

Future of Building Automation

Tom Schmidt
Schmidt Consulting
Revised 21 June 2005
tom@tschmidt.com
<http://www.tschmidt.com>

The advent of low cost wired and wireless network equipment has greatly expanded the small business and residential market. Network components are readily available at commodity prices. Configuration is easier than ever and numerous web sites and consulting services are available to help install and managed them.

The situation is much different in the building automation arena. Few open standards exist and those that do have not been widely adopted, such as EIA [CEBus](#). Someone contemplating an automation project needs to research numerous proprietary implementations. The most robust implementations are wired. Hardwired network are expensive to install especially in retrofit situation and create a rather inflexible design. The most popular wireless (Powerline) standard, X10, is extremely popular but painfully slow, lacks security and has limited addressability.

This paper discusses the emergence of ZigBee and wireless Mesh technology as the next step in building automation. These technologies promise to create extremely powerful sensor control networks at very low cost.

Ideal Building Automation Characteristics

Before looking into specific products and specification it is worthwhile developing a building automation wish list.

Flexibility

Usage patterns change over time, often dramatically. One of the great insights of EIA/TIA 568 structured cabling specification is that infrastructure has a much longer useful life than services that depend on it.

A similar argument can be made about building automation. In this case it is not so much the life expectancy of the devices themselves, as the way they are configured. Wall switches, occupancy sensors, and load controllers have long useful life. However the specific configuration of sensors and loads will likely evolve over time.

Ideally configuration does not need to occur when devices are physically installed. Configuration can occur at any time and be readily changed as needs evolve. A room entry switch or sensor can be reconfigured later to implement functions not envisioned when the sensor was initially installed.

Peer-to-Peer Binding

The relationship between sensor and controlled object are pretty straightforward and persist for long periods of time. This allows static functional binding between devices. A change detected by an occupancy sensor or wall switch is directly communicated to the appropriate load controller. Command and control functions are not dependant on third party application servers to mediate between sensors and loads for basic operation.

Open Specifications

Installing a building automation system is a long-term investment. No one wants to be locked into a single vendor over a decades long useful life. Open standards assure healthy competition and compatibility among multiple players reducing risk of obsolete or orphaned equipment.

Open stands encourage niche players to market specialty devices increasing the likelihood special needs can be met with off the shelf equipment.

Robustness

As more and more building functions are controlled electronically it is imperative they work in ways users expect, address both random and deliberate interference and

withstand the rigors of daily use. Failure of the automation system is almost as severe as power loss, perhaps even rendering the building unusable until the problem is resolved.

Security

Security is an often neglected topic. Automation systems must be able to protect themselves from attack. If an attacker gains unauthorized access to building automation she will be able to compromise building integrity perhaps even jeopardize life and property. The system must be able to determine the trustworthiness of control requests, and reject unauthorized commands. Security engineering is unique in that not only must correct operation be assured but also likely methods of attack anticipated and countermeasures developed.

Networks leak data, the military calls this signals intelligence. The automation design must be such that this leakage is of no value to a potential attacker. For example knowing which rooms are occupied and which entry points are unlocked is potentially valuable information to an attacker. In a wireless system monitoring command codes and device addresses easily discovers this type of information.

Ease of use

All technology goes through predictable evolution toward maturity. Early adopters are willing to invest in learning to exploit new and unproven technology. As technology moves into the mainstream implementation become easier so less up-front investment is needed to profitably exploit it. Today's building automation systems are still at an early stage, the province of specialists. As building automation matures more professionals and amateurs will gain the expertise needed to properly implement it.

Price

As with any market price point is driven by value and cost. So far building automation is limited to specific functions implemented on an as needed basis. The notion of networking everything and sharing information between multiple sensors is still an immature dream. Reducing system cost will greatly expand the market for building automation systems. Resulting in a virtuous cycle of expanded use made possible by low cost.

Energy efficient

As building automation becomes more ubiquitous energy consumption of the system become more important. The automation system represents a parasitic energy load placing great value on maximizing functionality while reducing energy consumption of the automation system itself.

Support

As building automation becomes ubiquitous business opportunity will expand to design and install them and provide ongoing support. Regardless of how user friendly these systems become there will always be opportunities for experts to install and manage them.

Wireless

Building automation systems are characterized by a large number of sensors and controlled objects distributed in three-dimensional space. Data throughput requirements are modest but guaranteed delivery is essential. Wireless is ideal because it eliminates the expense of hardwiring myriad devices. Until recently silicon cost to put a digital radio in every device was prohibitive. Advances in IC technology have dramatically reduced cost making radio based networks very attractive.

ZigBee Advantage

New wireless command and control technologies such as [ZigBee IEEE 802.15](#) are well suited to automation systems. The radios are optimized for reliable short burst low latency traffic. ZigBee radios have very low power consumption making them ideal for battery powered wireless sensors. Battery life in years is possible.

Radio based networks dramatically reduce cost, especially in retrofit situations.

Using a radio-based system eliminates the functional distinction between fixed location and portable devices. This minimizes development cost and maximizes reusability. The same basic radio and firmware can be used in a fixed location light switch and hand held A/V remote control.

Mesh Networks to the Rescue

Wireless is not without its downside. The transmission medium is hostile and devices share a finite RF spectrum. Reliability and range can be improved by increasing transmit power at the expense of battery life and mutual interference.

Mesh technology neatly addresses both issues at the cost of increased device complexity. In a mesh network devices no longer need to directly “see” one another, they only need to “see” a local neighbor. Intermediate nodes act as routers forwarding incoming messages toward the intended recipient. Two startups [Ember](#) and [Millennial Net](#) are developing products exploiting Mesh technology. Mesh sensor technology was developed at the famed MIT Media Labs and is now considered the optimum solution to implement wireless sensor networks.

Effective communication requires local device pairs be able to “see” each other. This dramatically reduces transmission power and allows spatial channel reuse. Mesh

networks greatly improve overall reliability while reducing power consumption, a critical resource for battery-powered devices. Device pairs at distant ends of the network are able to reuse channels without causing mutual interference. This allows Mesh throughput to greatly exceed the channel capacity of the radio itself. This is analogous to the advantage of replacing Ethernet Hubs with Switches.

Building a network from a large number of devices makes it easy to provide location aware services. Multiple devices near the sender “hear” it directly allowing the sender’s location to be triangulated. Location awareness is very useful for everything from E911 emergency service to room aware remote controls to “where am I” functions.

Mesh to IP Networking

As powerful as Mesh based sensor networks are interconnecting them to traditional computer networks takes advantage of [Metcalf’s law](#). The law states the value of a network device increases in proportion to the number of devices connected to it. While most transactions originate from relatively simple sensors bound to specific load controllers there is much to gain by using the rich user interface and power of traditional computers to implement complex control schemes and user interfaces that interact with Mesh devices.

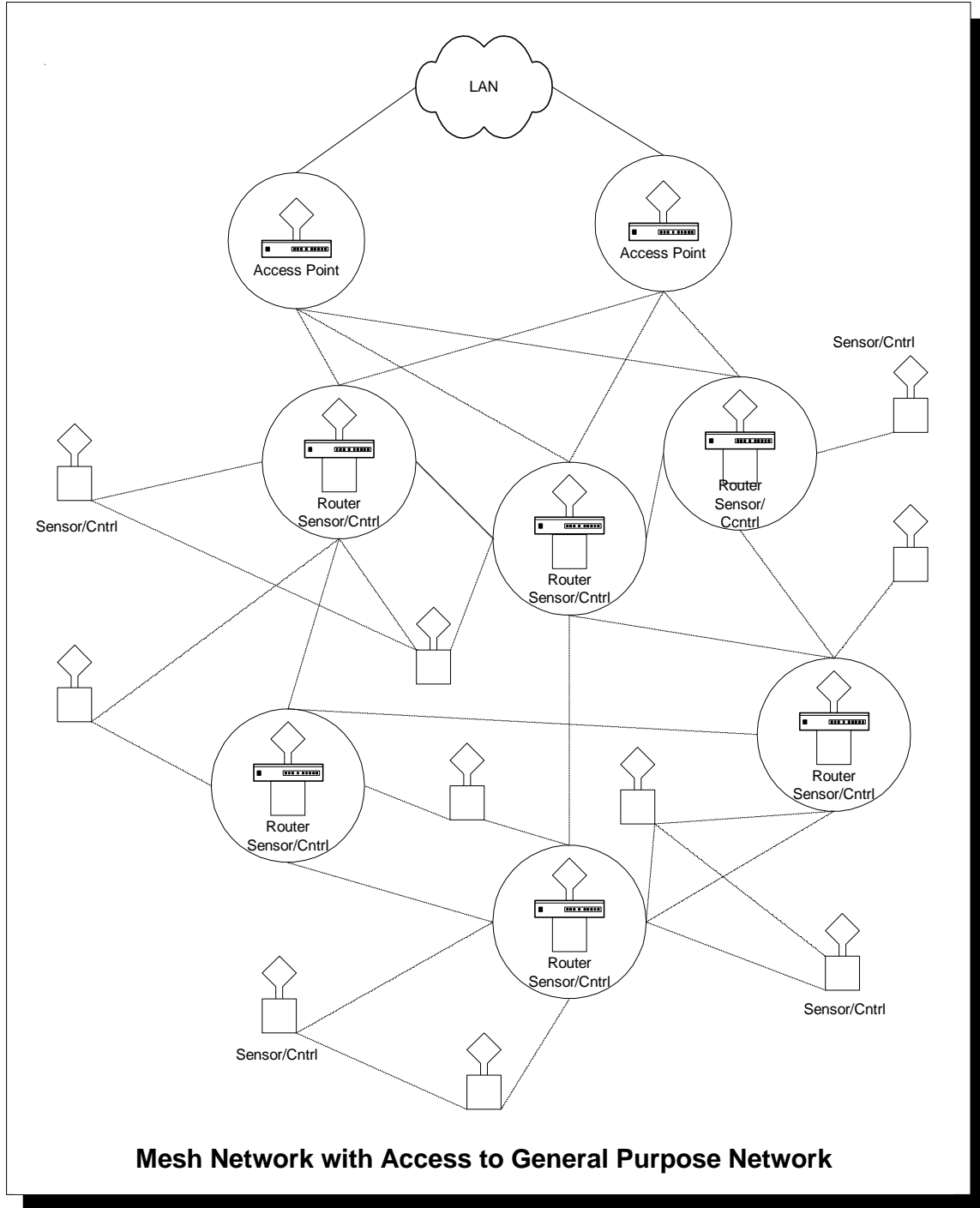
The rich GUI and powerful processing capability of general purposes computers allow post processing of sensor data to create complex control schemes not possible with directly connected devices. The computer obtains data from many sources and outputs complex commands. Features such as scene lighting, smart power management, occupancy and intrusion detections are typical of tasks best performed by a computer acting as an application server. Supervision functions that look for unusual activity across many sensors are more effectively then trying to obtain this information from a single sensor.

Interconnecting the Mesh network to general-purpose network makes it easy to gain remote access to the automation network using existing Internet secure remote access protocols such as SSL and IPsec VPNs. Security is critical to prevent an attacker from hijacking the automation system for nefarious purposes.

A hybrid approach provides the best of both worlds. For many functions the command and control Mesh network operates autonomously once it is configured. Basic operation is not dependant on availability of external network or computers. Where such connection exists richer functionality is possible. Interconnection requires use of an application level gateway (ALG) to mediate between networks and insure remote requests are authorized to perform the specific task.

Future Building Automation Network

The drawing below shows typical Mesh network consisting of sensor/control devices, wireless Mesh routers and Access Point linking Mesh to IP data network.



Wireless Mesh networks consist of three device classes: endpoints, routers and Access Points. Endpoints are limited functionality, often battery powered. Endpoints are able to transmit or receive messages, but do not forward external messages to other endpoints. Full function devices have all the capability of Endpoints in addition they act as routers forwarding incoming messages to the ultimate destination or the next router nearer the desired endpoint.

Access Points interconnect Mesh devices to the local IP network. Access Points allow browser based PCs to observe and control Mesh based devices. Either residing within the Access Point or elsewhere on the LAN an ALG interfaces Mesh to general purpose IP network.

Conclusion

Wireless Mesh technology promise to make building automation as common as traditional computer networks. In a few years one will be able to go down to the local Home Depot and pick up sensors and controlled devices, and quickly install and configure them. The next few years will be exciting as wireless Mesh technology revolutionizes building automation and security.