Evaluating Communication Options for Fire Alarm Monitoring in Commercial Buildings

Carl Weisman, MS, MBA

June 2018

Abstract

This whitepaper evaluates and compares the communication options for relaying fire alarm signals from commercial buildings back to the central monitoring station. Specifically, we investigate how public switched telephone network (PSTN), cellular/IP and wireless mesh technologies compare in regard to reliability, performance, total cost of ownership (TCO) and obsolescence. We come to the conclusion that when everything is considered, **Wireless Mesh Technology** offers the best option for fire alarm monitoring communications in commercial buildings.

Background/Introduction

Commercial buildings cannot get a certificate of occupancy until they have a fire alarm monitoring communications system in place. This is the system that monitors the building for fire alarms, and when an alarm is detected, relays that information to the central monitoring station.

When it comes to fire alarm monitoring communications, property builders, owners and managers are faced with one of three choices: PSTN, cellular/IP or wireless mesh. Each of these technologies has their advantages and drawbacks. In this whitepaper we consider all three, with specific attention paid to wireless mesh networks, as they are less familiar in the commercial building industry.

How the Systems Work

PSTN for fire alarm monitoring communication uses the plain old telephone system (POTS). The signal is transmitted from the building over copper or fiber optic cable to the nearest public telephone switching station. From there it traverses the phone network to the central monitoring station.

Cellular/IP uses local cellular service to relay the fire alarm signal wirelessly from the building to the nearest cellular tower. From there the signal is relayed to an internet gateway either via point-to-point microwave or over fiber optic cable. Once on the internet, the signal gets routed to the central monitoring station via IP protocol.

In wireless mesh networks, a collection of wireless routers is used to provide network access to wireless clients deployed in commercial buildings. Multiple mesh routers within the network serve as gateways to the central monitoring station.

Mesh networks work similarly to the way the internet works, in which internet routers use multiple hops to send information from one point to another. The only difference with mesh networks is that the signals are routed wirelessly, rather than over fiber optic cables.

Just like internet routers, wireless mesh routers have multiple paths to choose from to get the information to the end destination. They dynamically adopt to changing environments and essentially self-heal in case of a node or link failure. If one mesh router becomes obstructed or otherwise unavailable, traffic is automatically redirected via an alternative path.

Obsolescence

Both PSTN and cellular/IP expose users to technology migration and obsolescence risk. In just over 20 years, cellular technology has evolved from analog to digital to 2G, 3G, 4G and now 5G. With each technological leap, customers are expected to invest in the latest technology, even if they don't need it. And common carriers would like to do away with PSTN altogether and convert their customers over to cellular, where monthly fees are higher and adding new users is easier.

In contrast, wireless mesh users do not have to deal with forced technology migrations or obsolescence. The mesh router they deploy will work fine, as is, for the foreseeable future.

Total Cost of Ownership

One of the unique aspects of using a wireless mesh network for alarm transmission is that in doing so the user becomes part of the network service provider. Users become members of a network, with every member's router contributing to network communications. This cooperative nature of the network gives participants more control over the network, and more importantly, it lowers their cost.

Both PSTN and cellular/IP come with high monthly line or connections fees. Consequently both are also exposed to the inevitable rate and/or tax increases. This is in contrast to wireless mesh, where users avoid paying any monthly service charge for communication services.

A major benefit of using wireless mesh for alarm communication is that it dramatically lowers the total cost of ownership (TCO).

Reliability of the Systems

When it comes to system reliability, both PSTN and cellular/IP suffer from the same vulnerability: single point of failure. In the cellular/IP system, if any part of the communication chain (cellular base station, backhaul link, gateway or internet service provider) goes down, the communication link is broken and there is no work around. The same holds true for PSTN systems.

It is not uncommon for a backhoe to accidently cut a buried fiber cable or have an animal chew through local phone lines. When that happens, it can be hours or days before service is restored.

When it comes to reliability, wireless mesh networks have a benefit that is unmatched by either of the other communications technologies: path redundancy plus gateway redundancy.

With path redundancy, wireless mesh networks can survive a mesh router going down. The system simply reroutes the signal around the downed unit. The real unmatched benefit of wireless mesh networks though is gateway redundancy. Within the mesh network, there are multiple gateways connected to the central monitoring station. In the event one of the gateways goes down, the system reroutes the signal to another gateway.

The bottom line is there is no single point of failure anywhere in a wireless mesh network.

Performance of the Systems

When it comes to speed, both PSTN and cellular/IP have minimum dial times on the order of 45 seconds, which is relatively slow for emergency communications. In contrast, since there is no dialing required—wireless mesh networks are always on—network traversal times are on the order of 1 to 3 seconds.

In addition, since they use public networks in which public safety communications must share the available bandwidth with general voice traffic, both PSTN and cellular/IP can suffer from network congestion problems during times of heavy usage (e.g., during a natural disaster). This could adversely impact response times when fast replies are needed most.

In the event of a natural disaster, wireless mesh networks especially outperform PSTN and cellular/IP. With battery backup, a wireless mesh network will continue to work in excess of 24 hours even in a total blackout.

Conclusion

In this whitepaper, we have compared PSTN, cellular/IP and wireless mesh as a communications medium for relaying fire alarm signals from commercial buildings to central monitoring stations. The results are summarized in the table.

	PSTN	Cellular/IP	Wireless Mesh
Reliability	Single point of failure	Single point of failure	No single point of failure
Speed	45 second dial time	45 second dial time	1-3 second access time
Communication Fees	Monthly fees	Monthly fees	No monthly fees
Obsolescence	Yes	Technology migration	None

For property builders, owners and managers faced with the decision of which technology to use for fire alarm mounting communication, the choice is clear: **Wireless Mesh Technology** is the smart business decision.

About the Author

Carl Weisman is the author of *The Essential Guide to RF & Wireless* (Prentice-Hall), a standard text in the industry for over a decade. He has spoken at numerous industry events and has published articles in many industry magazines. He received his masters degrees in engineering from USC and his MBA in finance from Loyola Marymount University.