Security in Wireless Networks

Joe Tillison, Technology Director, Wireless Sensor Networks, Avnet Electronics Marketing

In March the Associated Press ran a story about security vulnerabilities in smart meters based on the research of InGuardians, Inc. The article highlighted the Achilles heel of any secure wireless system; the inadequate safeguarding of the security keys themselves. But perhaps even more damaging than simply identifying weaknesses in a few deployed products, the article stokes old consumer fears associated with emerging technologies that are not well understood. To win the public's confidence with these new gadgets, utility companies will have to develop a security strategy based on a top-to-bottom approach that protects the application at every level from attacks. These include both passive eavesdropping attacks and active attacks that might include jamming or physical tampering.

Data encryption can generally provide robust protection against passive eavesdropping attacks. Unlike Caesar's simple alphabetic shift cipher which was simple to decode; today's processor-driven algorithms use iterative transforms to successfully disguise information as random data. As an example, the IEEE802.15.4 radio, which is vastly popular for wireless sensor and actuator networks, uses the 128-bit Advanced Encryption Standard (AES) block cipher. The cipher is operated with a symmetric (shared private) key to encrypt frames at the link layer for data secrecy, and combined with nonces (number used once) to provide source authentication between conversing nodes. Encrypted frames are secure from over-the-air eavesdropping but once a key is acquired, the communication channel can be unlocked. IEEE802.15.4 defers the complexities of key generation, storage and distribution to the responsibility of higher layers in the protocol.

In addition to key management, the communications protocol generally provides a suite of security services to ensure nodes that participate in the network are authorized, and communication is both confidential and reliable. In sensor and actuator networks this can be particularly challenging since nodes can randomly join the network and routing configurations can change dynamically. Wireless devices are typically designed to be low cost and low power, and consequently have limited processing resources to manage a complex security scheme. Thus, security schemes for these types of networks are as creative and numerous as the number

of protocols available to operate them. Some have no security mechanism at all. ZigBee PRO provides two security options; standard security and high security. Both modes use a designated coordinator node as the Trust Center, responsible for all key management in the network. For a short list of other popular protocols see www.em.avnet.com/smartnetworks [1].

When protocols rely on devices to have pre-installed security keys, as many do, the network is vulnerable to physical attack, the scenario in the AP story. A “captured” node can be disassembled, the key stolen, and then used by an offending device to join the network masquerading as an authorized device. To protect against physical attacks, devices may employ hardware and software based anti-tamper mechanisms that disable the device or erase security sensitive memory when an intrusion occurs. Protection can also be provided at the application level, by guarding against abnormal activity outside the device’s usage profile.

Obviously the effort employed to defend a wireless network depends on the application where it’s used and the expected types of attack. Whether or not some miscreant would want to tamper with your smart meter is debatable. Nonetheless, it is incumbent on the industry to deploy secure products if there is to be broad public acceptance of wireless smart energy management technology.

Links:
[1] http://www.em.avnet.com/smartnetworks