MILLENNIUM
SECURE YOUR WORLD

April 26, 2017

Introduction to Wireless Locks

You can't have an access control system conversation for more than a few minutes these days without someone bringing up the topic of wireless locks. While this sounds like an ideal solution for a range of challenging use cases, the number of options can quickly become daunting for even the most seasoned access control professional! Thankfully, while there are many minor differences in the approach to wireless locks across different manufacturers and product ranges there are three basic approaches to "cutting the cord" to the door. Before exploring the technical details of each of these approaches, it is important to discuss those use cases where wireless makes sense and the instances where wireless may not be the best possible solution.

Wireless locks are increasingly part of the overall access control solution for many applications

When to Consider Wireless as an Option

The first and most critical variable to evaluate when considering the wireless option is the frequency of door access. Because wireless locks are virtually always battery powered, doors that have a very high access frequency such as primary entry doors are often not good candidates due to unacceptably short battery replacement intervals driven by the number of unlock/lock cycles. Conversely doors that are less frequently accessed like interior office doors, conference room doors, equipment closets and the like can be great candidates. Further factors that can increase the attractiveness of the wireless option include;

- Affordably adding doors to existing systems without incurring retrofit wiring costs
- Creating greater connected door density in new installations where wiring costs represent a barrier to the number of managed doors
- Adding access control to unique or historically significant buildings where disruption to the structure to install conventional wired access control is not permitted
- Adding managed access control to auxiliary doors such as outside storage, fence gate, and other cases where it would be prohibitively expensive to install the wire and conduit necessary for conventional access control

In short, any door with a moderate access rate and where it would be difficult or prohibitively expensive to provide power and data cabling is potentially a good candidate for the wireless option! However, it is important to consider the various technical solutions and select the option that best aligns with the needs of a specific use case.

While there is tremendous variability in the technical implementation, features and functionality across the commercially available solutions, there are three basic technical approaches to data transmission between wireless locks and the access control platform;

Credential Based Data Transmission

For this method of wireless access control, the physical hardware on the door is not directly connected to any central server, but rather access privileges are maintained and communicated via the credential. In this case, the actual media used for the credential can be any common format including Magnetic Strip, RFID, or increasingly smartphone based credentials. Logging is performed at the door level, and requires a specific tool and a visit to the door to retrieve information local to the lock.   Common examples of this approach include **Assa Abloy VingCard** and the **Kaba SafeLok** product offerings when the optional RF communication option is not included in the installation

One interesting derivative of the disconnected lock model is the **Salto Virtual Network (SVN) System**. In simple terms, this system effectively uses the credentials to communicate between the individual locks and the application server. When a user accesses a door, their credential will update the access tables and schedules for that specific door, and download log, battery life and other information back to the card or token. A small number of access points are hardwired back to the central server to create the data path between the access control server and the lock infrastructure.

The Salto Virtual Network Solution uses the credential in a manner equivalent to a USB drive reading and writing data to the lock during each access

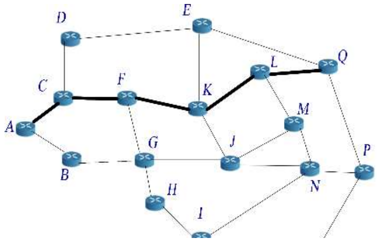
The disconnected lock model has the two key advantages. First, because there is no actual radio in the lock battery life can be longer than other solutions that have to power both the core lock function but also the communication electronics. The second advantage is that no additional hardware or associated design constraints related to radio frequency ranges are required. The primary disadvantage of this approach is the very limited ability to send or retrieve information from the lock.

Wireless Low Power Network Based Access Control

For this style of access control, the door hardware includes low power radios typically based on network protocols specifically designed for low power and relatively low bandwidth communication. The communication protocols most commonly used for this approach include Zigbee, Z-Wave and variants of 900 Mhz wireless protocol . Zigbee and Z-Wave are very common protocols that work on very low power because each node (or in this case lock) is both a transmitter and a receiver, which allows data to "hop" from door to door until it reaches a network node that is hard wired. This is known as a "mesh" network due to the many possible pathways between each device on the network.

The Radio Frequency option for **Assa Abloy VingCard** utilizes this approach as does the **Kaba LENS™** enhancemnt for their lodging solution. Another option in the low powered radio category uses (typically) 900 Mhz spectrum and point to point communication with a Panel Interface Module (PIM). The **Allgeion AD-400** series of locks works using the 900 Mhz protocol which works very much like, and on the same spectrum as cordless phones and baby monitors.

The advantage of this approach is that the low power radios combined with the multiple paths of the mesh network allow for long battery life and significant network resilience. However, these systems typically require additional hardware in the form of a wired node every 100 to 200 ft to provide a data path back to the access control server.



Mesh networks provide multiple pathways to a hardwired node on the network, allowing for improved resilience and battery life

Wi-Fi Based Locks

Wi-Fi based locks take advantage of the fact that nearly every building already includes a Wi-Fi network due to the prevalence of laptops, smartphones and other devices that rely on this communication protocol for connectivity. These locks communicate using the same wireless gateway as these other devices, but because Wi-Fi is a relatively power intensive communication protocol these locks don't communicate constantly, but rather will "phone home" at pre-configured intervals to upload and download any changes in onboard access tables or status.

The **Assa Abloy IN120** series of locks use this approach to communicate with the central access control server. The advantage of this approach is no additional network equipment is required presuming the facility is already equipped with Wi-Fi for its occupants. However, these locks typically require consideration of the frequency of communication relative to battery replacement intervals. For example, setting the locks to update themselves one a day (every 24 hours) versus every 4 times per day (every 6 hours) can result in a 10% or more increase in battery life. Although Wi-Fi locks do have higher power requirements than other options due to the nature of the network protocol, the high level of flexibility in defining communication intervals generally allows for at least a 1 year battery life for typical use cases.

Wi-Fi locks share the same wireless network infrastructure as laptops and Wi-Fi connected smartphones

The advantage of this approach is that presuming the availability of a conventional Wi-Fi network, no additional infrastructure or design effort is required. The disadvantage is that the higher power demands for communication may, depending upon configuration result in shorter battery life compared to other options.

Conclusion

The various technical approaches to wireless locks provide great flexibility to the access control professional in tailoring a specific solution to the needs of his or her client. However, there is one use case where all currently available options represent a poor choice, and that is the case where immediate and dependable lockdown capabilities are required. An important difference between conventional wired and wireless locks is that wireless locks are never "always on and connected" so use cases such as lock down that require immediate access are generally not a good fit for wireless.

Wireless locks are a great opportunity for access control professionals, but a thorough understanding of the technical approach, features, benefits and tradeoffs of the current options on the market will ensure that you can make the best recommendation for your customer.

Millennium Group Inc. is a growing provider of reliable, highly scaleable state of the art building access control solutions. With a legacy stretching back more than 50 years as a premier supplier of high quality access control to organizations of all sizes, we focus on partnerships with factory trained and certified system integrators to ensure that every system is carefully tailored to meet the unique needs of building owners. Whether you have one door or thousands of doors across multiple campuses, Millennium has a solution for you.