TCIPG

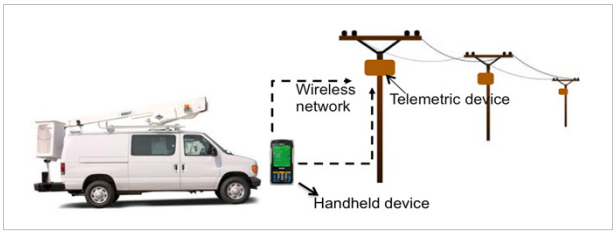
Password-Changing Protocol

SCAPACH: Scalable Password-Changing Protocol

Rehana Tabassum, Haiming Jin, Klara Nahrstedt, Edmond Rogers, and King-Shan Lui

GOALS

- Design fast, cost-effective, scalable, and robust password-changing protocol framework for collecting data from telemetric devices (TD) on pole tops in real-time under varying maintenance scenarios.
  - Ensure unique authentication.
  - Secure the measurements from unauthorized access.
  - Protect against malicious change of data.

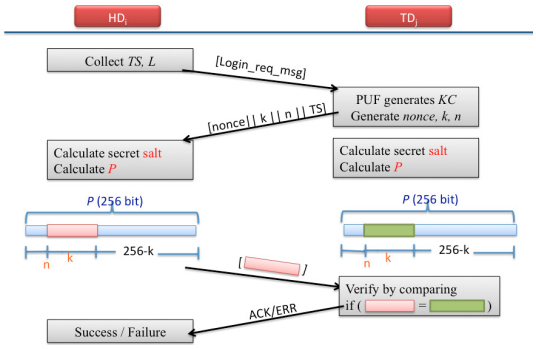


CHALLENGES

- **Scalability:**
  - Large scale of telemetric devices.
  - Telemetric devices are typically secured by simple passwords.
    - Known to many users
    - Large number of devices
- **Security:**
  - Weak passwords and vulnerable authentication protocol.
    - Simple password
    - Long duration of same password
    - Wireless channel for data transmission
    - Continual security reviews and cryptanalysis advancements
- **Resource limitation:**
  - Limited storage and computational capacity of telemetric devices.
  - Lengthy deployment & change management capabilities.

APPROACH

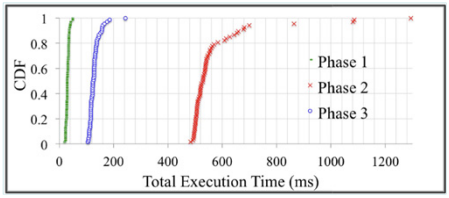
- **Phase 1:** Authentication of **operator** to handheld device (**HD).**
- **Phase 2:**
  - Secure password-changing algorithm for generation of shared key (device password) at each TD/HD device pair.
  - Authentication of HD to TD.



  - Generation of unique, short-lived passwords and symmetric keys with physical information & changeable stored secret.
  - Use of Physical Unclonable Functions (PUFs) to alleviate the load of TD.
- **Phase 3:** Secure communication protocol for exchange of telemetric data from TD to HD.

RESEARCH RESULTS

- SCAPACH is computationally fast
  - Phase 1 execution time: ~26.7 ms
  - Phase 2 execution time: ~600 ms
  - Phase 3 execution time: ~150 ms
  - Network communication delay: 15–20ms



- SCAPACH maintains Perfect Forward Secrecy; secure against different security attacks (e.g., replay attacks, MITM attacks).

BROADER IMPACT

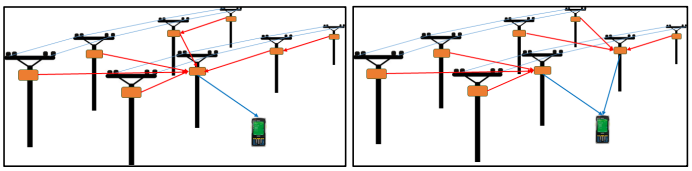
- Allow secure access of data at devices in the field.
- Identify responsible operators in case of insider attacks.
- Ensure good situational awareness.

INTERACTION WITH OTHER PROJECTS

- Trustworthy Framework for Mobile Smart Meters.

FUTURE EFFORTS

- **Cluster-based secure data collection in the smart grid:**
  - Group key pre-distribution.
  - Joint optimal cluster formation and cluster head election.
  - Secure password-changing between TD and HD.



Large cluster size vs. small cluster size

- **Goal:**
  - Improve the **scalability** and **efficiency** of the current version (one-to-one).
- **Challenges:**
  - Group key pre-distribution mechanism needs to be efficient in terms of **computation** and **storage**.
  - The definition of utility function needs to **capture various aspects of performance** that we aim to optimize:
    - Communication overhead among TDs.
    - Limited storage of TDs.
    - Energy efficiency for TDs and HD.
  - Cluster formation and cluster head determination might be **dynamic** and based on network conditions.
  - Algorithms need to be computationally efficient.

Contact Information:
Rehana Tabassum: tabassu2@illinois.edu
Haiming Jin: hjin8@Illinois.edu

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T