Teja Kuruganti

Oak Ridge National Laboratory

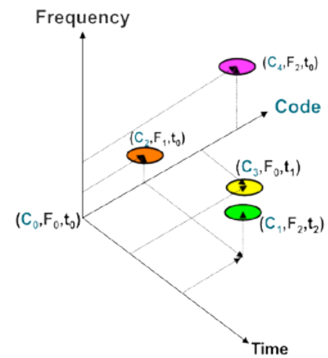
Next Generation Secure Scalable Communication Network for Smart Grid

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

Summary: Next Generation Secure Scalable Communication Network for Smart Grid

- **Objective**
  - Security in Lower Layers – Next generation secure PHY and MAC layer for EDS applications
  - Scalability and self-configuring – Advanced Multi-user techniques for seamless scalability of devices
  - Breakthrough reliability and availability
- **Technical Approach**
  - Quantify Utility Requirements
  - Laboratory prototype bringing all concepts from novel spread spectrum and multi-user detection techniques together and demonstrate to end-user community
  - Leveraging work in secure communications and industrial wireless communications
  - Identifying commercialization partners
    - Cost study performed to verify feasibility



HSS

OSI Model

	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

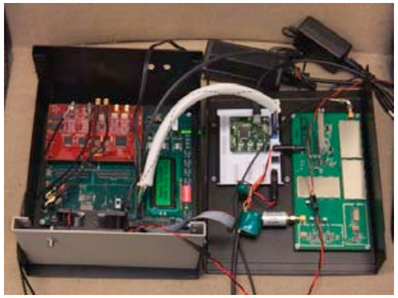
- **Schedule:** On schedule & scope 9/12
- **Performers:** ORNL, PNNL, Virginia Tech, OCG, KSC, UTK
- **Partners:** Southern Company, EPRI, PG&E, SCE

Technical Approach and Feasibility

- State of the Art: EDS security is currently achieved by
  - Compute intensive cryptographic techniques
  - Key management that does not scale as devices are deployed exponentially
  - A level of network complexity of current EDS devices that inhibits scalability
- Technical approach –
  - Quantify utility requirements;
    - Stakeholders advisory board is recruited to generate requirements
  - Laboratory prototype bringing all concepts (spread spectrum, multiple access, multi-user detection) together and demonstrate to the user community;
    - Laboratory demonstration for end-user evaluation
    - Laboratory prototype evaluated by PNNL
  - Commercialization partners
    - Discussion with Invensys: currently interacting on evaluation and identifying potential applications
    - Potential opportunities with Texas Instruments and Analog Devices
    - Publications to facilitate deployment
  - Extrapolate technology to other PHY layers and applications in utility environments

Technical Approach and Feasibility

- **Feasibility**
  - Potential end-user benefit
    - Reduced key management overhead
    - Provably secure EDS communication networks
    - Scalable devices for future EDS applications
    - Reduced network complexity
      - No time slots
      - Reduced network management
    - Replaces prescriptive security guidance with deterministic Quality of Service (QoS) guarantees
    - Directly traceable to end-user requirements for seamless integration with existing systems



Technical Approach and Feasibility

- **Challenges to Success**
  - Cost-performance tradeoff for highly secure communications
    - Improvements in hardware design methods including all-digital processing for low-cost designs
    - Prototype platforms to facilitate intermediate design verification
    - Cost study performed to verify commercialization feasibility
  - Simplifying options for end-user deployment
    - Configurable communication physical layer technology that is secure-by-design and can be programmably configured to application requirements
    - Provably secure coding schemes for spread spectrum waveforms
    - Multi-user detection and interference mitigation techniques
  - Mathematically rigorous estimation of performance improvement
    - Security, reliability, and network management
  - Information-theoretic limits to scalability of the communication networks used for EDS
    - Use of code division multiple access techniques in distributed (ad-hoc) networks for improved scalability
    - Enhanced multi-user detection for improved performance specific to utility environments

Progress to Date

- Successful demonstration of fast hybrid spread spectrum technology on laboratory hardware with clear path towards commercialization using commercial digital hardware for utility applications
- Performance measurements demonstrated close to theoretical limits (verified independently at PNNL)
- Analytical framework for optimal coupling of application requirements and communication parameters making secure communication design an engineering process (VTech)
- Actual Progress (technical, $, and time) vs Planned Progress
  - Prototype platform – completed ahead of schedule, with in budget
  - Mathematical framework publication – completed on schedule, on budget, review for journal
  - Third-party testing and assessment of platform – in progress (PNNL, KSC)

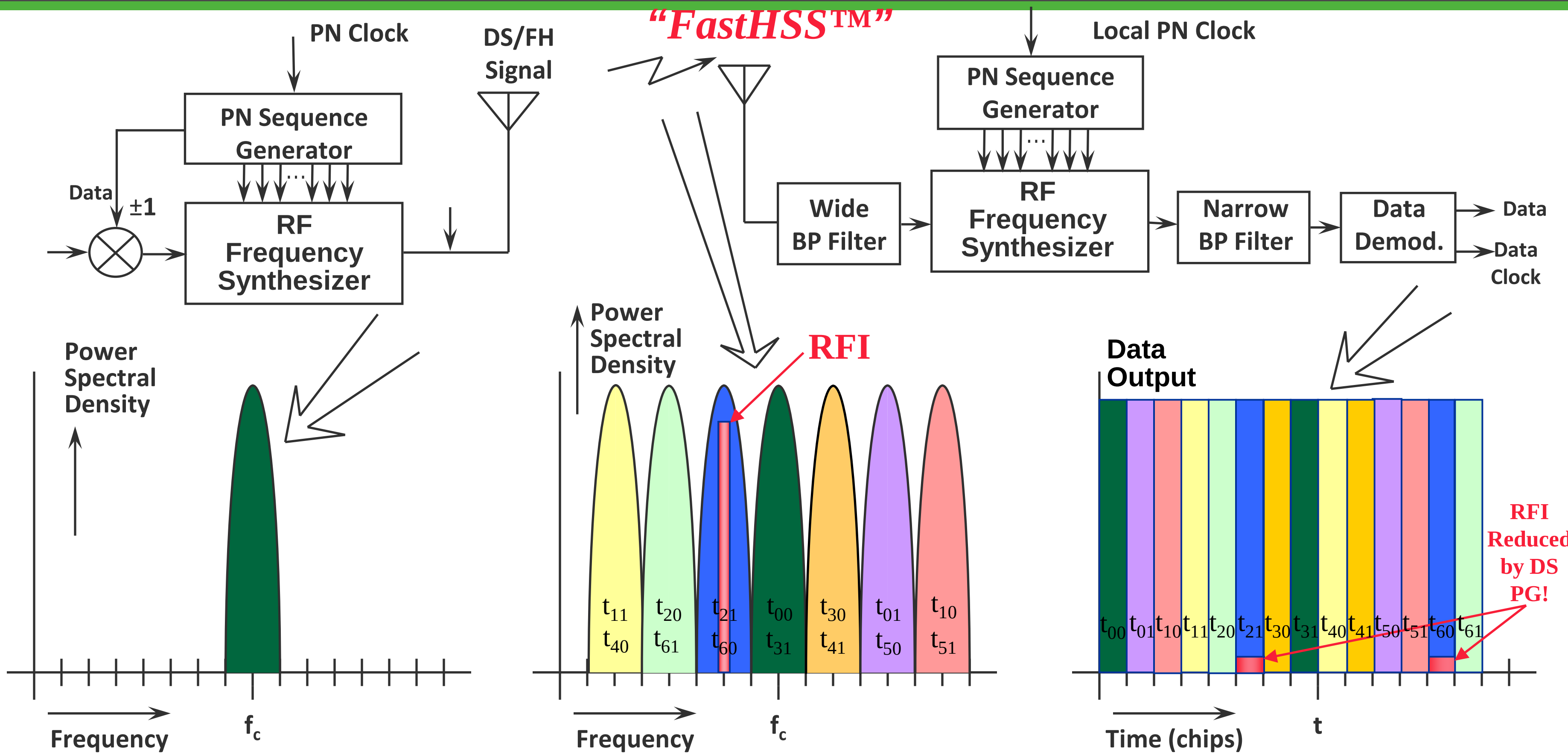
Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Demonstrations at EDS end-users and suppliers
    - Planned testing at Southern Company in FY12 Q4
  - Demonstration of secure, interoperable communication networks with existing EDS deployments
  - Engage utility industry experts for design requirements specification for future communication networks in EDS
  - Host interested suppliers to review the potential of the technology
  - Publications at academic and industry conferences
  - Next generation wireless communication will enable smart grid applications envisioned

Next Steps

- **Approach for the next year or end of project**
  - System-level optimization for integrated performance & MAC layer demonstration
  - Reconfigurability for specific end-user requirements
  - Quantitative comparison with current key management and transport layer security
  - Field testing of the devices in utility environment
    - Planned testing at Southern Company in FY12 Q4
    - Testing on ORNL AMI Interoperability Testbed
  - Risks faced
    - Key commercialization partner for technology development (utility partners are very keenly interested)
    - Interoperability with existing systems
- **Future**
  - Network provisioning for control over wireless networks for future smart grid applications
  - Precise position location and time synchronization in GPS-constrained environments
  - Secure code selection and analysis
  - HSS for other PHY layers
- **Describe potential follow-on work, if any**
  - Technology commercialization for specific EDS applications (2-3 years)
  - Optical/Quantum spread spectrum for utility backhaul networks (2 years)
  - Penetration testing of HSS-enabled device (1 year)

FAST HYBRID SPREAD-SPECTRUM (DS/FFH)



DS (wide) spectrum at output of modulator while hopping

Spectrum has same bandwidth and power density after hopping with PN sequence (PN Rate >> Data Rate for FastHSS™; e.g., as above, 2 hops per bit).

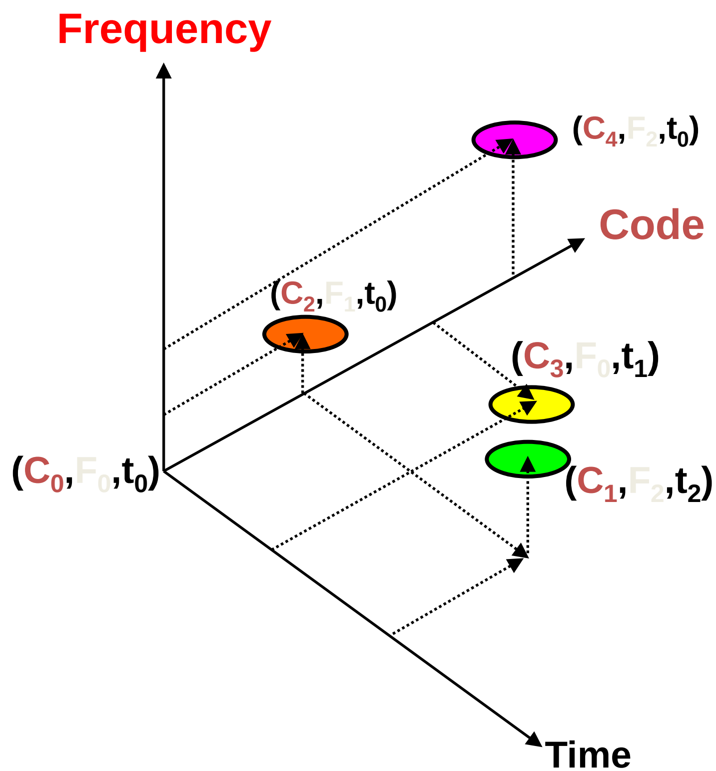
Original narrowband, high power data stream is restored if local PN sequence is same as and lined up with received PN sequence

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

Summary

HSS is a Multidimensional Signal

- HSS can be defined in 3 axes (code, frequency, and time).
  - Each dimension is orthogonal with the others.
  - Permissible signal spaces along an axis may also be ~ orthogonal.
    - » Codes
    - » Frequencies
    - » Time slots
- Easily adaptable to exploit many degrees of freedom to meet system requirements.
- Some signal overlaps may be orthogonal.
- Numerically Controlled Oscillator for Fast Frequency Synchronization
- Specific PN code generator to exploit properties of code

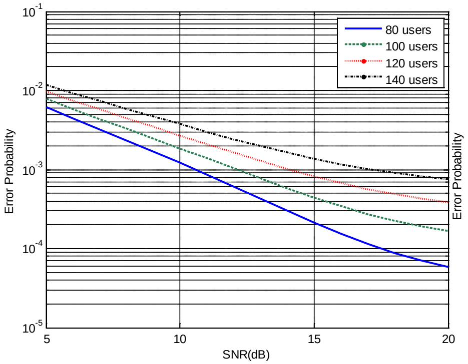


Publications, Reports, and Patents

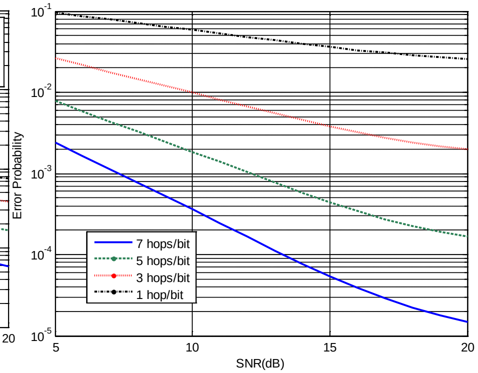
- **Publications** (3 under preparation not mentioned)
  - M.M. Olama, X. Ma, P.T. Kuruganti, S.F. Smith, and S.M. Djouadi, "Hybrid DS/FFH Spread Spectrum: A Robust, Secure Transmission Technique for Communication in Harsh Environments," *Proceedings of the IEEE Military Communications Conference (MILCOM)*, pp. 2136-2141, Nov. 7-10, 2011
  - S.L. Clements, H. Kirkham, M. Elizondo,S. Lu, "Protecting the Smart Grid: A Risk Based Approach," IEEE PES Meeting July, 2011
  - M.M. Olama, S.F. Smith, P.T. Kuruganti, and X. Ma, "Performance Study of Hybrid DS/FFH Spread-Spectrum Systems in the Presence of Frequency-Selective Fading and Multiple-Access Interference," *Proceedings of the IEEE International Communications Quality and Reliability (CQR) Conference*, May 15-17, 2012
  - X. Ma, M.M. Olama, P.T. Kuruganti, S.F. Smith, and S.M. Djouadi, "Determining System Parameters for Optimal Performance of Hybrid DS/FFH Spread-Spectrum," *Accepted for Publication in the IEEE Military Communications Conference (MILCOM)*, Oct. 29-Nov. 1, 2012.
  - X. Ma, M.M. Olama, P.T. Kuruganti, S.F. Smith, and S.M. Djouadi, "Security of Classic PN-Spreading Codes for Hybrid DS/FH Spread-Spectrum Systems," *Submitted to the IEEE International Conference on Computing, Networking and Communications (ICNC)*, Jan. 28-31, 2013.
- **Reports (significant)**
  - Xiao Ma, Mohammed Olama, Teja Kuruganti, Stephen Smith, "Literature Review of Hybrid Spread Spectrum Technology"
  - Stephen F. Smith, Teja Kuruganti, and Stephen M. Killough, "Hybrid Spread Spectrum (HSS) System Design For Utility Smart Grid Applications"
  - B.A. Akyol, H. Kirkham, S.L. Clements, M.D. Hadley, "A Survey of Wireless Communications for the Electric Power System"
  - Shravan Garlapati et al., "Analysis of Network Bandwidth Requirements for the Advanced Metering Infrastructure"
  - MD Hadley, SL Clements, TE Carroll, "AMI Communication Requirements to Implement Demand-Response: *Applicability of Hybrid Spread Spectrum Wireless"*
  - Mohammed M. Olama, Stephen F. Smith, Teja Kuruganti, Xiao Ma, "HSS Provides Physical Security for Smart Grid Communications"
  - Mohammed M. Olama, Stephen F. Smith, and Teja Kuruganti, Code Acquisition of Hybrid Spread-Spectrum Signals, Technical Report, 2012.
  - Michael Buehrer et al., "Spreading code design and multi user detection for HSS and CDMA" (2 reports)
  - Michael Buehrer et al., "Collaborative localization techniques" (draft reports)
- **Patents**
  - "Spread Spectrum Signal Processing for Low Power Transmitters," Stephen Killough (Invention Disclosure filed)
  - "Hybrid Spread Spectrum Radio System", Stephen F. Smith and William B. Dress, U.S. Patent 7,660,338
  - "Hybrid Spread Spectrum Radio System", Stephen F. Smith and William B. Dress, U.S. Patent 7,656,931
  - "Hybrid Spread-Spectrum Technique for Expanding Channel Capacity", U. S. Patent 7,092,440, W. B. Dress, Jr., S. F. Smith, and M. R. Moore

Performance of a Hybrid DS/FFH System

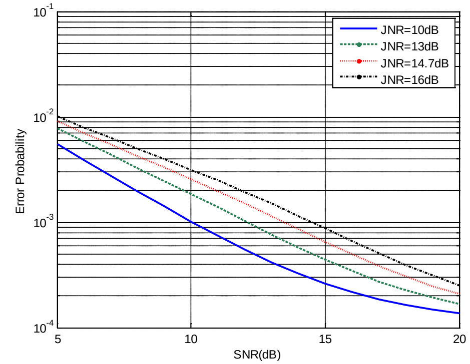
Effect of multi-user interference



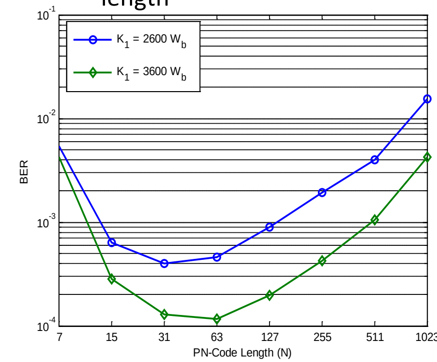
Effect of different number of hops per bit



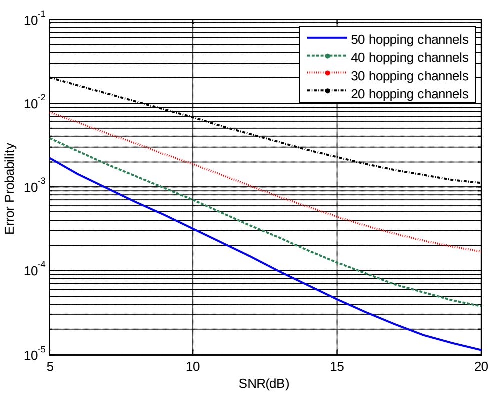
Effect of different jamming-to-noise ratios (JNRs)



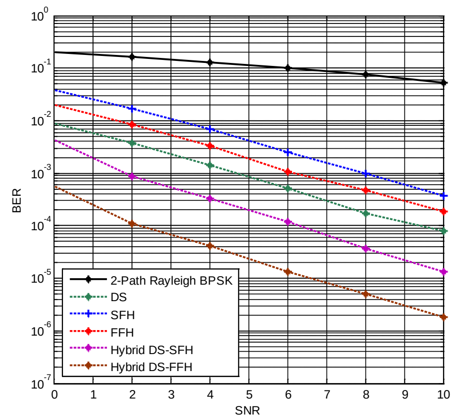
Optimal DS PN-code length



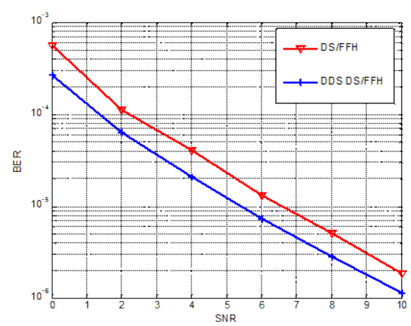
Effect of different number of hopping channels



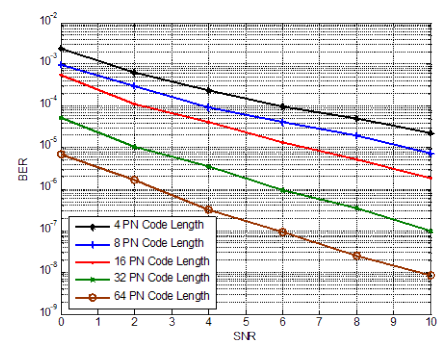
Performance comparisons of SS



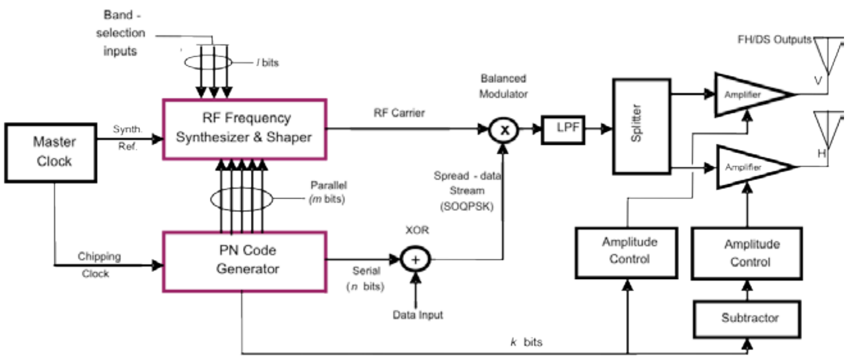
Effect of DDS hopping technology



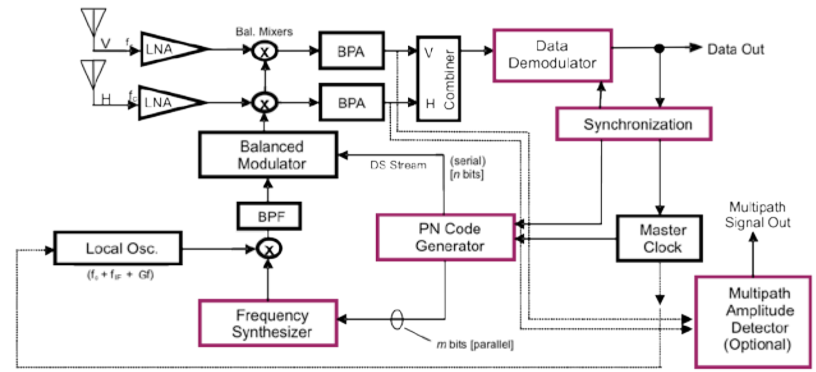
Effect of different PN-code lengths



Laboratory Prototype



= New technologies from this project



= New technologies from this project