Technical Article

Smart Wi-Fi® Locks Will Soon Open Many Doors

Benjamin Moore

Intelligence can take you a long way in the world. But in many cases, it's one of your networking connections that will get you where you want to go. Such is the case with smart electronic locks (e-locks). Because of TI's recent innovations in low-power Wi-Fi® and the advantages of a direct connection to the cloud, a new generation of Wi-Fi-enabled e-locks will soon open plenty of doors.

In the not-so-distant future, forgetting to lock the front door won't trigger a frantic race back home to lock it. Consumers will be able to lock or unlock an e-lock with Wi-Fi connectivity from their smartphone. Or, instead of leaving a key under the doormat, they can simply open the door for the plumber anywhere at any time. They will also enjoy faster software updates thanks to the higher throughput of Wi-Fi.

Breaking Down the Power Barrier

Most e-locks were initially based on peer-to-peer wireless connectivity protocols such as *Bluetooth*® or radio-frequency identification (RFID), which grant access to a door from a handheld device or ID card. However, these protocols cannot connect directly to the internet or the cloud without going through an intermediary device like a smartphone or a bridge plugged into the home's electrical supply. In contrast, an e-lock with Wi-Fi connectivity has direct connectivity to the cloud through the home's Wi-Fi access point.

Previously, the higher power consumption of some Wi-Fi connectivity technologies had restricted the wireless connectivity in e-locks to low-energy protocols like Bluetooth low energy and Sub-1 GHz. Now, SimpleLink™ Wi-Fi wireless microcontrollers (MCUs) or network processors have broken through the power barrier such that an entire Wi-Fi and Bluetooth low energy e-lock can operate for almost four years on four AA batteries. Driving down power consumption and providing a Wi-Fi radio and MCU on a single chip to run the application code allows e-lock providers to drastically reduce costs and design complexity.

Figure 1 demonstrates how the Wi-Fi-enabled door lock in a home can connect directly to the cloud, all while being controlled by your mobile device.

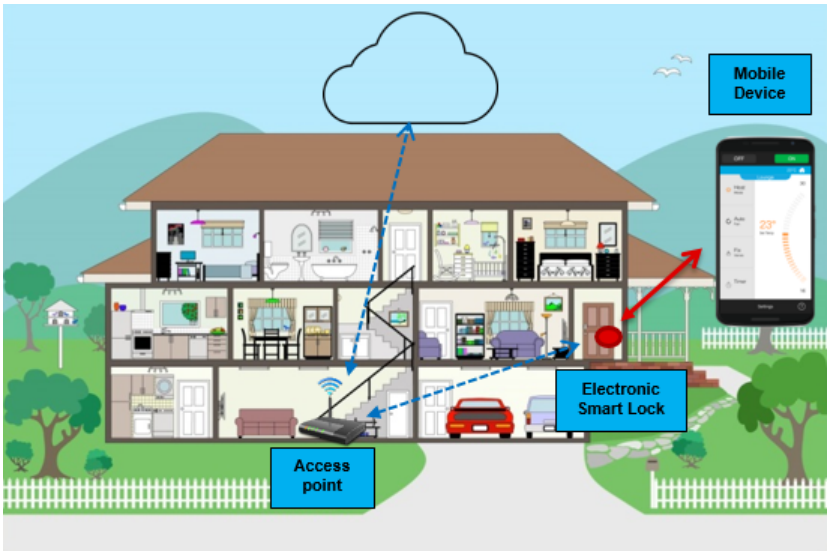

Figure 1. Smart Lock Connection to the Cloud and Smartphone

Lowering Power

TI optimized the SimpleLink™ Wi-Fi CC3120 wireless network processor and CC3220 wireless MCU for low power. When intermittently connected to the access point – meaning that they must first wake upon a sensor or button trigger before operating – the CC3220 device consumes as little as 4.5 µA (microamps). That level of low power consumption is what enables battery life of almost four years.

An additional power-saving capability of CC3120/CC3220 devices is their fast wake-up cycle. For example, when used in intermittently connected mode, these devices can wake up and connect securely to a local Wi-Fi access point in less than 310ms and to a server in less than 200ms with the help of the hardware cryptography engines. As a result, SimpleLink Wi-Fi wireless devices can remain in low-power mode as long as possible and still respond when needed.

In always-connected mode – meaning that the network connection or “sockets” are maintained at all times – the battery life will still be 1.5 years. Remaining always connected to the access point provides on-demand access without compromising battery life, enabled by a low-power deep-sleep mode, automatic use of Institute of Electrical and Electronics Engineers (IEEE) 802.11 Power Save and user-defined sleep intervals. With the ability to dynamically choose between intermittent and always-connected modes, it is possible to enjoy the best of both worlds.

Frequently, a good portion of the power consumed by a Wi-Fi connectivity device is dictated by the behavior of the access point to which it connects. The SimpleLink Wi-Fi wireless MCU’s network learning algorithm observes the behavior of the access point and network path and adjusts its power modes accordingly, reducing power consumption significantly.

Enabling Security

How protected would a home be if the e-lock on the front door was not as secure as possible? CC3120/ CC3220 devices help defend against malicious over-the-air (OTA) attacks with a full suite of security safeguards, including on-chip encryption engines, Wi-Fi security protocols and a built-in trusted root-certificate catalog. The CC3220 device’s MCU core and its Wi-Fi connectivity radio are encapsulated in completely separate on-chip environments to further protect against theft of intellectual property (IP) through the Wi-Fi port.

This high level of security is essential for OTA updates of an e-lock’s firmware. Physical access to the lock is not necessary for such updates and the encrypted IP transmitted to each e-lock remains safeguarded. Plus, SimpleLink Wi-Fi devices incorporate fail-safe files and bundle protection to maintain system integrity during an OTA update. Ending up with a bricked smart lock after an OTA update is no longer an issue because protected files are all saved at the same time, after verification that the system works correctly.

CC3120 and CC3220S/SF devices also simplify protection of the e-lock firmware, access keys and data stored on the system. An integrated, unique device ID encrypts the file system and prevents the e-lock from being cloned or its files from being read by another device. You can further protect individual files through encryption, authentication and access tokens to help prevent any compromise of a user’s account or lock even if attacked.

Simple, Interoperable Wi-Fi

The Wi-Fi Alliance has already certified SimpleLink Wi-Fi devices, and this certification is transferrable from TI to you. The CC3220 device is also offered in a self-contained, ready-to-go Wi-Fi connectivity drop-in module. Therefore, you need not be an expert in Wi-Fi technology to quickly add Wi-Fi connectivity to your e-lock.

Once it’s in the marketplace, TI’s extensive interoperability testing procedures ensure that an e-lock will work seamlessly with practically any Wi-Fi access point. SimpleLink devices are tested for interoperability against more than 225 Wi-Fi access points from manufacturers around the globe, ensuring low power everywhere.

Now that you've learned why utilizing Wi-Fi can be a great solution for your connected project, see below in Figure 2 for a diagram on how to build your own smart door lock.

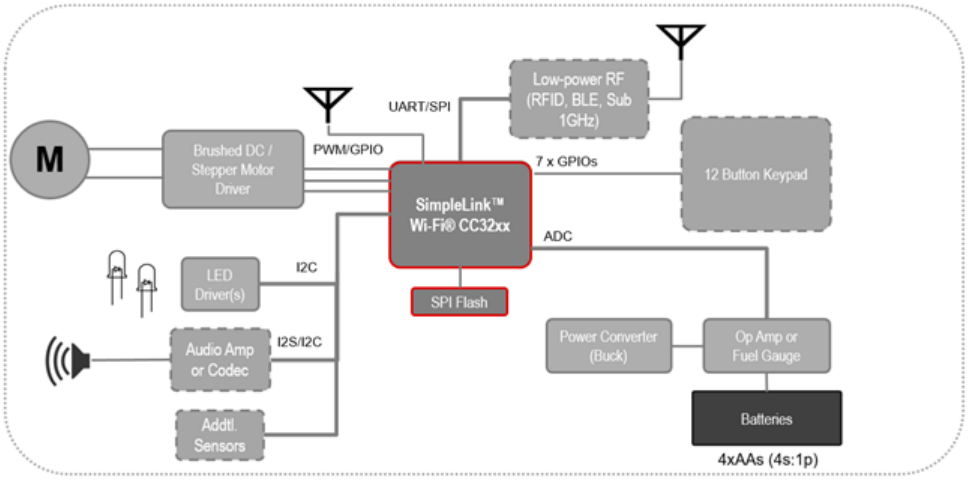

Figure 2. Smart Lock Diagram with SimpleLink Wi-Fi CC3220 Wireless Microcontroller

Additional Resources

- Get more information on Wi-Fi e-locks from this application report, "SimpleLink™ Wi-Fi® Enabled Electronic Smart Lock."
- Read the application report, "SimpleLink CC3120, CC3220 Wi-Fi Internet-on-a-Chip Networking Subsystem Power Management."
- The blog post, "Embrace IoT living through the gateway of electronic door locks," includes a comprehensive list of resources on how to build your own e-lock.
- Find more TI integrated circuits used in electronic smart lock designs.
- Learn more about the SimpleLink Wi-Fi family.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265