Focus Area: Communication and Control Protocols

Presented by Klara Nahrstedt

Personnel

- Senior PIs/Personnel
  - David Bakken (WSU)
  - Anjan Bose (WSU)
  - Carl Hauser (WSU)
  - Himanshu Khurana (UIUC)
  - Klara Nahrstedt (UIUC)
  - William Sanders (UIUC)
  - Anna Scaglionne (Cornell)
  - Robert Thomas (Cornell)
  - Zhifang Wang (Cornell)
  - Von Welch (UIUC)
  - Marianne Winslett (UIUC)
- Student Alumni
  - Harald Gjermundrod (PhD '06)
  - Ioanna Dionysiou (PhD '06)
  - Venkata Irava (PhD '06)
  - Joel Helkey (MS '07)
  - Stian Abelsen (MS '07)
  - Erlend Viddal (MS '07)
- Current Students/Other Personnel
  - Dave Anderson (WSU)
  - Rasika Chakravarthy (WSU)
  - Tamal Das (UIUC)
  - Terry Fleury (UIUC)
  - Loren Hoffman (WSU)
  - Shrut Kirti (Cornell)
  - Jim Kusznir (WSU)
  - Adam Lee (UIUC)
  - Chris Masone (Dartmouth)
  - Kazuhiro Minami (UIUC)
  - Sunil Muthuswamy (WSU)
  - Hoang Nguyen (UIUC)
  - Raol Rivas (UIUC)
  - Ravi Sathyam (UIUC)
  - Nathan Schubkegel (WSU)
  - Erik Solum (WSU)
    Yang Tao (WSU)
  - Saman Aliari Zonouz (UIUC)

University of Illinois • Dartmouth College • Cornell University • Washington State University

Problem Space

Trend/Premise:

Next Generation Power Grid Infrastructures will deploy COTS Computing and Communication components for their process control SCADA cyber-infrastructure

Needs:

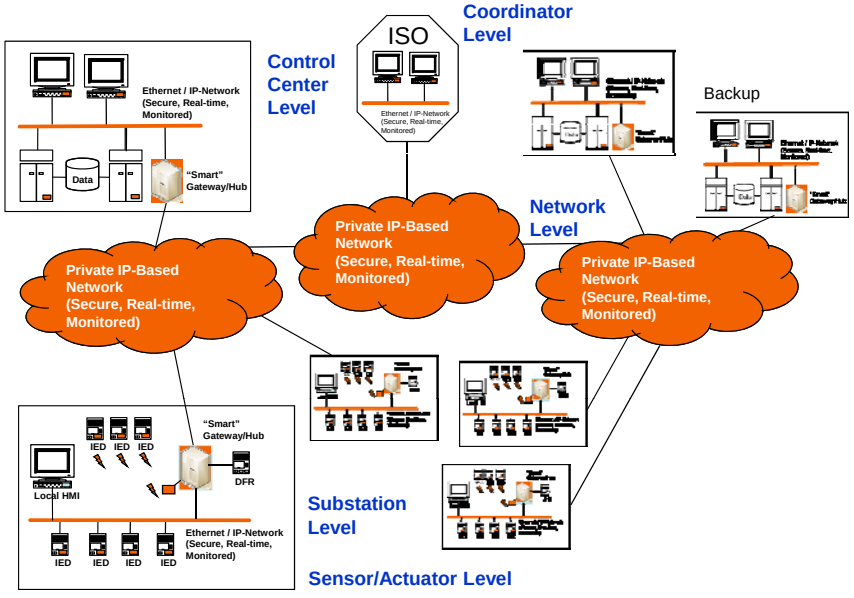
Cyber-infrastructure for PowerGrid needs holistic end-to-end protocol and service solutions with respect to performance and trust issues

Refined Protocol/Service Challenges:

- End-to-end key management
- End-to-end authentication, access control and trust negotiation
- End-to-end real-time/QoS guarantees
- Provision of real-time and reliable monitoring, detection, alert, containment and recovery solutions in case of perturbations, vulnerabilities and attacks

University of Illinois • Dartmouth College • Cornell University • Washington State University

Vision: End-to-End Trust Provisioning for Power Grid Monitoring and Control



University of Illinois • Dartmouth College • Cornell University • Washington State University

Threat Modeling

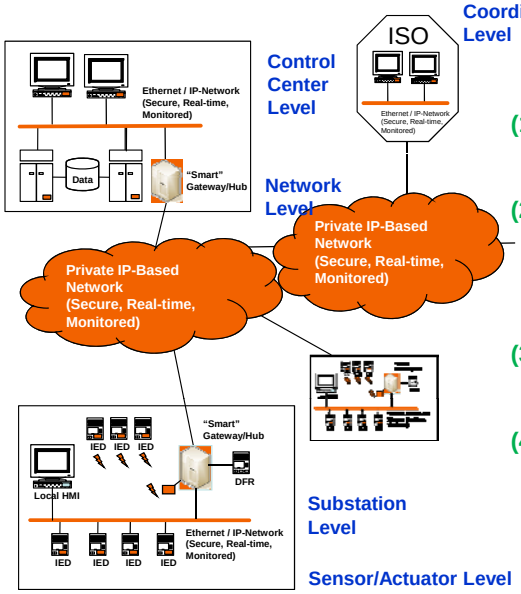
- **Problem: Assess cyber threats to Power Grid to**
  - Aid in defining the scope of security problems
  - Allow for assessment of efficacy of security solutions
  - Enable development of a taxonomy
- **Approach: Develop modeling framework**
  - Emphasize vulnerabilities and potential damage
  - Survey known attacks to build and populate framework
- **Results**
  - Attack-Vulnerability-Damage framework
  - Surveyed >50 known attacks

- **Example Cyber Attacks**

Attack			Vulnerability	Damage		
Name/ Origin	Action	Target	Vulnerability	State Effect	Perf. Effect	Severity
Data Storm/ Local	Flood	Network	Specification	Avail.	Precision	Medium
Slamm-er/ Remote	Copy	Process	Implementation	Integrity	Accuracy	Low
XA21/ Local	Terminate	Process	Implementation	Integrity	Timeliness	Medium
NMAP Scan/ Remote	Probe, Scan	Network	Specification	Conf.	None	Low
TCP Reset/ Remote	Terminate	Network	Specification	Avail.	Timeliness	High

University of Illinois • Dartmouth College • Cornell University • Washington State University

End-to-End Trust Provisioning for Power Grid Monitoring and Control



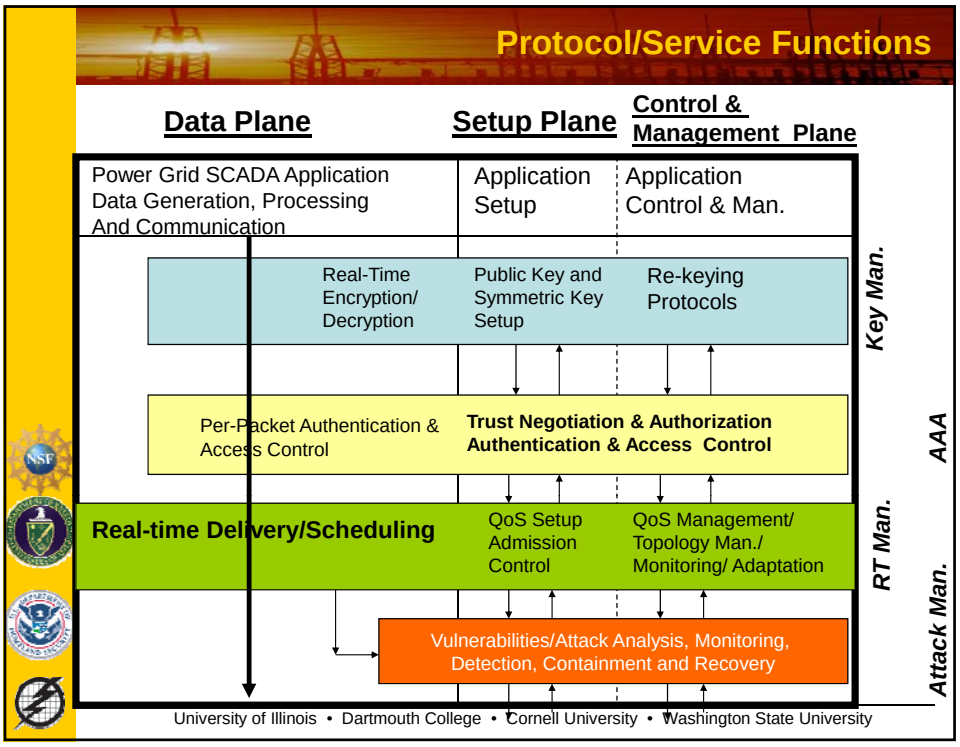
(1) End-to-End Key Management

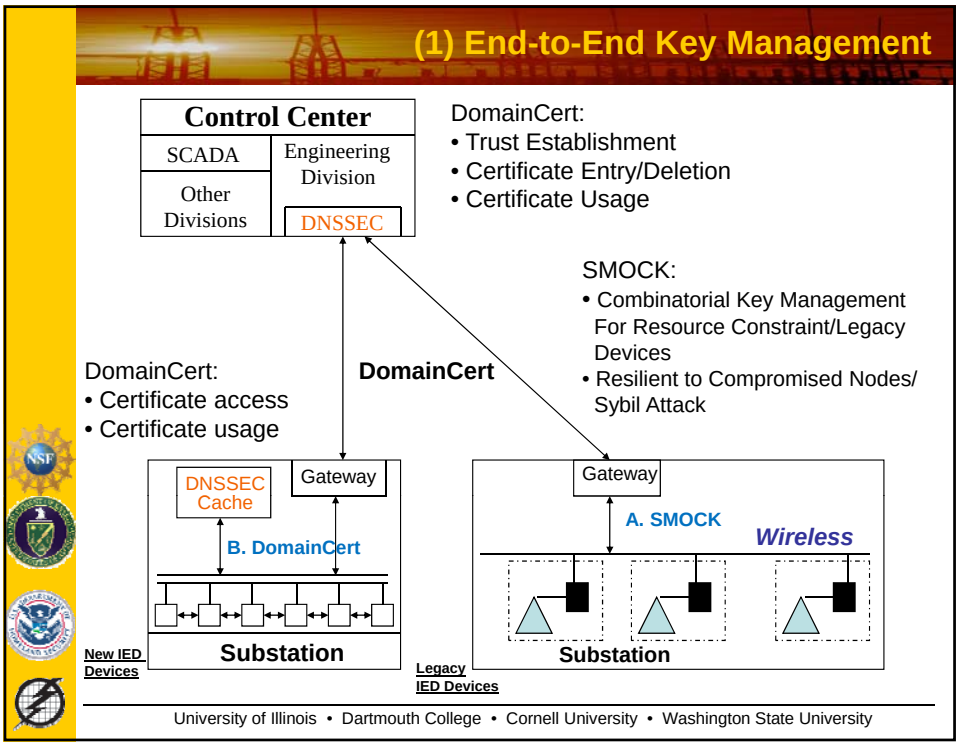
(2) Authorization, Authentication And Access Control (AAA)

(3) Secure and Real-Time Transmission

(4) Vulnerabilities/Attacks Monitoring, Detection, Containment, Recovery

University of Illinois • Dartmouth College • Cornell University • Washington State University


Protocol/Service Functions
Data Plane
Setup Plane
Control & Management Plane
Power Grid SCADA Application Data Generation, Processing And Communication
Application Setup
Application Control & Man.
Real-Time Encryption/ Decryption
Public Key and Symmetric Key Setup
Re-keying Protocols
Key Man.
Per-Packet Authentication & Access Control
Trust Negotiation & Authorization Authentication & Access Control
AAA
Real-time Delivery/Scheduling
QoS Setup Admission Control
QoS Management/ Topology Man./ Monitoring/ Adaptation
RT Man.
Vulnerabilities/Attack Analysis, Monitoring, Detection, Containment and Recovery
Attack Man.
University of Illinois • Dartmouth College • Cornell University • Washington State University


(1) End-to-End Key Management
Control Center
SCADA
Engineering Division
Other Divisions
DNSSEC
DomainCert:
• Trust Establishment
• Certificate Entry/Deletion
• Certificate Usage
SMOCK:
• Combinatorial Key Management For Resource Constraint/Legacy Devices
• Resilient to Compromised Nodes/ Sybil Attack
DomainCert:
• Certificate access
• Certificate usage
DomainCert
DNSSEC Cache
Gateway
B. DomainCert
Substation
New IED Devices
Gateway
A. SMOCK
Wireless
Substation
Legacy IED Devices
University of Illinois • Dartmouth College • Cornell University • Washington State University

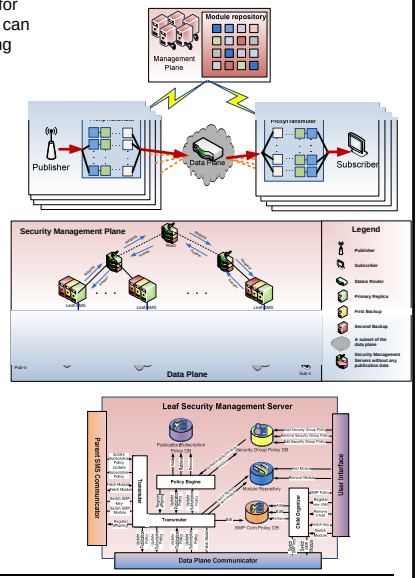
(2) End-to-End AAA – Trusted Authorization of GridStat Secure Status Dissemination

- **Problem**

  Achieve confidentiality, integrity and availability (CIA) for GridStat's status dissemination in a dynamic way that can evolve with changes in the security field during the long lifecycle of information systems for the power grid.

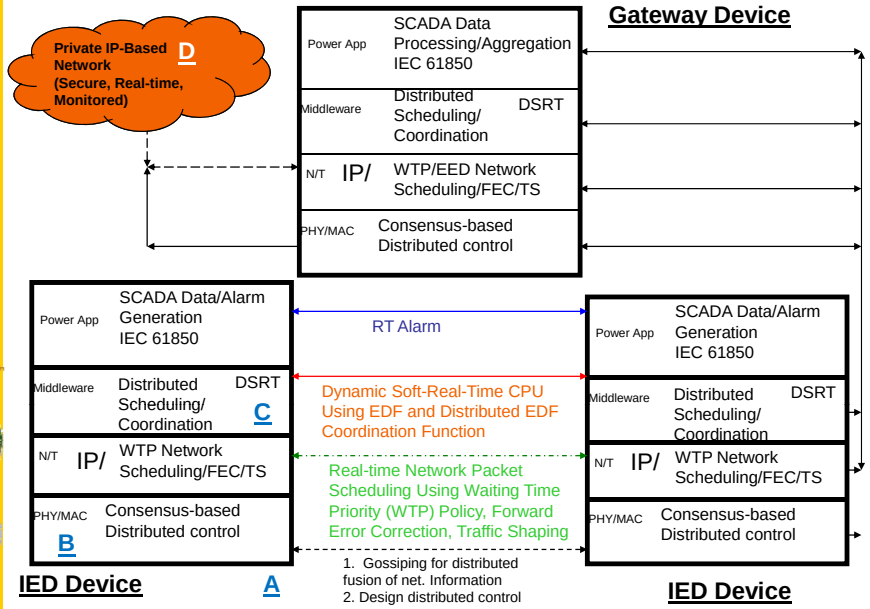
- **Approach**
  - Design and implement proof of concept modules with different functional and performance attributes such as bandwidth, latency and throughput attributes.
  - Evaluate the Data Plane Security Architecture together with developed modules in terms of their dynamics and performance and gained confidentiality, integrity and accessibility
  - Authorization via *trust negotiation;* Policy compiler, high-performance runtime policy; compliance checker; Resilience to attack via careful replication

- **Results**
  - Replaced modules and keys over the wire at runtime without relying on root keys/certificates
  - Implemented **encryption**, **authentication, etc**
  - TrustBuilder2 framework for experimenting with trust negotiation (SourceForge); Fastest policy compliance checker for Datalog-style policy languages



University of Illinois • Dartmouth College • Cornell University • Washington State University

(3) End-to-end Real-Time Data Delivery



University of Illinois • Dartmouth College • Cornell University • Washington State University

Project 3.A: Random Topology Power Grids

- **Problem:**
  - Develop a methodology to produce a large number of test power grids with appropriate topologies and scalable network size, in order to design, examine or verify any proposed implementation. One example is to answer how much communication flow do I need between different parts of the network in order to manage it and control it.
- **Approach:**
  - Formation of random topologies
    - Nodal locations
    - Link selection
    - Connectivity Check
  - Assignments of power grid parameters
    - Impedance of transmission lines
    - Loads and generation settings
    - Initial operating equilibrium

Results

- Model proposed is able to generate random-topology power grids which effectively approximate the topological and electrical characteristics of real power system grids.
- Eigenvalues distribution of the generated power grids is very similar to that of IEEE standard system. Between the two varieties of the model, Poisson-RT works better than Uniform-RT to approximate the selected standard model systems.

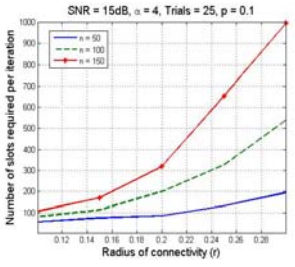
University of Illinois • Dartmouth College • Cornell University • Washington State University

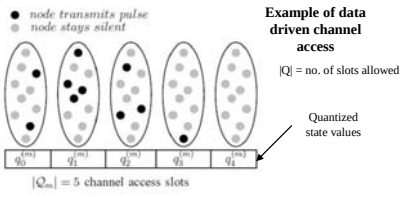
Project 3.B: Scalable Communication Protocols for Real-Time State Estimation in Power Networks

- **Project Problem**
1. How to achieve decentralized state estimation (DSE)?
2. How to design communication architecture that enables DSE directly at all of the PMU's?

- **Approach**
1. DSE → distributed Kalman Filter
2. Message structure - Extend the use of "average consensus" protocols to extended Kalman filters [Olfati-Saber CDC05]
3. Media Access Control (MAC) Coding - Data driven channel access $\lim_{k\to\infty} \hat{y} = \sum_{i=1}^{n} y_i(k)$: fast average consensus [Kirti and Scaglione CI

- **Results**
1. Designed data driven communication protocol
   - Scalable physical layer gossiping protocol for quantized average consensus
   - Uses node data to drive the transmission scheduling and modulation
   - Opportunistically exploits broadcast wireless channel to perform desired computations
2. Implemented distributed Kalman filter using data driven communication → figure shows distributed tracking of object's position

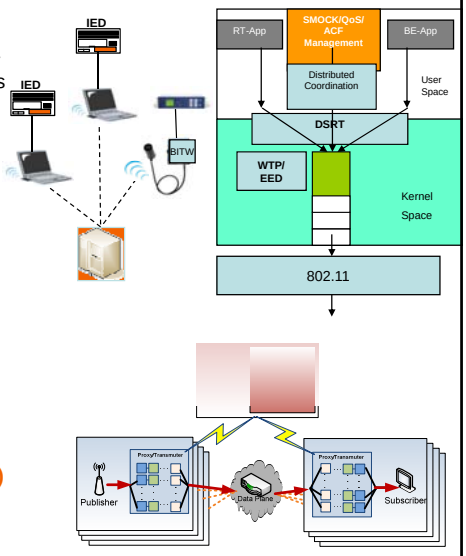




University of Illinois • Dartmouth College • Cornell University • Washington State University

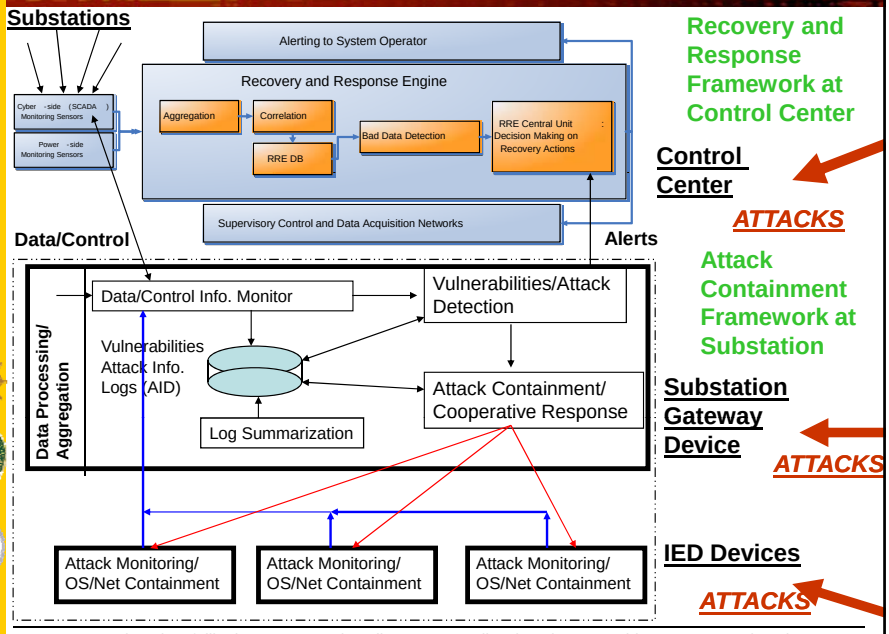
Project 3.C/D – Integrated CPU and Network Scheduling in 802.11 Wireless Networks and QoS Routers

- Problem:
  - Provide end-to-end real-time delivery over wireless and wide area networks
- Approach:
  - Dynamic Soft Real-time Scheduling (DSRT) with EDF policy as CPU scheduling at IEDs & gateway
  - Waiting Time Priority (WTP) as intra-network scheduling on IEDs & Gateway
  - End-to-end Earliest Deadline Network Scheduling Policy at Gateways, Routers & Control Center
  - Coordination Protocol among DSRT(s) for allowing Distributed Scheduling
- Results
  - **End-to-end delay is in the order of milliseconds (< 10ms)**
  - Smaller jitter
  - QoS Routers in Gridstat
  - C/C++ implementation for faster, more predictable performance



University of Illinois • Dartmouth College • Cornell University • Washington State University

(4) Vulnerabilities/Attacks Monitoring, Detection, Containment, Recovery



University of Illinois • Dartmouth College • Cornell University • Washington State University

Accomplishments

- Theory
  - Exploration of mathematical models for scalable channel coding to achieve consensus among nodes
  - Random Topology Power Grids
  - Modeling of end-to-end attack monitoring, detection and containment/ recovery (Probabilistic Real-Time Intrusion Detection & Attack Containment and Attack Degree Modeling)
  - Compliance checker
  - Trust negotiation state consistency enforcement algorithms
- Software
  - Secure Real-time End-to-end Delivery Protocol for Wireless Networks in Substations (DSRT CPU RT Scheduler & WTP Network RT Scheduler & SMOCK)
  - Optimized TrustBuilder2 framework for trust negotiation
  - Compliance Checker
  - GridStat –based Real-time Command Control (RT and Reliable Router & RPC for Actuator Control)
  - DomainCert Prototype
- Evaluation
  - Evaluation of secure real-time protocols over 802.11b and 802.11a wireless technologies (see Demo)
  - Evaluation of Integrated TrustBuilder2 and GridStat (see Demo)
  - Evaluation of other theoretical distributed algorithms and protocols via simulations (see Posters)

University of Illinois • Dartmouth College • Cornell University • Washington State University

Future Work

- Integration of research results within Protocols Group
  - Gridstat AAA and End-to-End Key Management
  - End-to-End Key Management with DomainCert and SMOCK
  - End-to-End Attack Monitoring/Detection with RRE and ACF
  - Integration of Attack Protection Management with Attack Characterization
  - Integration of End-to-End Secure Real-Time Delivery from Substation to Control Center with DSRT/SMOCK/ACF/WiFi and GridStat
  - Collaboration on state estimator problem
- Integration of research results with Evaluation Group
  - Considerations of Wireless Channels in RINSE –802.11i, 802.11e, Zigbee, Bluetooth,…
  - Use of RINSE for Scalable Wireless/IP/Transport/Overlay Protocols Validation
- Integration of research results with Device Group
  - DomainCert/SMOCK Key Management Integration with Secure IEDs
  - Usage of Trusted Hardware for Secure Real-time End-to-End Protocols to Protect SCADA data and Commands within Substation and between Substations and Control Centers

University of Illinois • Dartmouth College • Cornell University • Washington State University