Next-Generation Secure, Scalable Communication Network for the Smart Grid

An advanced radio technology that is inherently secure and robust for utility environments

Background

Spread spectrum techniques are used in communication systems to disperse signals, creating a wider bandwidth. This can establish more secure communications and resist interferences or jamming.

There is a significant gap between commercially available communications systems and those needed to satisfy the requirements associated with the electric sector. These requirements include noise/interference resistance, scalability, latency and data security. Several spread-spectrum wireless signal transmission protocols that are adequate for consumer applications are available, but none of them are sufficiently robust to operate within utility environments.

Barriers

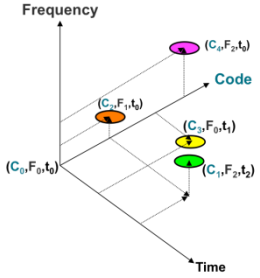
- Electric grid modernization efforts are rapidly increasing the complexity of systems
- Commercial wireless signal transmission protocols are not sufficiently robust to operate with high reliability in utility environments
- Utility environments include large amounts of multipath, noise and interference (including jamming), and they require data security, location tracking and support for operating hundreds to thousands of devices in close proximity

Project Description

This project involves developing a wireless technology that is robust, secure and scalable for smart grid applications, with advanced radio technology capable of high reliability in utility environments.

The project team will use Oak Ridge National Laboratory's Hybrid Spread Spectrum (HSS) waveform to develop code division multiple access (CDMA)-based wireless mesh networks. These networks are primarily used in the context of closed-loop and open-loop control systems such as advanced metering infrastructure (AMI) and distribution management. The team will also discuss existing and evolving wireless standards for utility environments for comparative analyses and design purposes.

HSS is a three dimensional signal



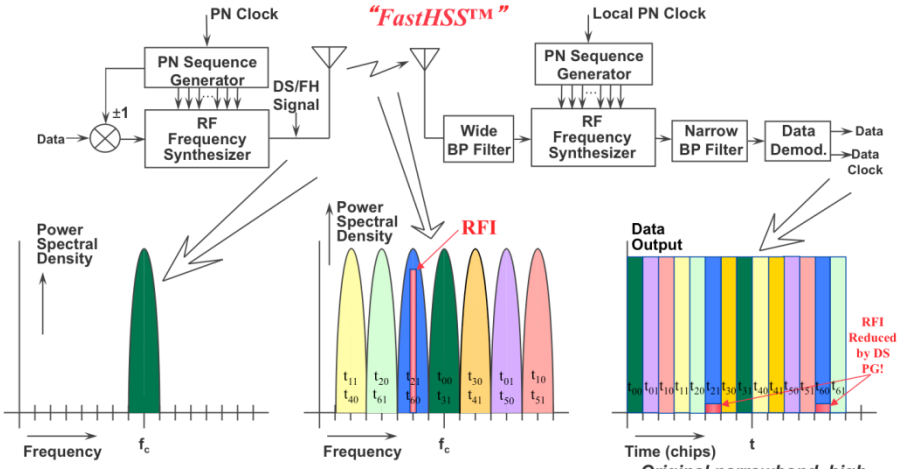
Benefits

- Addresses latency, jitter and security issues
- Uses adaptive hybrid spread-spectrum modulation format
- Suits high quality-of-service applications
- Provides superior resistance to multipath, noise, interference and jamming

Partners

- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Virginia Tech
- University of Tennessee-Knoxville
- OPUS Consulting
- Kenexis Consulting

Demonstration of FastHSS protocol



$G_{p(FH/DS)\,dB} = G_{p(FH)\,dB} + G_{p(DS)dB} = 10\ log\ (no.\ of\ hopping\ channels) + 10\ log\ (BW_{DS}/R_{info})$

Technical Objectives

The core objective of this project is to conduct research, development and demonstrations leading to a next-generation, secure and scalable communication network for the smart grid.

- Security in lower layers: Next-generation secure physical and media access control layer for smart grid applications. Implement full-scale simulation of the HSS in utility environments
- Scalability and self-configuring: Advanced multi-user techniques for seamless scalability of devices. Conduct a study to understand the coding considerations for HSS waveform design
- End-use applications: Secure-by-design with end-use application and deployment requirements including interoperability considerations
- Platform for robust control: Facilitate robust closed-loop control systems over communication networks in future smart grid applications
- Finalize the HSS/CDMA transceiver design for smart grid applications
- Conduct extensive performance analysis

End Results

Project results will include:

- A reduction in the gap between commercially available communication systems and systems needed to satisfy the demanding requirements of the electric sector
- Enhancement in the cybersecurity of smart grid communication and control systems

August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) R&D Program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

For More Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Teja Kuruganti
R&D Staff
Oak Ridge National Laboratory
865-241-2874
kurugantipv@ornl.gov

Visit Our Website:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity