Cryptographic Challenges for Smart Grid Home Area Networks Secure Networking

Author – Apurva Mohan, Honeywell ACS Labs

Wireless control devices used in home area networks and industrial control systems are resource-constrained, battery-powered wireless devices typically running on 8-bit, 50MHz microcontroller with 16KB ROM, and 512 Bytes RAM. To conserve their low battery power over long deployment periods, techniques like short messages, low cryptographic overhead, and long sleep cycles are employed.

Typical messages in these environments are short (4-12 bytes). Hash algorithms with 32 byte signatures or 16 byte block ciphers create a big overhead in terms of additional traffic, higher processing times and shorter battery life (even with hash truncation). Additionally, some control systems have strict response time requirements. Considering these requirements, developing cryptographic algorithms for secure communications in these environments becomes quite challenging because they should provide at least 112 bit security, create small signatures and small cipher blocks to minimize resource overhead, and facilitate efficient processing in resource constrained environments to adhere to strict response time requirements. Developing a robust PKI system is also challenging because the certificates should be processed by these devices efficiently and validated with limited or no internet connectivity.

Key management in these networks is challenging because it requires that devices store manufacturer's created strong pre-configured keys (or PKI certificates) and be able to authenticate with other manufacturer's devices. This requires establishing CA chains or inter-domain key management techniques. Key domain separation and provisions for forward and backward secrecy are also important concerns. These low cost devices do not have a trusted platform module to prevent physical extraction of the cryptographic keys and MAC address spoofing. Maintaining network security in the presence of such threats presents additional challenges.

Developing 1) Novel cryptographic algorithms for these environments, 2) Key management techniques, and 3) Providing network security in the presence of weak hardware protection are some important research challenges that deserve research attention.