Privacy-Preserving Data Collection and Access in 802.11s-based Smart Grid Applications

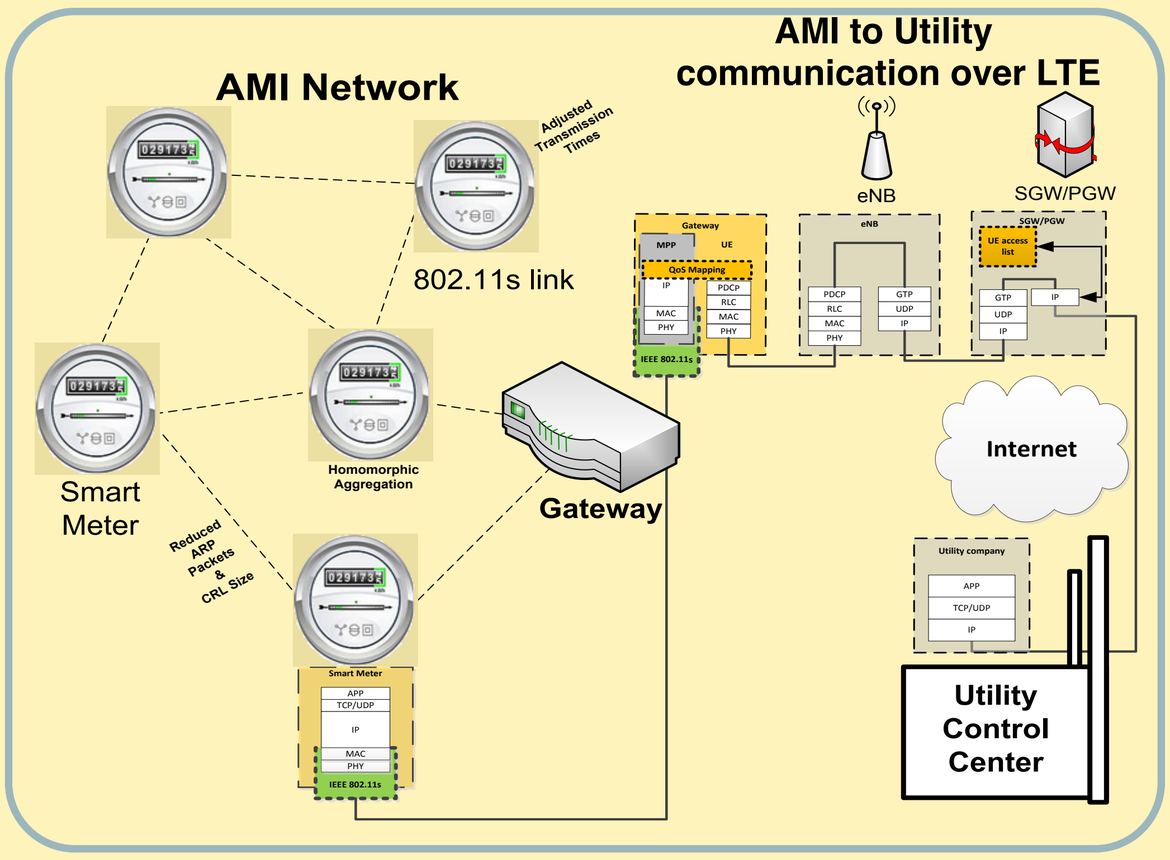
PIs: Kemal Akkaya, Florida International University
Xiuzhen Cheng, The George Washington University
https://adwise.fiu.edu/research-2/smartgridprivacy/

Objectives

- To develop secure, reliable and privacy-preserving data communications protocols for IEEE 802.11s-based Smart Grid Advanced Metering Infrastructure (AMI) applications
- To build a testbed to assess the overhead of the protocols and that can be used by the researchers interested in Smart Grid communications

Approach

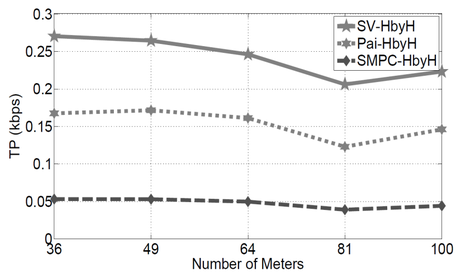
- Optimization of IEEE 802.11s for secure and privacy-preserving Smart Grid AMI data collection
- Adaptation of Fully Homomorphic Encryption (FHE) and Secure Multiparty Computation (MPC) for privacy
- Use of Attribute-based Cryptography for multicasting on AMI
- A Wireless Mesh AMI Network composed of Raspberry PI and Beaglebone Black boards

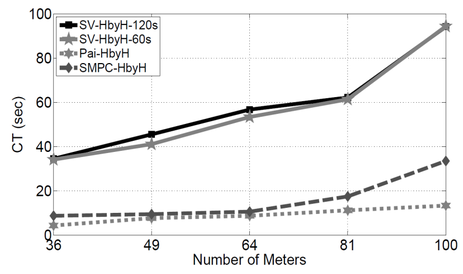


Adaptation of Fully Homomorphic Encryption and Secure Multiparty Computation

- An implementation of Smart-Vercauteren HE scheme used
  - Its feasibility and performance analyzed in an AMI network under TCP
  - Excessive size of encrypted and aggregated data causes packet reassembly problem
- Hierarchical secure MPC proposed
  - Performance comparison with Partially HE and Fully HE

Performance Comparison: FHE vs MPC



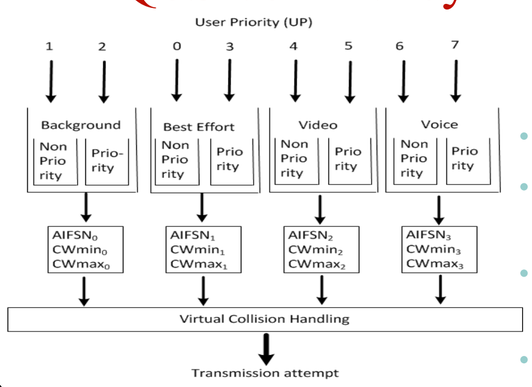


- Secure MPC better than FHE in both throughput and completion time
- Data overhead of FHE approximately five fold of secure MPC

Attribute-based Multicasting

- Firmware updates can target different group of smart meters in an AMI network
- Secure and reliable attribute-based multicast-over-broadcast protocol proposed
  - Access policy defined based on an access tree
  - Access granted if attributes of the user satisfies the access tree

QoS vs Privacy in 802.11s AMI

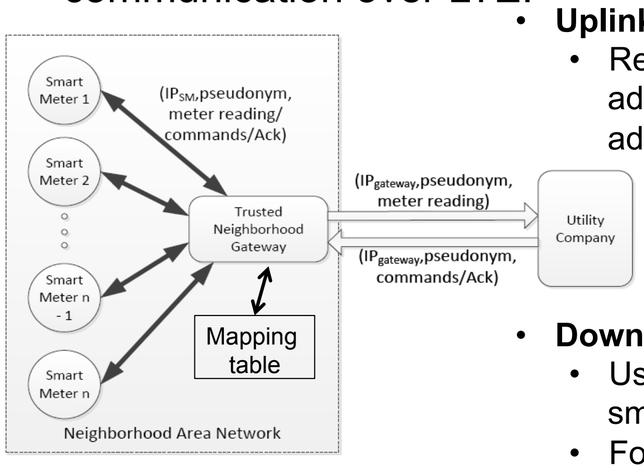


Dual Queue for IEEE 802.11s EDCA for QoS and HE

- EDCA only supports 4 ACs in four queues.
- Secure/Privacy traffic can have higher priority than non-secure/privacy traffic.
- Priority queue (PQ) is added in each AC for priority access .
- Secure/Privacy traffic uses PQ

LTE Integration

- Network Interoperability issues in AMI to UCC communication over LTE:



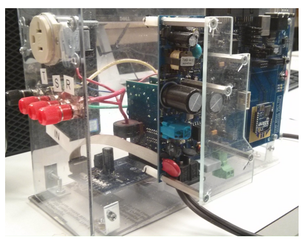
- **Uplink traffic :**
  - Replace smart meter IP address with its IP address, add a pseudonym

Gateway Address Translation

- **Downlink traffic :**
  - Use the pseudonym to find smart meter IP address
  - Forward it to the appropriate Smart meter

AMI Testbed

- An AMI testbed at FIU that integrates with FIU Smart Grid Testbed – actual smart meters
- Raspberry PI, Beaglebone Black and TP-LINK WiFi dongle for communication module
- OpenSSL certificates installed on meters
- Accessible via Internet for experimentation
- Hop-by-hop and End-to-End aggregation methods tested for plaintext, AES and Paillier data



Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

FIU FLORIDA INTERNATIONAL UNIVERSITY
THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC