelon and ZWave solutions, many of which have significant ramifications with respect to features, warranty costs, and the need for ongoing support. A field test (see Figure 2) validates our claims with respect to the poor field performance of the ZWave RF technology.

Table 1. Echelon Power Line vs. ZWave® Radio Frequency

Subject	ECHELON PL	ZWave RF
Field Proven *Consequence*	**Yes — >24 million PL devices installed** No field surprises.	**No — limited number of devices fielded** Unknown performance.
Open Standard Protocol *Consequence*	**Yes** ANSI/CEA 709 EN 14908 IEEE 1473L SEMI E54.16 AAR US KS Korea Multiple sources of supply, validated technology.	**No** ZWave is proprietary and has not been adopted by any internationally recognized standards bodies. Sole-sourced technology, non-validated technology.
One Solution for Domestic and International Markets *Consequence*	**Yes** PL solution is legal worldwide using C-Band CEN mode. Fewer production variations.	**No** Requires different frequencies for N. America, Europe, and Japan. More production variations.
Reliability *Consequence*	**>99.7% successful messaging observed** Range <u>not</u> affected by metal foil insulation, metal foil wall paper, metal lathe plaster, reinforced concrete/ masonry, cordless headsets, wireless speak expanders. Useful for any application anywhere within a home. Few returns, high customer satisfaction and loyalty.	**<50% successful messaging observed** Range <u>is</u> affected by metal foil insulation, metal foil wall paper, metal lathe plaster, reinforced concrete/ masonry, cordless headsets, wireless speak expanders. Useful only for very short range applications where reliability is not critical. More returns, high warranty costs, low satisfaction.
Robustness *Consequence*	**Very high** Plug-and-play in 5,000-square-foot homes without phase couplers, repeaters, or bridges. Low support costs	**Low** Not plug-and-play even in 2,700-square-foot homes. Requires repeaters — 100' maximum range claimed, but observed range was substantially less, depending on building material and interference sources. High support costs
Repeaters *Consequence*	**Not required** Simpler, lower-cost systems. No batteries to replace.	**Required — must be AC-powered or battery life will be very short** Complex system set-up.

Subject	Echelon PL	ZWave RF
Fault Tolerance *Consequence*	**Very high** Devices may be removed and changed with no adverse system effects. Each device operates autonomously and makes its own decisions. A controller-based design may be used but is not recommended. Peer-to-peer networking doesn't depend on a central controller. Low support costs.	**Low** Removing a node causes an All On/All Off command to lock up the system for >2 minutes due to the missing ACK. In some ZWave devices, changing a setting requires erasing a device and starting over. Controller-based architecture — if the battery fails in a controller, the system won't work. High support costs.
Scalability *Consequence*	**Extensive** The protocol is fully featured and can manage any control application: lighting, appliances, HVAC, security, fire, energy, sun blinds, weather station, A/V, multi-room IR repeating, and irrigation. Many applications using the same products and technology.	**Minimal** The lightweight protocol is constrained to simple on/off/dimming applications. Extra-cost microprocessor required for all but the simplest tasks. Limited applications.
In-Home Performance *Consequence*	**Plug-and-Play** Trouble-free operation.	**Highly unreliable signaling (see results in Figure 2)** High warranty and service costs.
Self-installation without Tools *Consequence*	**Yes** The LonTalk protocol and Neuron core allow automagic self-installation without using any additional tool/display, should this be desired. Echelon supports plug-and-play, plug-press-and-play, and preconfigured systems.	**No** The protocol is too lightweight and the processor too limited in processing power to support self-installation. An installation tool/ display is required. Systems require installation tool.
Interoperability *Consequence*	**Yes** Messages can be shared interoperably using LonMark objects (hundreds have been defined).	**No** Device classes must be created. Only about 40 classes exist today. Each class consumes device memory. Users cannot define their own message classes.
Multiple Media Support *Consequence*	**Yes** PL, twisted pair, RF, IR, and coaxial cable may be mixed and matched as desired and required.	**No** RF only. If the environment is not RF-friendly, costly repeaters will be required and the system may not work at all.

RX Location	TX Location	Distance	900MHz Phone	Light function	Remote Ack
RX1	TX2	68ft	Off	No (0/10)	No (0/10)
“	TX3	60ft	“	Yes (10/10)	Yes (10/10)
“	TX4	56ft	“	No (1/10)	No (1/10)
RX2	TX5	33ft	“	Yes (10/10)	Yes (9/10)
“	TX6	30ft	“	Yes (10/10)	Yes (10/10)
“	TX7	41ft	“	No (0/10)	No (0/10)
“	TX8	37ft	“	No (0/10)	No (0/10)
“	TX4	48ft	“	No (5/10)	No (5/10)
“	TX9	58ft	“	No (0/10)	No (0/10)
RX3	TX7	45ft	“	No (0/10)	No (0/10)
“	TX8	37ft	“	No (4/10)	No (4/10)
RX1	TX1	22ft	On, 3ft from TX	Yes (10/10)	Yes (10/10)
“	TX3	60ft	On, 4ft from TX	No (0/10)	No (0/10)
RX2	TX5	33ft	On, 3ft from RX	No (0/10)	No (0/10)
“	TX5	33ft	On, 6ft from RX	Yes (10/10)	Yes (10/10)
“	TX6	30ft	On, 6ft from RX	Yes (10/10)	Yes (10/10)
“	TX1	37ft	On, 6ft from RX	No (1/10)	No (1/10)

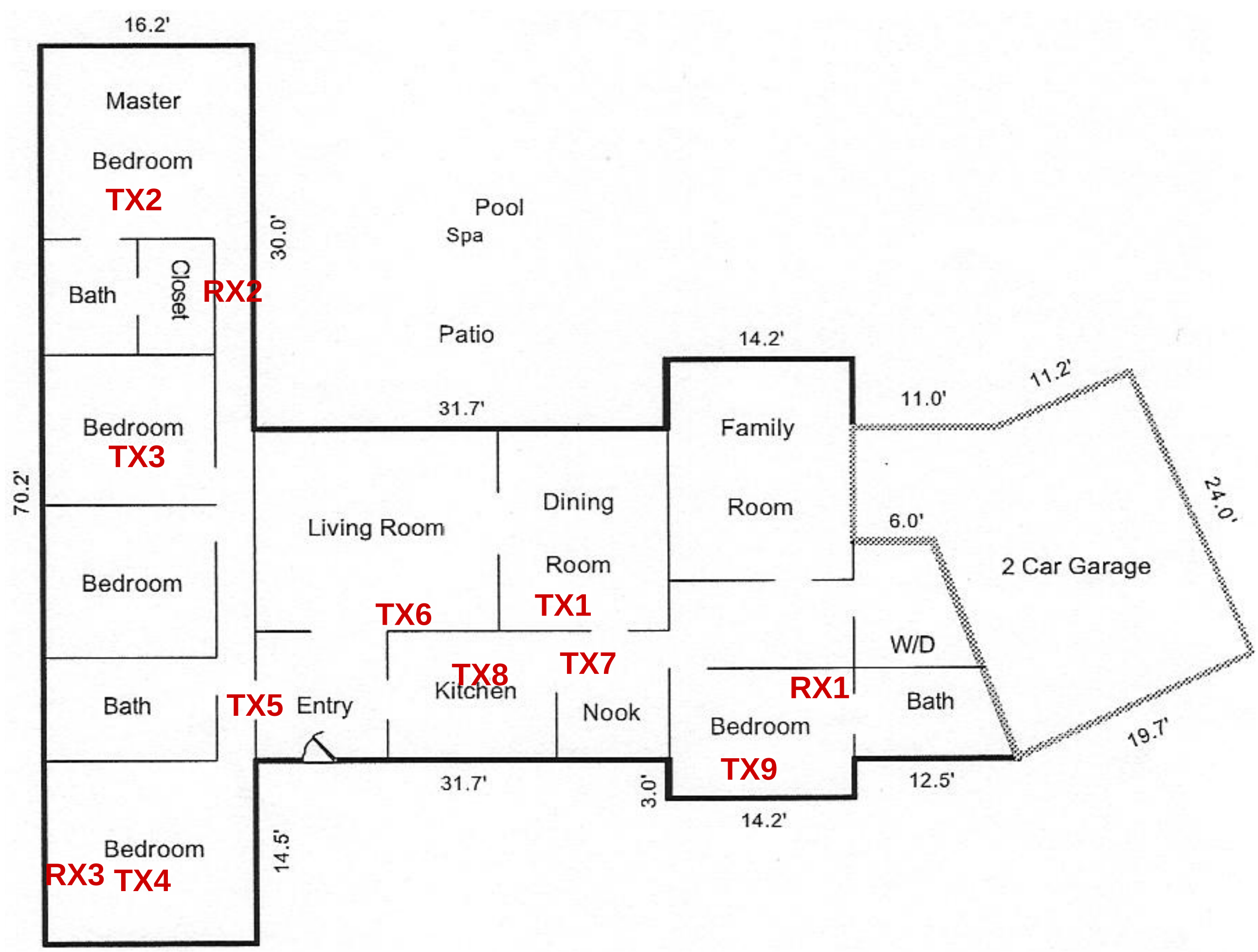

Figure 2. Home Test with ZWave System
Unreliable Communications Traced to Metal Lathe-Backed Stucco and Portable Phone
(Making TX5 a Repeater Did Not Rectify Communication Issues)

What Can Designers Do?

The current limitations of RF mesh technology should raise tremendous concern among designers who are considering using it for their control systems. Adopting this immature technology poses critically high risks to company reputations, life cycle costs, and warranty exposure.

So what can designers do? The first step is to carefully evaluate real-world communication range, battery life, and life cycle costs in a statistically meaningful number of typical installations. Demonstrating a working RF mesh in a development laboratory yields very different results than a trial in situ at hundreds of test sites. The likely outcome, based on our field tests, will be a conclusion that RF mesh is simply not ready for widescale deployment.

Fortunately, there are reliable, cost-competitive alternatives to RF mesh technology. Power line signaling offers a viable alternative for all residential and many building/industrial applications. Most of the control devices in these applications require a connection to electric power, be it AC or DC voltage, making power line signaling an ideal solution.

For new commercial building applications, free topology twisted pair wiring offers proven reliability, no battery replacement issues, and very low maintenance costs. For commercial building retrofit applications, such as overhead and emergency lighting devices, power line is a better and more reliable alternative to RF mesh networking.

Conclusion

We have no doubt that RF technology will improve over time; however, we don’t believe that manufacturers should be test vehicles for unproven technology. RF technology suppliers should continue development until they can produce a robust, field-proven solution on which product manufacturers can rest the good names of their companies. The value of RF technology — if it can be made to work well at low cost — appears clear for a range of battery-powered sensor monitoring applications. The value of mesh networking, on the other hand, has yet to be proven in control applications where its sole purpose today is to compensate for poor-quality radios.

Appendix 1. Media Comparison for Control Networking

Medium	Strengths	Weaknesses
Twisted pair	• Highly reliable • Low cost of materials • Installation can be done by unskilled labor	• Low to moderate installation costs
Power line	• Highly reliable (only true for Echelon PL technology, not true for X10 PL technology) • Low cost of materials • No new wiring required (leverages existing power wiring)	• Some devices may require an electrician to install power connections
Fiber optic	• Highly reliable • Immune to electrical interference	• High cost of materials • Installation costs can be very high and requires skilled technicians
Coaxial cable	• Highly reliable •	• Moderate material costs • Moderate installation costs
Infrared	• No new wiring required • Low cost of materials • Well controlled field of operation	• Short range • Cannot pass through walls or floor • Reliability varies by location and exposure to infrared from other sources (fluorescent lamps, sunlight)
RF	• No new wiring required (except for certain types of repeaters) • Low to moderate cost of materials	• Hard to pass through walls and floors • Installation costs vary by location • Repeaters may be required • Reliability affected by a wide variety of sources, the interference from which may not be obvious (WiFi routers, cordless phones and headsets, consumer products, among others) • Battery replacement in completely unwired devices

Twisted pair technology has long been a mainstay of control networks because of its low cost, ease of use, and very high reliability. Hundreds of manufacturers of twisted pair cables exist, and the wide availability has kept prices low. Cables are manufactured in a wide variety of types for use in environments with extremes of temperature, moisture, pollutants, and electrical noise. New twisted pair technology — called free topology twisted pair (FT) — allows the cabling to be installed regardless of the wire route; wiring can be installed in a bus, star, loop, daisy chain, or any combination thereof — with confidence of essentially perfect transmission reliability.

Power line technology superimposes control signals onto the high- or low-voltage alternating current (AC) or direct current (DC) power circuits that send power to a machine or device. Using this technology, a machine or device can be connected to a control network by simply plugging in a power connection. No new wires are required. New ANSI/CEA 709.2-compliant power line technology employs sophisticated digital signaling processing and error correction algorithms, and can communicate reliably despite the presence of electrically noisy devices operating on the power line.

Fiber optic technology communicates by sending light waves through flexible glass or plastic cabling that conducts light. Fiber optic systems are highly immune to electrical interference since light waves — not electrical waves — carry the signal. For this reason fiber optic systems are highly reliable, and have been popular in environments with very high electromagnetic noise, such as industrial plants. The interconnection of fiber optic cabling requires the use of special tools and fittings, and skill is required to install, troubleshoot, and maintain a fiber optic network.

Coaxial cable technology communicates by sending data through a specially insulated cable that's covered with an electrical shield. This shielding makes coaxial cable systems relatively immune to electrical interference, though not to the same degree as fiber optic cabling. Care must be taken with the interconnection of coaxial cabling, which, like fiber optic cabling, requires the use of special tools and fittings. Skill is also required to install, troubleshoot, and maintain a coaxial cable network.

Infrared technology uses invisible infrared light to carry control signals. The light waves cannot penetrate solid objects like walls and floors, so signal dispersion can be well controlled. In addition, the cost of the technology is low. However, infrared signaling is typically limited to relatively short range because the signal strength is relatively low. Sources of infrared energy, such as sunlight and some fluorescent lamps, can interfere with infrared signaling systems.

RF technology uses radio waves to carry control signals. An advantage of RF signaling is that radio waves propagate widely (depending on the characteristics of the antenna), and depending on the frequency may pass through some building materials. The allowable frequency of the radio signals is determined by each country, although some frequency bands such as the ISM band (2.4GHz) are available for use worldwide. The cost of RF technology has dropped in recent years, especially for short-distance RF transceivers. The downside of RF is that it's hard to penetrate metal building materials; the allowable frequency bands are increasingly crowded and therefore, subject to interference; and the short range of low-cost, bidirectional RF devices requires either multiple receivers or repeaters to propagate a reasonable distance.