SmartMesh Embedded Wireless Mesh Networks Enable Sensors to be Placed "Anywhere"

By Ross Yu, Product Marketing Manager, Dust Networks Product Group, Linear Technology Corp.

Whether on the surface of a city street to sense available parking spots, or in industrial hazardous locations, the demand for sensor information has never been higher, and new applications require sensors to be placed in locations that were previously thought to be impractical. In order to place a sensor anywhere data needs to be collected, sensors must be truly wireless—both for communications and power. Since sensors need to be placed optimally for data collection, and not necessarily optimally for RF communications, the devices must be able to communicate both reliably and securely if wireless sensor networks are to continue to gain acceptance and to be used ubiquitously.

SmartMesh embedded wireless mesh sensor networks, from Linear Technology's Dust Networks product line are successfully deployed by end users in some of the toughest RF environments, including industrial process plants[1], data centers[2], smart parking applications[3], railcars, and mining (Figure 1).

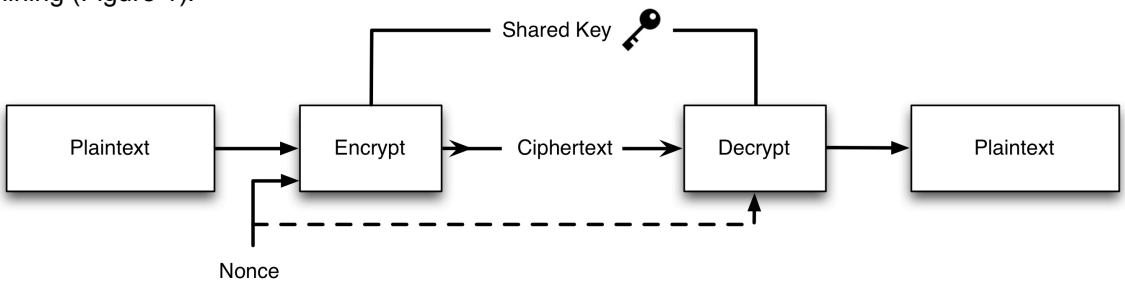

Figure 1: Streetline has deployed SmartMesh wireless mesh networks from Linear Technology's Dust Networks product line to improve parking in such cities as Hollywood, CA

Built on the Linear's ultralow power, LTC5800 802.15.4 System-on-Chip, SmartMesh networks are embedded systems complete with both hardware and networking software that deliver secure mesh sensor networks with >99.999% data reliability and ultralow power (Figure 2).

[1] Case Study – Emerson Process and Dust Networks – www.linear.com/docs/41383
[2] Case Study – Vigilent and Dust Networks Reduce Data Center Energy – www.linear.com/docs/41384
[3] Case Study – Streetline and Dust Networks Make Cities Smarter and Happier – www.linear.com/docs/41387

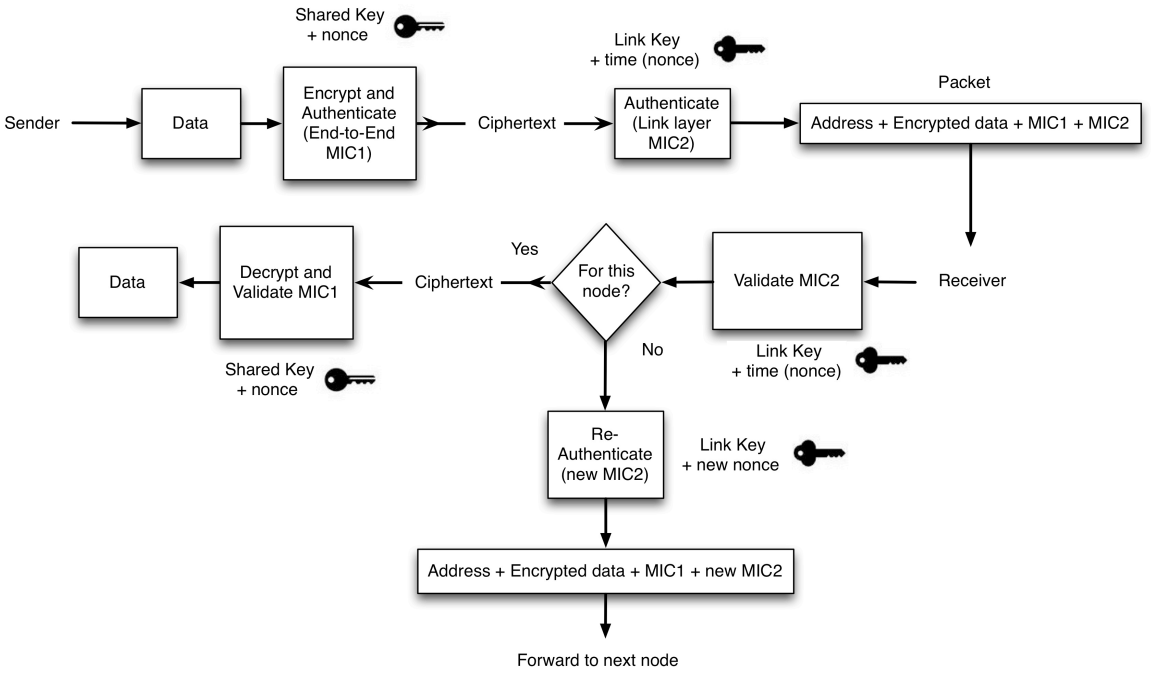

Figure 2: SmartMesh embedded wireless sensor networks from Linear Technology deliver >99.999% data reliability, multi-year battery life and are easily integrated using the LTC5800 system-on-chip in a compact QFN package.

Time Synchronized for Low Power

SmartMesh networks communicate using a Time Synchronized Channel Hopping (TSCH) link layer, a technique pioneered by Dust Networks and a foundational building block of wireless mesh networking standards, such as WirelessHART (IEC62591) and IEEE 802.15.4e. In a TSCH network, all motes in the network are synchronized to within a few microseconds, enabling network nodes to sleep at ultralow power between scheduled communications, typically resulting in a duty cycle of < 1%. In a SmartMesh mesh network, wireless nodes, even routing ones, typically consume <50µA average[4], enabling multi-year battery life on a pair of lithium AA batteries, or even operation on energy harvested power.

Path and Frequency Diversity for Reliability

Time synchronization enables channel-hopping on every transmitter-receiver pair for frequency diversity. With a SmartMesh network, every packet exchange channel-hops to avoid inevitable RF interference, and multiple transmissions can occur simultaneously, increasing overall network bandwidth. Each device has redundant paths to overcome communications interruption due to interference, physical obstruction or multipath fading. If a packet transmission fails on one path, a mote will automatically retry on the next available path and a different RF channel (see Figure 3).

[4] SmartMesh Power and Performance Estimator - www.linear.com/docs/42452

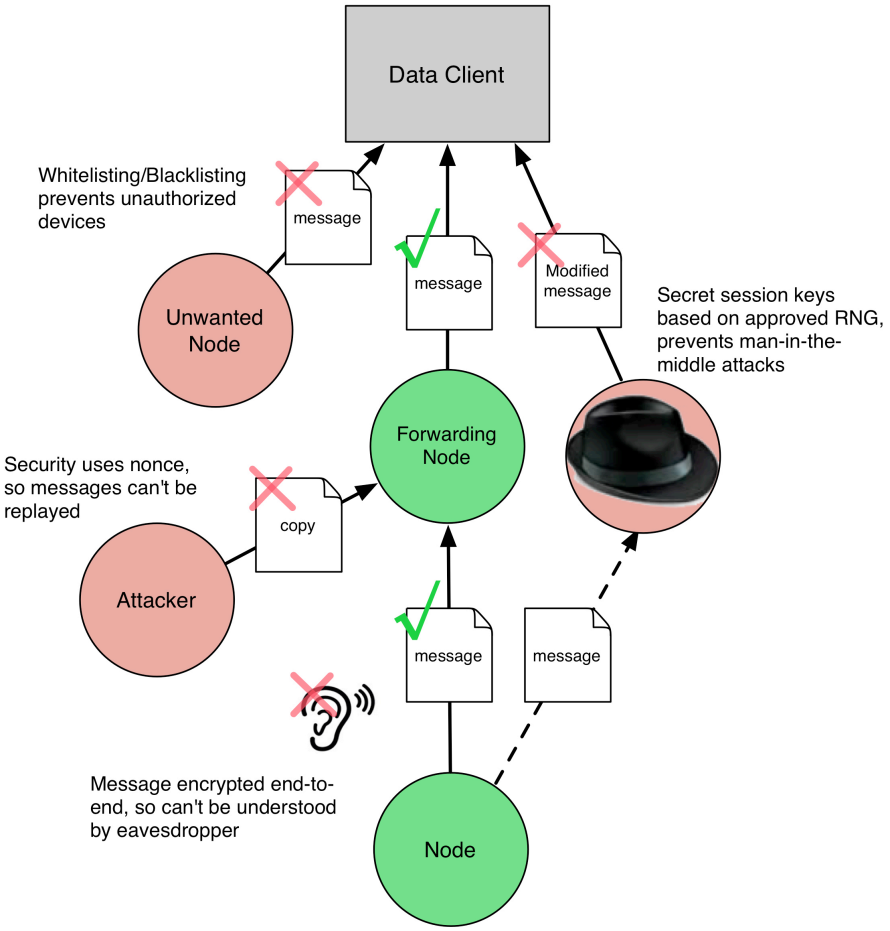

Figure 3: Path and Frequency Diversity – In a SmartMesh wireless network, if communication fails on the "green" arrow, node D retries on the "red" arrow using another channel

Secure Mesh Solution

SmartMesh networks have several layers of security to address confidentiality (through encryption), integrity (of a message) and authenticity (verifying that a message is from the stated sender). At the link-layer, packets are authenticated at each hop using a Message Integrity Check (MIC) based on a run-time key and a time-based counter. This ensures that only motes that are synchronized and have been admitted into the network by the manager can send messages. Additionally, packets are authenticated and encrypted end-to-end using run-time session keys and a shared counter. This ensures that only the intended recipient will understand the message (data privacy), and that replays, data corruption, or man-in-the-middle attacks can be avoided (data security). Furthermore, SmartMesh's 128-bit AES cipher has been certified to U.S. NIST Advanced Encryption Standard, FIPS-197. Encryption keys are generated using a true thermal random noise generator, as measured in the LTC5800 RF front-end with the antenna disconnected. This serves as the entropy source to seed a cryptographic random number generator (see Table 1).

Table1: SmartMesh Security Features

Security Feature	Benefit
Device Authentication	Choose from three increasingly strong levels of device authentication with the use of Access Control Lists (ACLs)
Encryption	128-bit AES-based encryption (NIST FIPS-197 certified) with multiple keys ensures privacy and confidentiality of the data
Thermal Random Noise Generator	Uses thermal noise as measured in the LTC5800 as the entropy source
Message Integrity Check (MIC)	Data transmitted is protected by message authentication codes to ensure that it has not been tampered with
Synchronized Key Changeovers	The entire network can be programmed to change over to a new encryption key automatically
Customized Key Rotation	The customer decides how often the network should change keys, balancing extra security with additional network traffic

Conclusion

By delivering reliable, secure, ultralow power wireless communications that are easily integrated, SmartMesh embedded wireless sensor networks are enabling users to design sensor networks that can be placed anywhere.