TCIPG

Password-Changing Protocol

Secure Data Collection in the Smart Grid

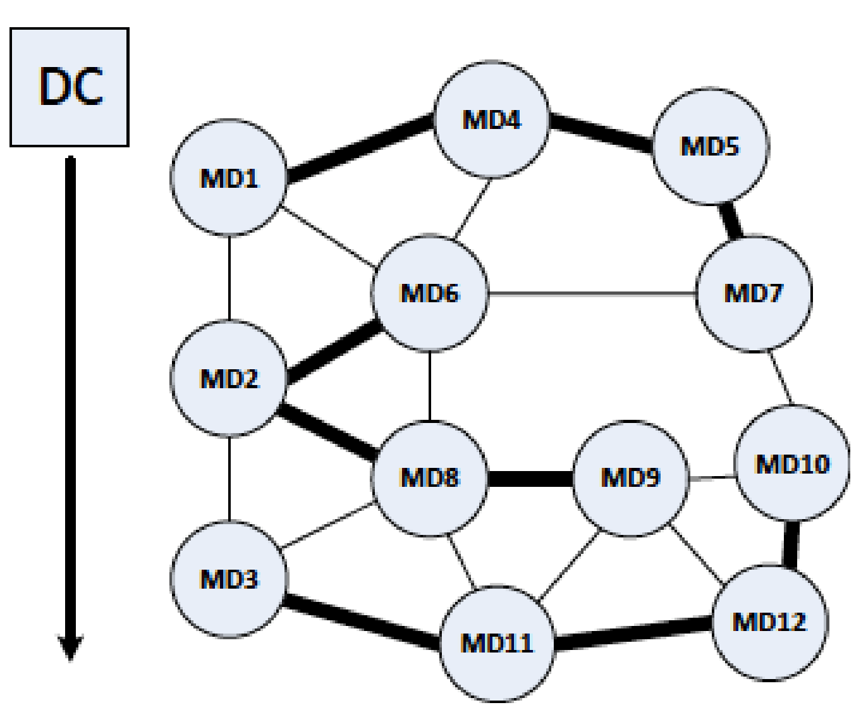
S. Uludag, K.-S. Lui, H. Jin, W. Ren, G. Dan, R. Tabassum, Q. Zhu, and K. Nahrstedt

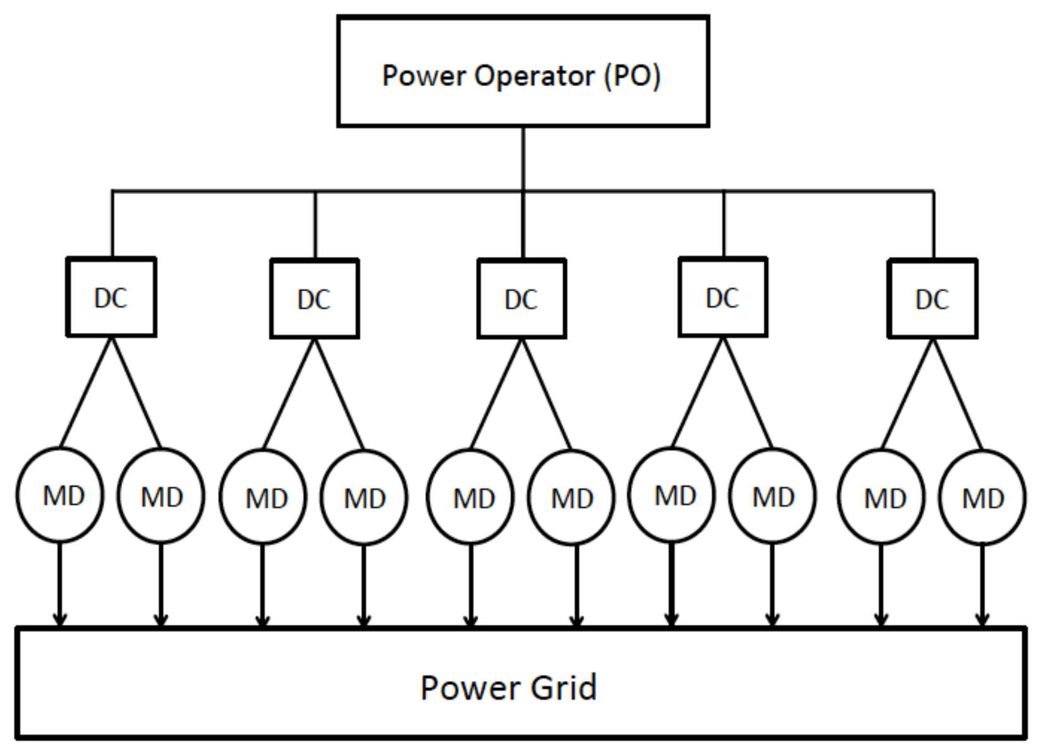
GOALS

- 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.
- PO delegates Data Collectors (DCs) to collect the data from devices.
- DCs may be mobile and subject to security attacks.
- MDs may not have direct contact with DC.
- We explore how to **collect the data** from sensors and measurement devices securely and efficiently **via honest-but-curious data collectors.**
- We study how to **optimize the data collection**.
- To understand the feasibility of implementing the protocol on computationally constrained devices, we **implement our protocol in our test-bed**.

FUNDAMENTAL QUESTIONS/CHALLENGES

- No direct communication between power operator and measurement devices exists.
- Data collectors are not completely trustworthy and should not be allowed to read the data collected.
- Some measurement devices may not have direct connection with a DC, and MDs have to form a tree communication topology.
- Measurement devices have limited memory and computational capabilities.
- To reduce the storage needed, a PO should not have to keep state information per measurement device.
- The protocol should be scalable.
- The protocol should allow trade-offs among data collection time, memory, computational, and security requirements.



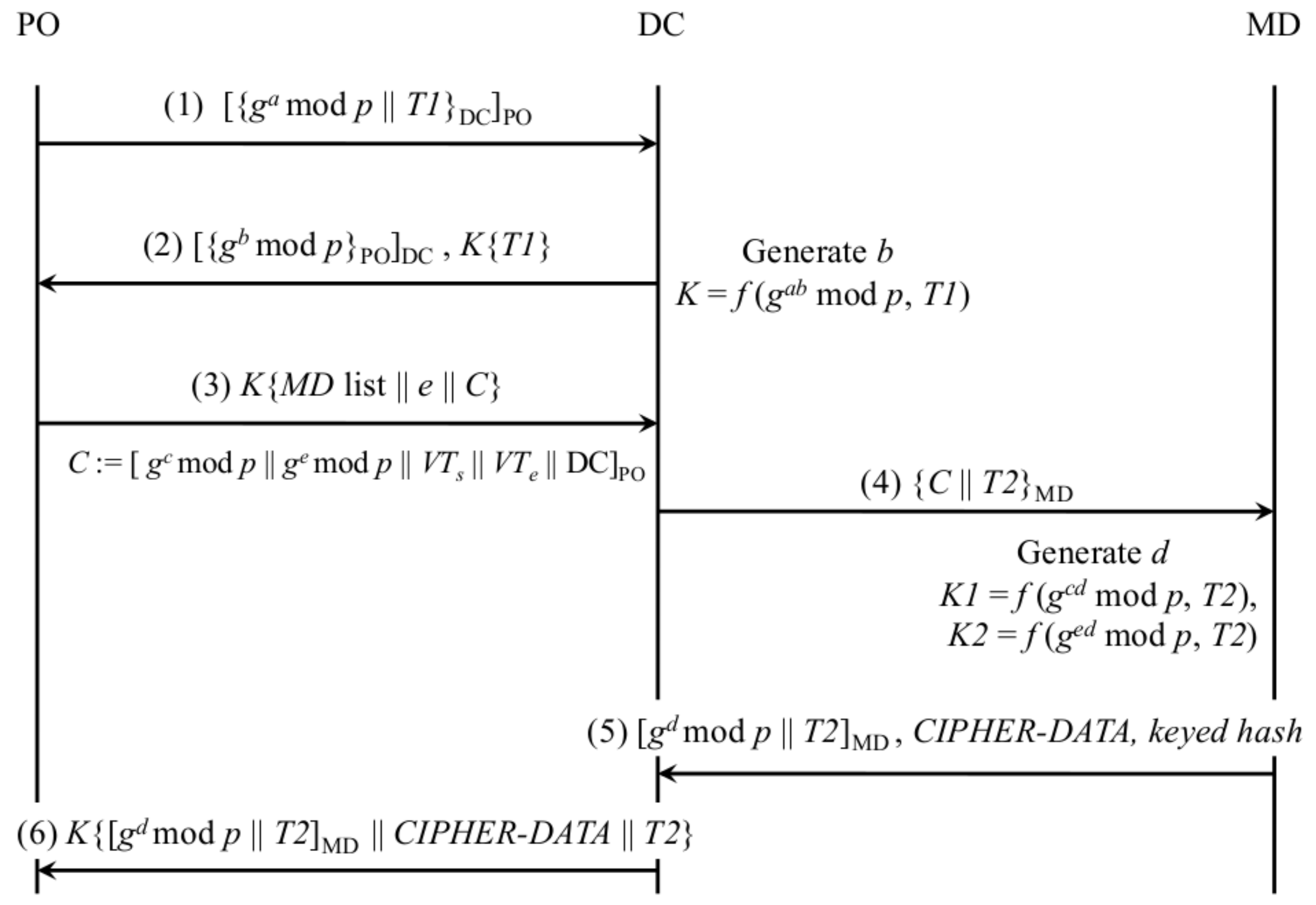


RESEARCH PLAN

- Develop secure, scalable, and lightweight protocols for data collection and command delivery in different scenarios.
- 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 attacks.
  - 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.
  - Diffie-Hellman keys are also used for immediate nodes for relaying data.
- Study the time needed for data collection that depends on network delay and computational time.
- Study which trees to use for MDs to report data in a multi-hop manner.
- Study the DC-MD association as an optimization problem.
- Study whether the mechanisms are feasible in computationally constrained devices.

RESEARCH RESULTS

PROTOCOL DESIGN


PO

DC

MD

(1) $[\{g^a \bmod p \parallel T1\}_{DC}]_{PO}$

(2) $[\{g^b \bmod p\}_{PO}]_{DC}$, $K\{T1\}$

Generate b
$K = f(g^{ab} \bmod p, T1)$

(3) $K\{MD \text{ list} \parallel e \parallel C\}$

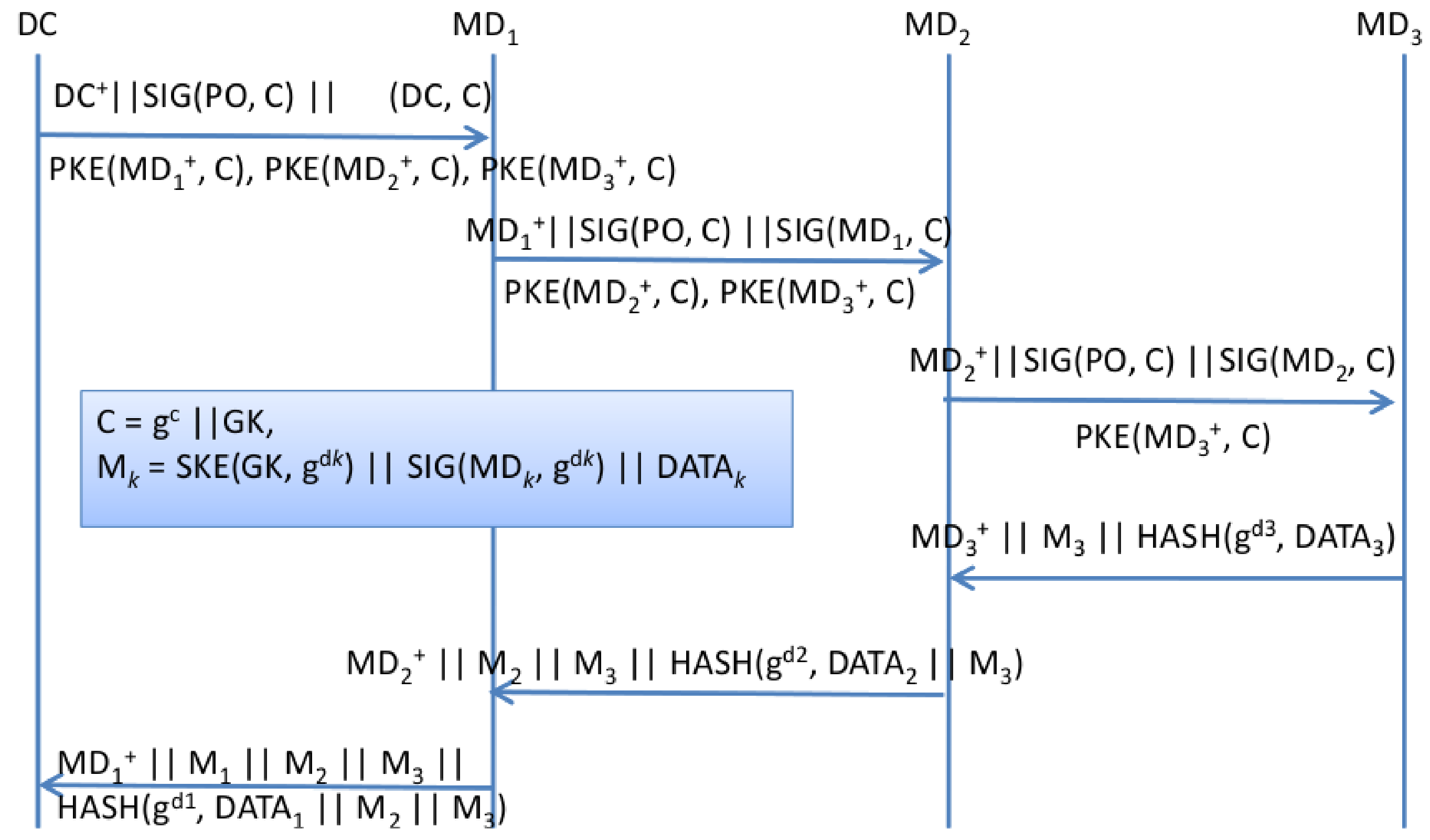
$C := [\, g^c \bmod p \parallel g^e \bmod p \parallel VT_s \parallel VT_e \parallel DC]_{PO}$

(4) $\{C \parallel T2\}_{MD}$

Generate d
$K1 = f(g^{cd} \bmod p, T2)$,
$K2 = f(g^{ed} \bmod p, T2)$

(5) $[g^d \bmod p \parallel T2]_{MD}$, *CIPHER-DATA, keyed hash*

(6) $K\{[g^d \bmod p \parallel T2]_{MD} \parallel CIPHER\text{-}DATA \parallel T2\}$


DC

MD_1

MD_2

MD_3

$DC^+ || SIG(PO, C) ||$ (DC, C)
$PKE(MD_1^+, C), PKE(MD_2^+, C), PKE(MD_3^+, C)$

$MD_1^+ || SIG(PO, C) || SIG(MD_1, C)$
$PKE(MD_2^+, C), PKE(MD_3^+, C)$

$MD_2^+ || SIG(PO, C) || SIG(MD_2, C)$
$PKE(MD_3^+, C)$

$C = g^c || GK,$
$M_k = SKE(GK, g^{dk}) || SIG(MD_k, g^{dk}) || DATA_k$

$MD_3^+ || M_3 || HASH(g^{d3}, DATA_3)$

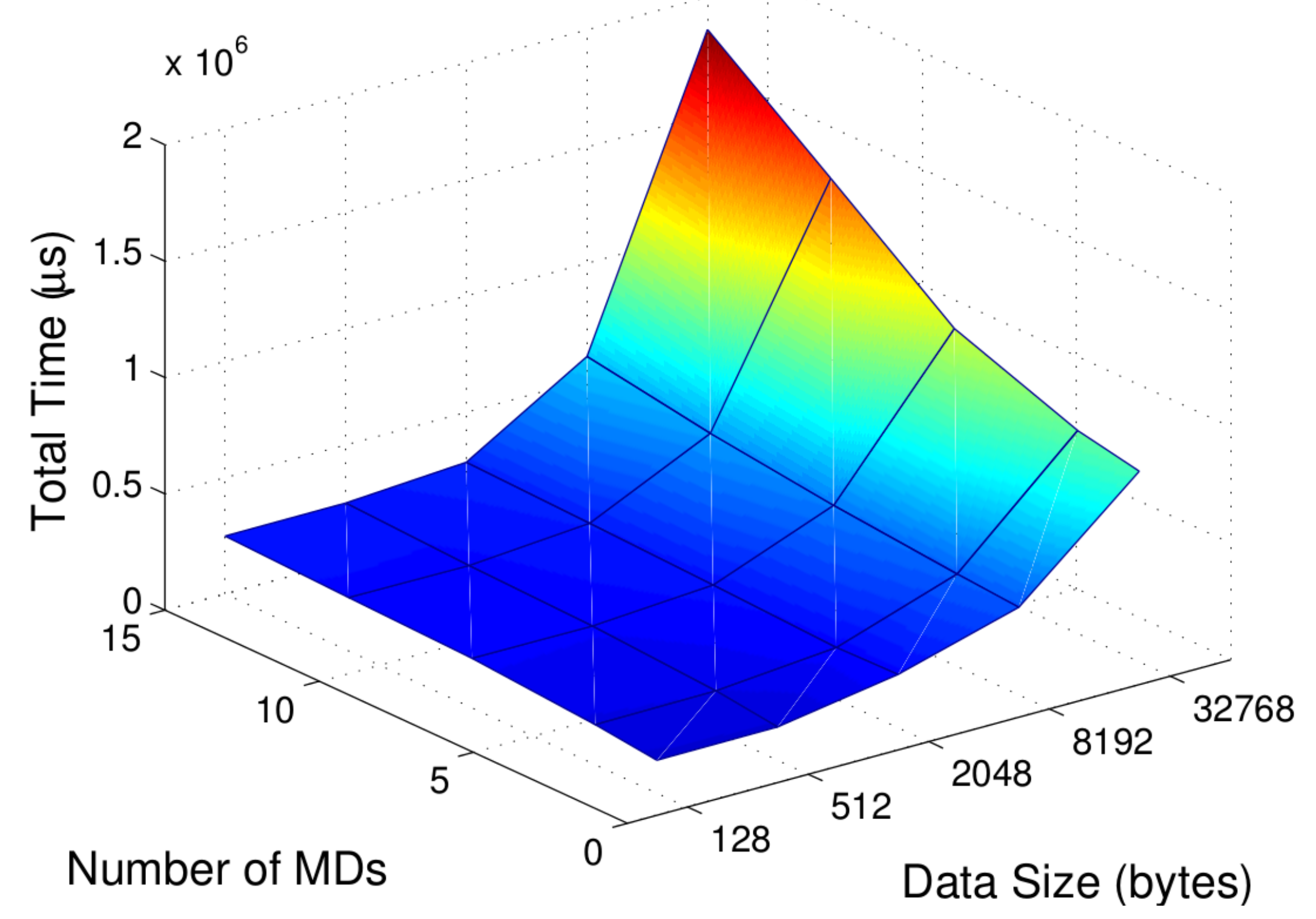
$MD_2^+ || M_2 || M_3 || HASH(g^{d2}, DATA_2 || M_3)$

$MD_1^+ || M_1 || M_2 || M_3 ||$
$HASH(g^{d1}, DATA_1 || M_2 || M_3)$

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 prove that the protocol is not subject to small subgroup attacks.

COMPLEXITY ANALYSIS



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

- Perform more complete security analysis and test-bed studies.
- Continue to study the optimization problem on balancing data collection time and security.
- Study the long-term key management issue.

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T