TCIPG

Password-Changing Protocol

Secure Data Collection in Smart Grid

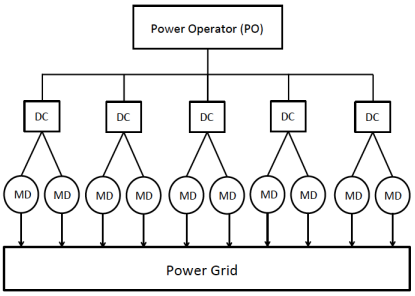
G. Dan, K.-S. Lui, R. Tabassum, Q. Zhu, and K. Nahrstedt

GOALS

- Sensors and measurement devices (MD) should report data securely and efficiently.
- Power operator (PO) cannot establish a secure session with each device to collect data as it is too expensive.
- Power operator delegates data collectors (DC) to collect the data from devices.
- Data collectors can be mobile and subject to security attacks.
- We explore how to **collect the data** from sensors and measurement devices securely and efficiently **via honest but curious data collectors.**

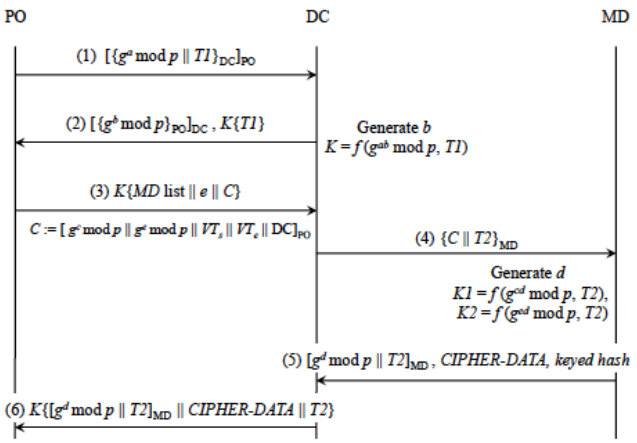
FUNDAMENTAL QUESTIONS/CHALLENGES

- No direct communication between power operator and measurement devices.
- Data collectors are not completely trustworthy and should not be allowed to read the data collected.
- Measurement devices have limited memory and computational capabilities.
- To reduce the storage needed, a power operator (PO) should not have to keep state information per measurement device.
- The protocol should be scalable.
- The protocol should allow trade-offs among memory, computational, and security requirements.



RESEARCH PLAN

- Develop a secure, scalable, and lightweight protocol.
- Assume that each entity has a public and private key pair.
- Adopt Diffie-Hellman protocol to establish session keys.
- Diffie-Hellman session keys support perfect forward secrecy.
- Include timestamps in the messages to detect replay attack.
- Timestamps allow expensive Diffie-Hellman keys to be reused to reduce complexity.
- Allow PO to use a single Diffie-Hellman half key to establish different encryption keys with different MDs.



RESEARCH RESULTS

PROTOCOL DESIGN

- When **PO wants to collect data**, it talks to DC to establish a session key (K) using Diffie-Hellman (DH) key exchange mechanism.
- PO securely provides the following to DC:
  - the list of MDs from which the DC has to collect data,
  - DC's DH private key for talking to MD, and
  - a certificate to present to MD.
- The certificate contains PO's DH public key and DC's public key.

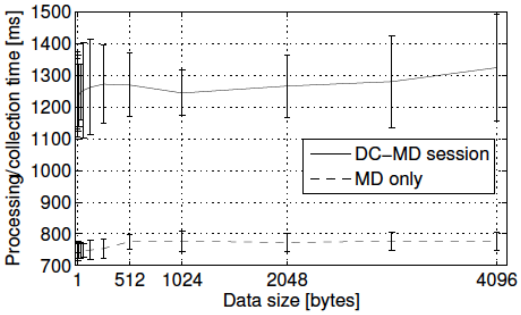
- When **DC presents the certificate to MD**, MD creates its public DH key.
- The same half key is used to:
  - generate an encryption key with PO's DH key to encrypt data that only PO (but not DC) can decrypt, and
  - generate an integrity key with DC's DH key so that DC can detect whether the message has been tampered with.

SECURITY ANALYSIS

- Data are encrypted using a key known only to PO and MD.
- Diffie-Hellman keys provide perfect forward secrecy.
- Timestamps allow detection of replay attacks.
- We formally proved that the protocol is not subject to small subgroup attacks.

COMPLEXITY ANALYSIS

- Expensive DH keys can be reused to reduce the number of expensive operations.
- Simulation results show that the protocol is scalable with the amount of data sent.



BROADER IMPACT

- Data reported by measurement devices are hidden from the data collectors.
- It is safe for data collectors to be mobile nodes that are subject to higher security risks.
- Outsourcing of data collection becomes possible.

INTERACTION WITH OTHER PROJECTS

- Trustworthy Framework for Mobile Smart Meters.

FUTURE EFFORTS

- Extend to multi-layer data collection architecture.
- Apply formal analysis to verify security.
- Implement on real devices to understand computational and memory requirements.
- Explore how to cluster measurement devices for more secure and efficient key management.

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