Project Kick-Off Meeting: Integrated Learning Environment for Cyber Security of Smart Grid

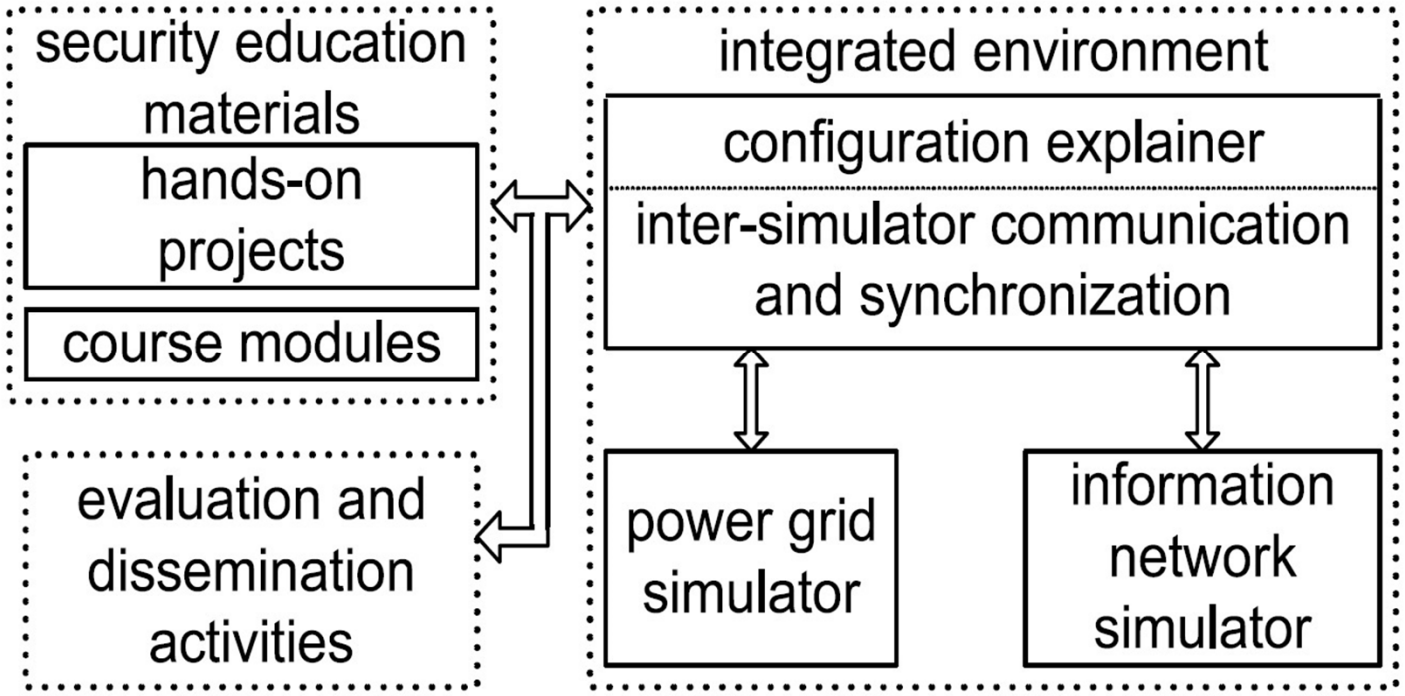
Participation Universities: UNCC, Georgia State, and Texas A&M

Jan/24/2014, Charlotte, NC.

- Background:
  - The project was first submitted as NSF TUES Phase II in 2012;
  - Submitted to NSF SFS program "capacity building" track in Oct 2012;

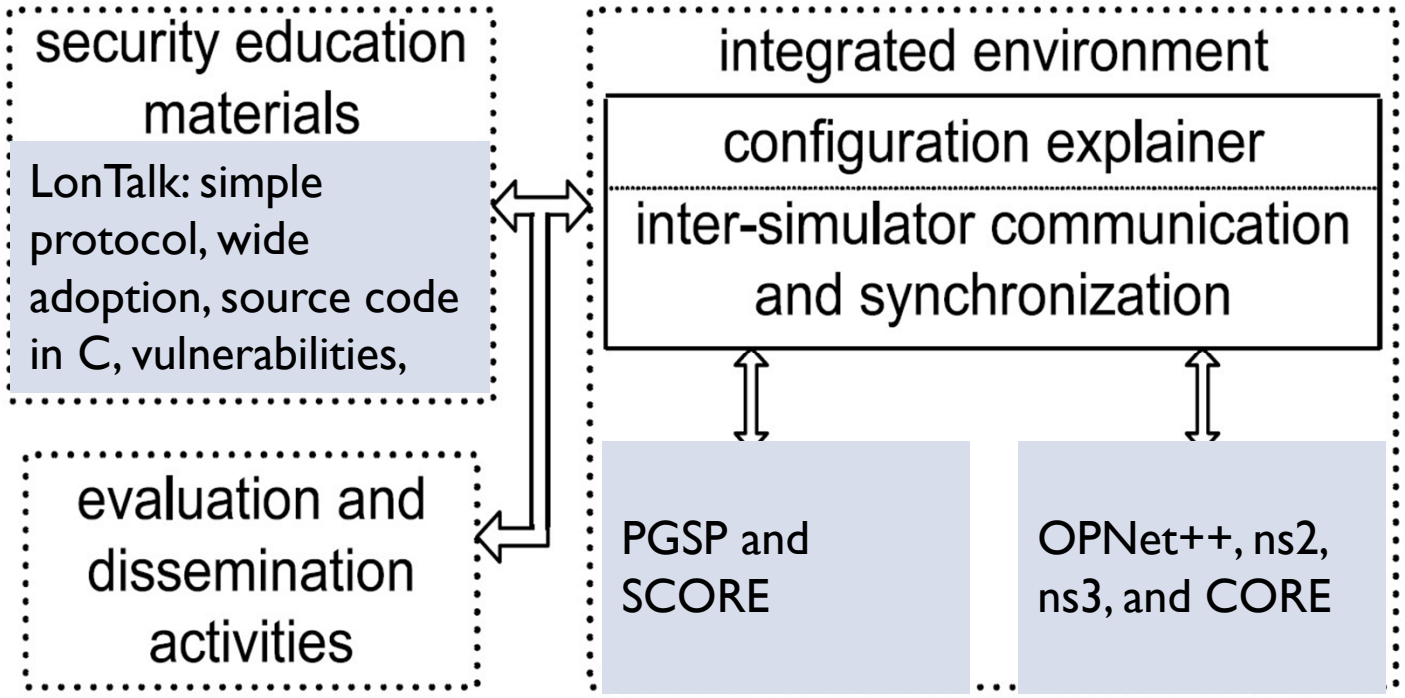
- Team member:
  - UNCC: Weichao Wang, Yu Wang, and Chuang Wang;
  - Texas A&M: Le Xie;
  - Georgia State: Yi Pan and Wenzhan Song

- Overall architecture of the project



- What is new:
  - An integrated, open source system that covers both power grid and information networks;
  - Real time interaction b/w the two systems;
  - Focus on the user-end protocols instead of generation and distribution sides;
  - Educational materials and evaluation;

- Overall architecture of the project

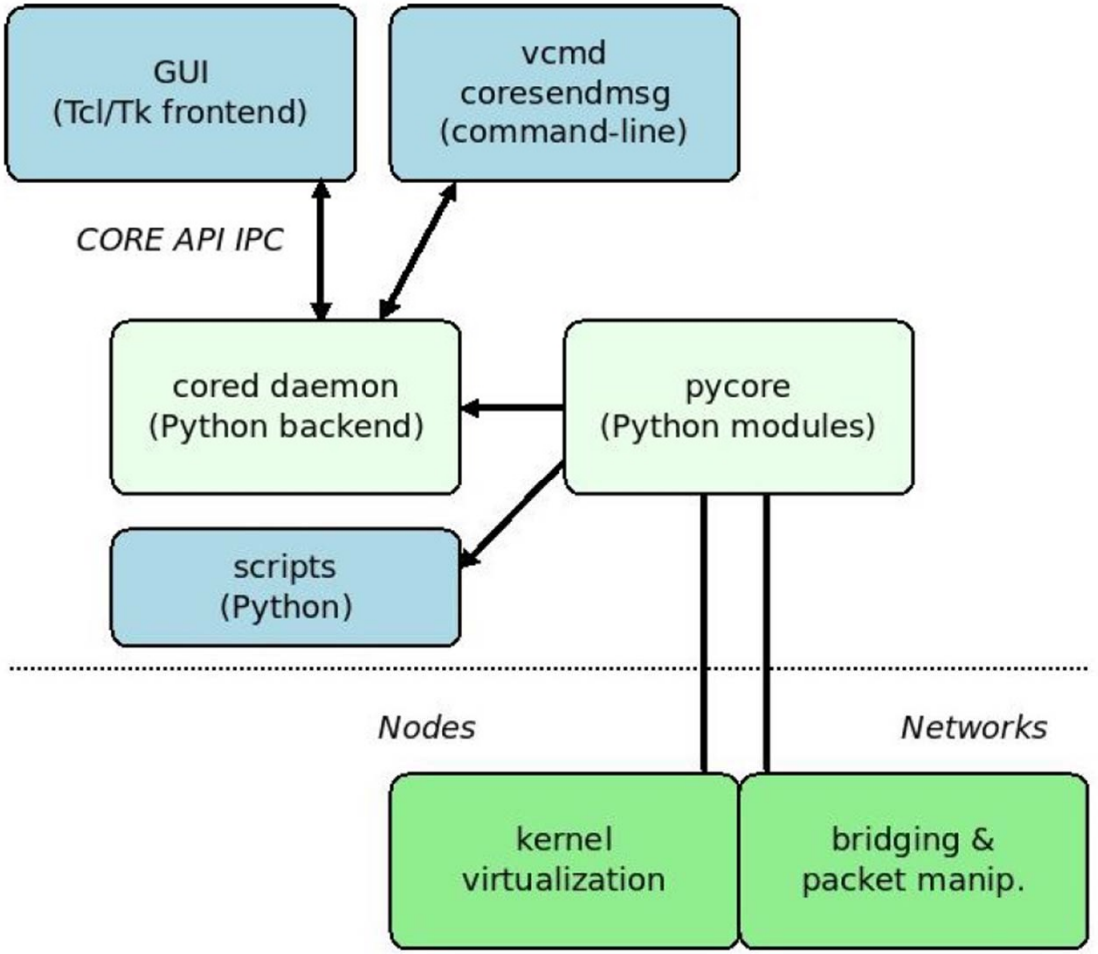


- Major challenges
  - Choose a platform;
    - Implement LonTalk in the chosen platform;
    - Interconnection between the cyber and physical systems and how they impact each other;
    - Associate the efforts with educational activities and work force development;

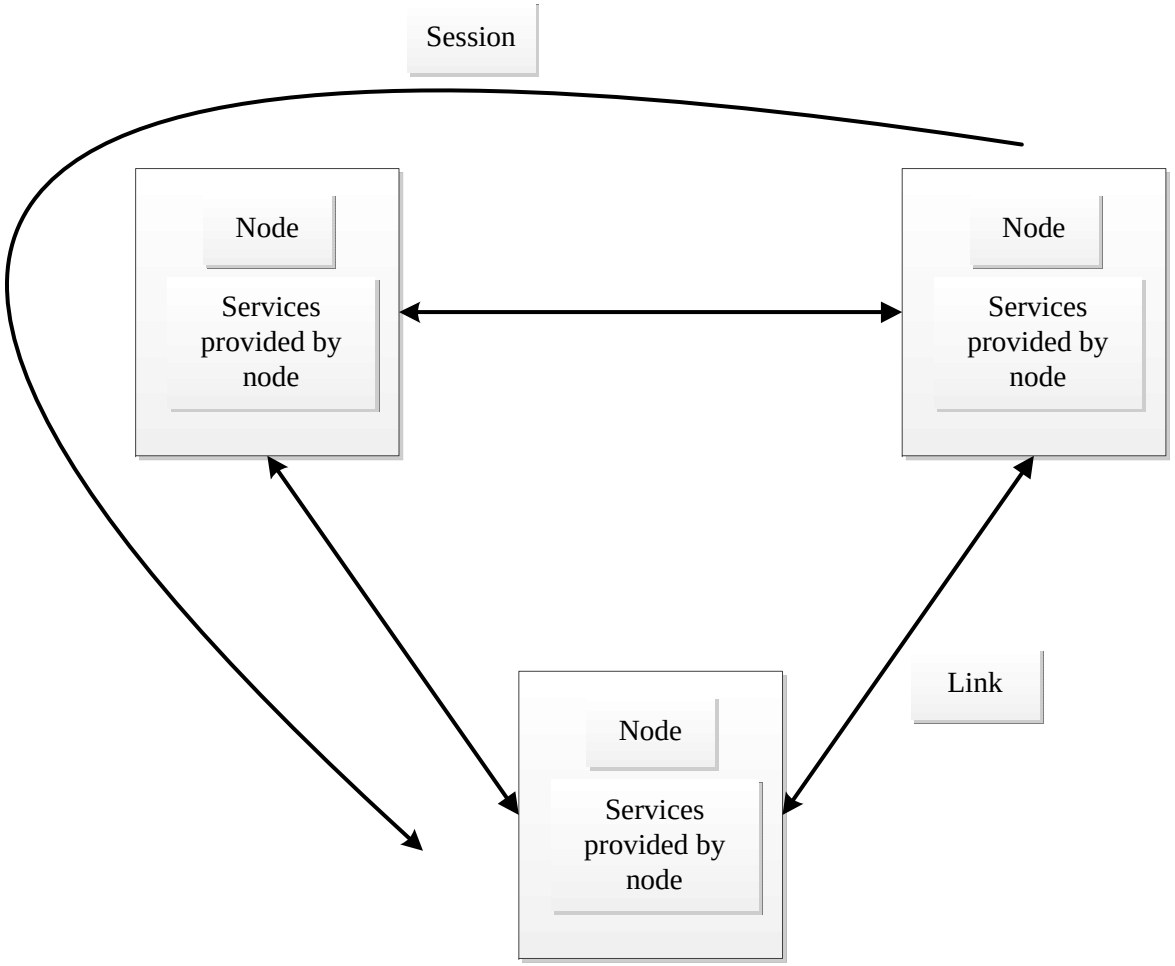
- Task 1: Choose a platform
  - We have considered the following network simulators: OMNeT++, ns2, ns3, and CORE;
  - The following power grid simulators: Power Grid Simulator Program (PGSP), SCORE
  - Thanks to the contribution of Wenzhan, we plan to choose CORE and SCORE as the foundation of the project.

- CORE (common open research emulator)
  - Designed by Boeing, now under the wing of Navy;
  - A communication network emulator;
  - Front side is TCL/TK, back side is written in Python;
  - Run in Linux environments;

- CORE structure

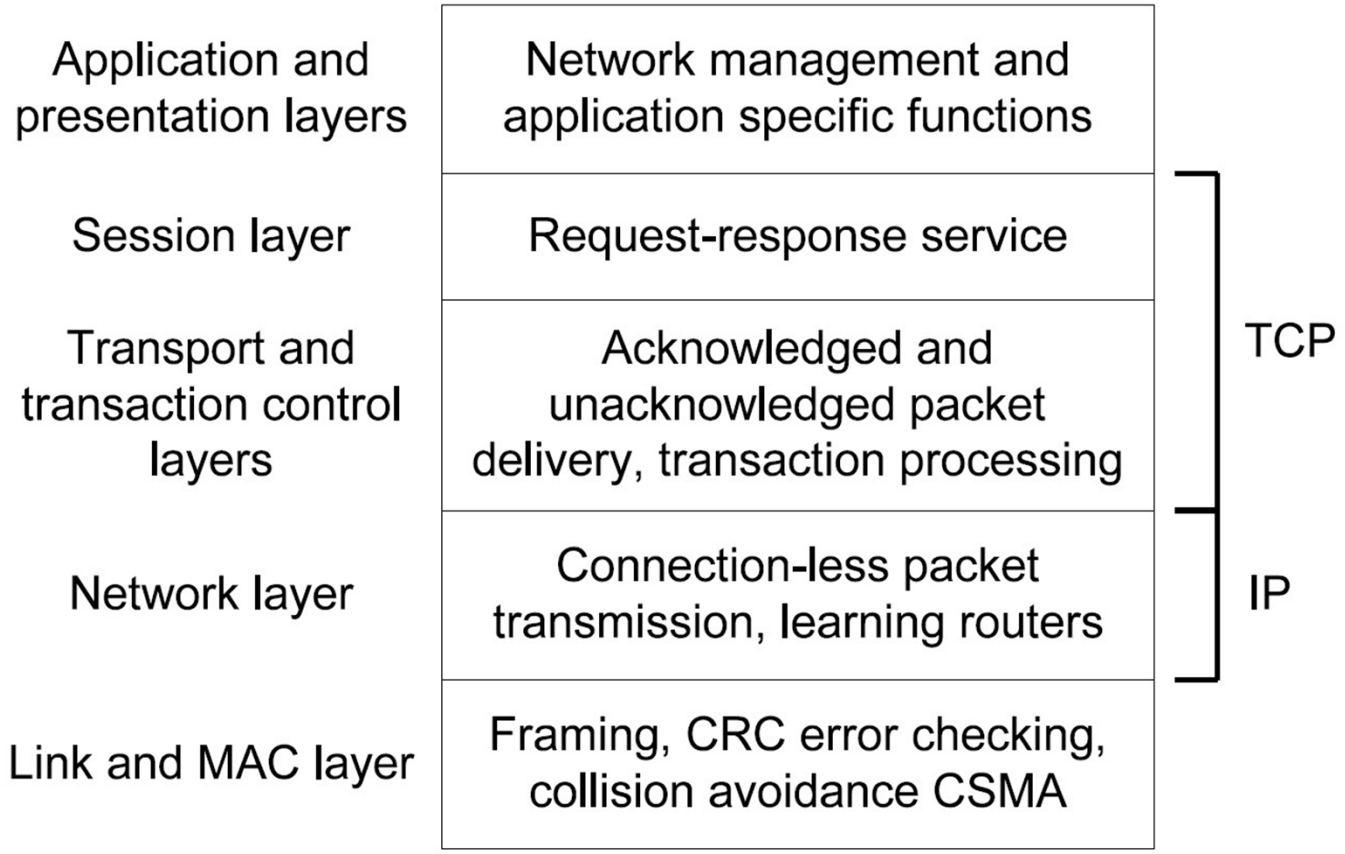


- More details
  - Use Linux embedded virtualization technique (namespaces);
  - Every node is a virtual machine: with its own network stack and process environment;
  - Shared file system;
  - Use Linux Ethernet bridging to communicate;
  - Can simulate wireless networks;
  - Can connect to outside real network devices (for emulation);
  - Support distributed emulation;


Session
Node
Services provided by node
Node
Services provided by node
Node
Services provided by node
Link

- Major challenges
  - Choose a platform;
  - ❖Implement LonTalk in the chosen platform;
  - Interconnection between the cyber and physical systems and how they impact each other;
  - Associate the efforts with educational activities and work force development;

- LonTalk


Application and presentation layers
Network management and application specific functions
Session layer
Request-response service
Transport and transaction control layers
Acknowledged and unacknowledged packet delivery, transaction processing
Network layer
Connection-less packet transmission, learning routers
Link and MAC layer
Framing, CRC error checking, collision avoidance CSMA
TCP
IP

- LonTalk
  - a popular industry standard adopted by US, EU, and China;
  - More than 35 million smart meters are connected through the protocol;
  - For short messages, low bandwidth, and weak processing capabilities;
  - Hierarchical address: (Domain, Sub-net, Node)
  - No routing needed within a subnet

- LonTalk
  - Support multicast through “groups”;
  - Parties communicate through “transactions”: servers can support 16 transactions and slaves can support 2;
  - Acknowledged messages or unacknowledged repeated messages;
  - Support one way authentication of the slaves;

- Add LonTalk into CORE
  - Approach 1: change the network component of CORE or even Linux
    - Difficult and time consuming;
    - Accurate and wide deployment for future;
  - Approach 2: implement LonTalk as a service upon TCP/IP
    - Easy and fast;
    - Extra overhead and encapsulation;

- Either approach will work for our proposed hands-on exercise: DoS, authentication, replay attack, work attack;
- May impact future projects using the system;

- Major challenges
  - Choose a platform;
  - Implement LonTalk in the chosen platform;
    - Interconnection between the cyber and physical systems and how they impact each other;
  - Associate the efforts with educational activities and work force development;

- Three questions need to be answered
  - How can the two systems communicate with each other?
  - What are the possible events → messages → responses?
  - Is there chain effect?

- How can the two systems communicate with each other?
  - CORE IPC API
- What are the possible events → messages → responses?
  - Directly depend on the power grid simulator
- Is there chain effect?
  - Directly depend on the power grid simulator
  - Real clock instead of fake clock;

- Educational materials
  - Course modules
  - Hands-on projects

- Course modules
  - Intro to Smart Grid and its Cyber Security (9 hours)
  - Network Security and Infrastructure Stability (9 hours)
  - Data Security and Privacy in Smart Grid (9 hours)

- Hands-on Projects
  - DoS
  - Authentication
  - Replay attack
  - Worm attack