Resilient and Scalable Data Collection in Energy Distribution Networks

Tianyuan Liu, King-Shan Lui, and Klara Nahrstedt

MOTIVATION

- Failures in energy distribution networks (EDN) can cause enormous damage but are difficult to monitor.
- Although sensors are deployed along the pipelines for safety purposes, these sensors are vulnerable to incidents, natural events, or malicious attacks.
- Mechanisms to detect or tolerate sensor failures in EDN are desirable.

PROBLEM DESCRIPTION

- Our goal is to design a data collection protocol in EDN that is:
  - fast and scalable;
  - resilient, in that it guarantees data availability at a sensor as long as the sensor does not fail; and
  - secure, such that it (1) prevents eavesdropping of data, and (2) ensures integrity of data.
- We consider the following scenario in our protocol:
  - An "honest-but-curious" mobile data collector (DC) collects data from pipeline sensors (PSs), and eventually delivers data to a pipeline manager (PM).
  - Sensors can fail in any stage of the protocol.

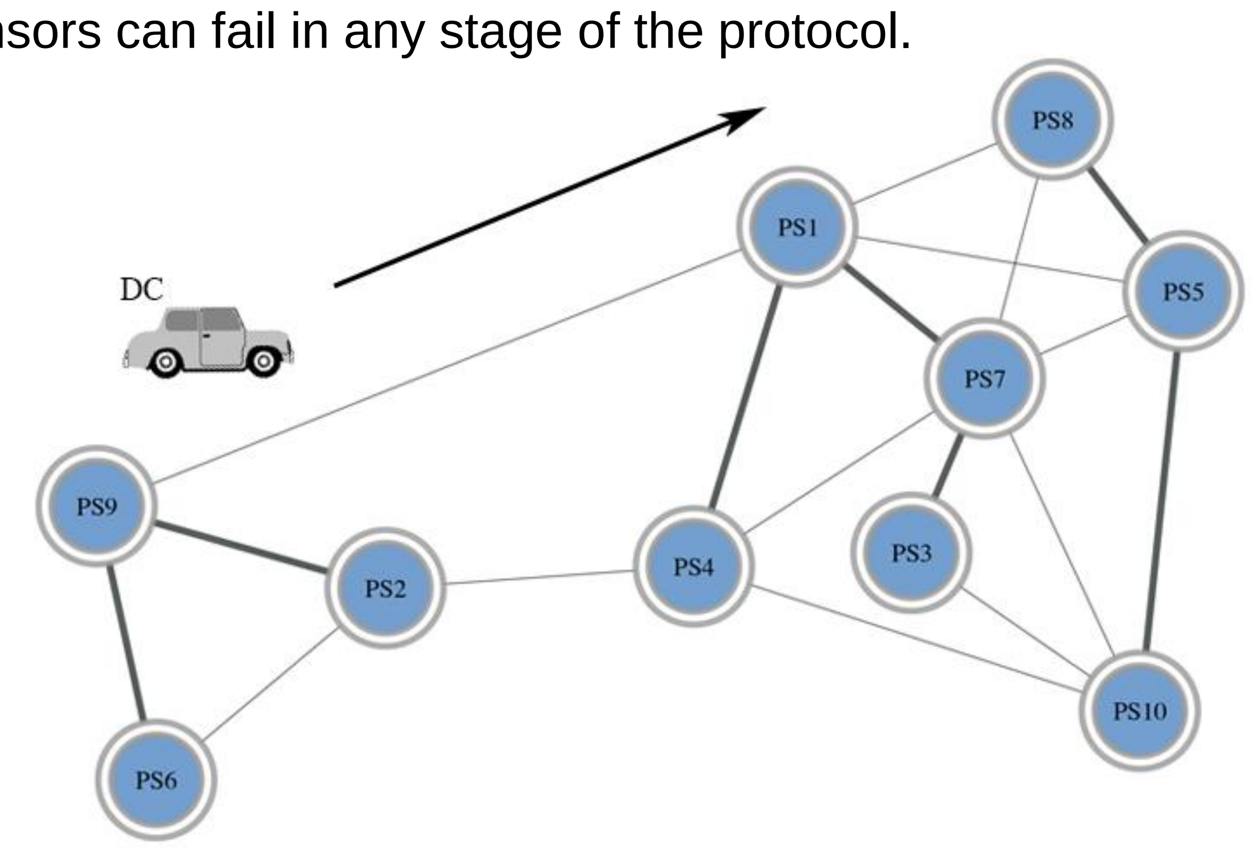

Fig. 1. Data Collection in EDN

RELATED APPROACHES

- Secure tree-based data collection protocol in the smart grid [1].
- Scenario: in smart grid, data collector (DC) collects data from measurement devices (MD) and delivers to power operator (PO).

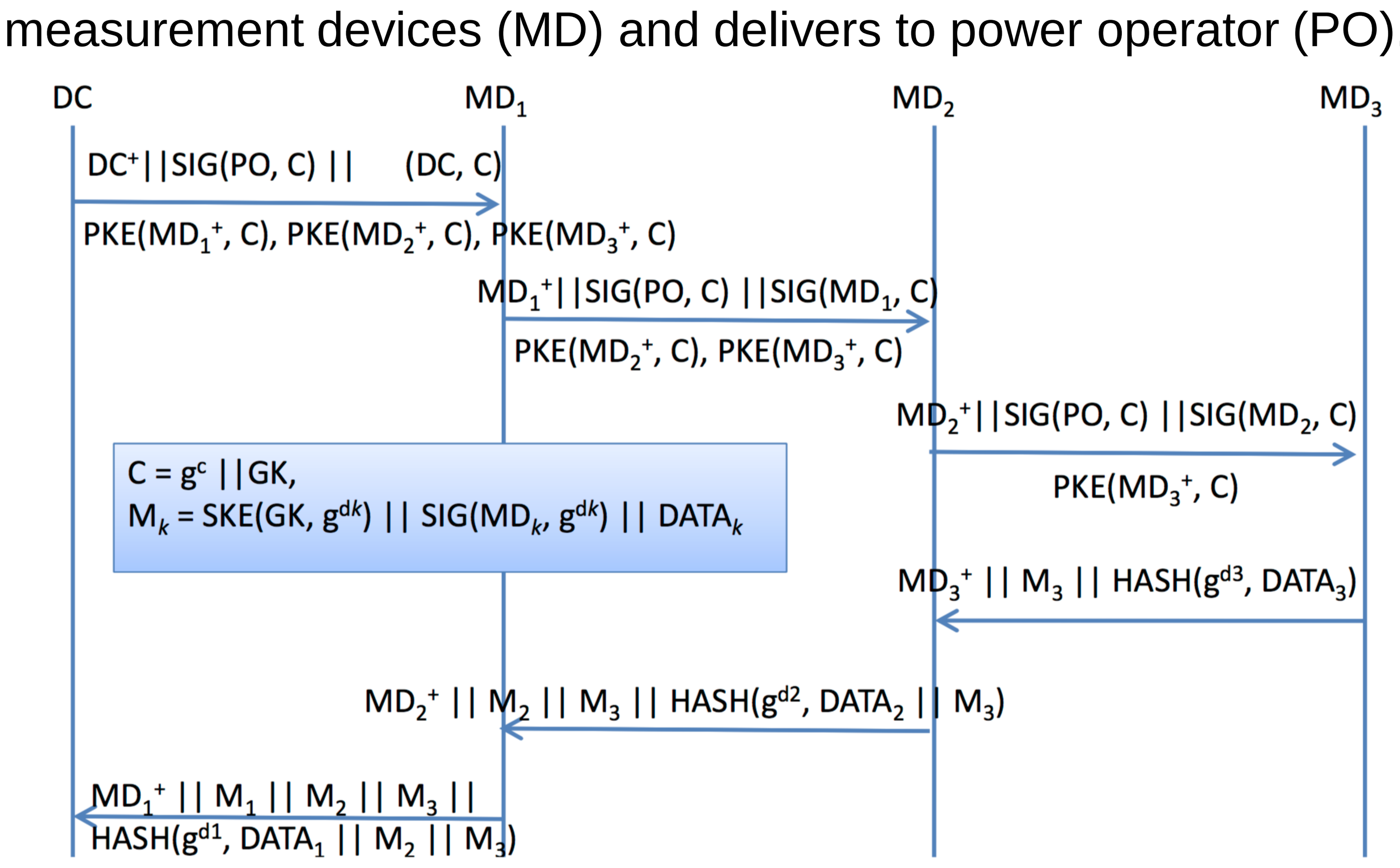

Fig. 2. Data Collection on a Tree Branch

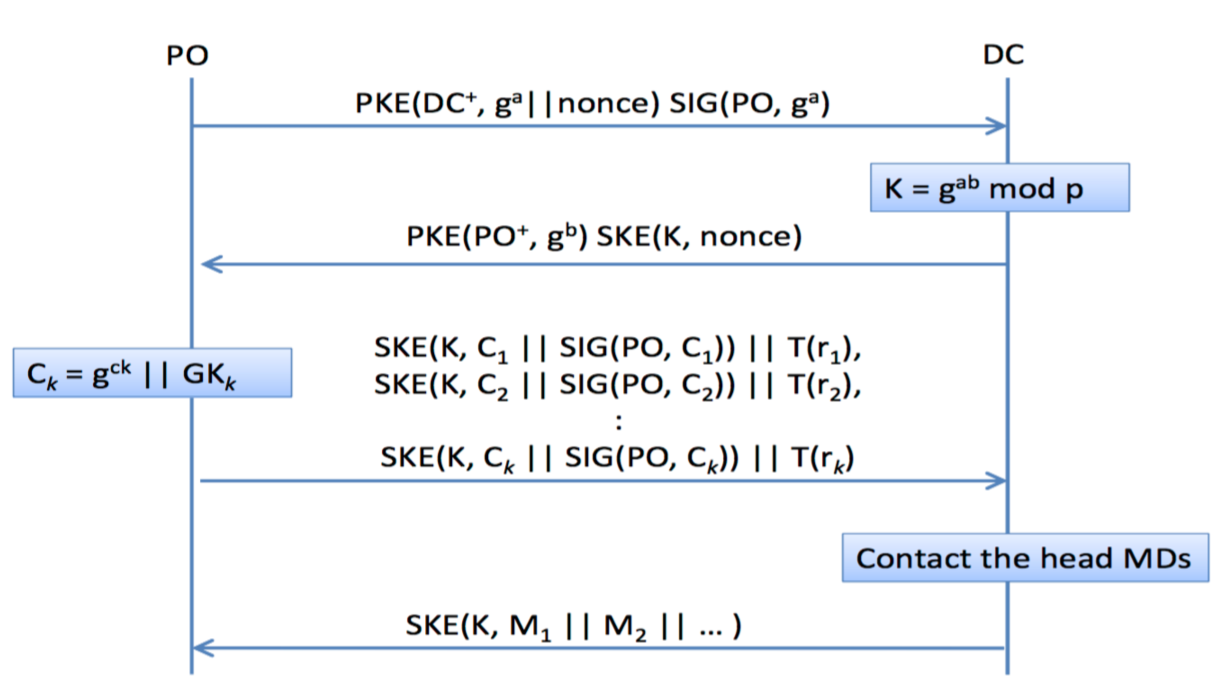

Fig. 3. Communication Between PO and DC

[1] Haiming Jin, et al. "Secure data collection in constrained tree-based smart grid environments." *Proc. 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2014.

RESEARCH PLAN

- Formulate resilient data collection as a tree-based disjoint-path backup integer optimization problem, referred to as the *Resilient Tree Collection (RTC)* problem.
- Provide an algorithm to solve the optimization problem.
- Design a protocol to achieve secure and scalable data collection with/without failure.
- Evaluate the performance of the data collection scheme on real-world dataset.

RESILIENT TREE COLLECTION (RTC)

- Notation

	Notation	Description
Constants	$G = \langle \mathcal{R}, \mathcal{S}, \mathcal{E} \rangle$	G-directed graph, $\mathcal{R}$-set of candidate roots, $\mathcal{S}$-set of PSs, $\mathcal{E}$-set of links
	$c_{i,j}$	Energy consumption of transmitting 1 bit through link (i, j).
	$p_{i,j}$	Probability that link (i, j) fails.
	N_{th}	Maximum number of nodes that can share a group key.
Variables	$x^s_{i,j}$	$= 1$ if link (i, j) is in the primary path of PS s; $= 0$ otherwise.
	$y^s_{i,j}$	$= 1$ if link (i, j) is in the backup path of PS s; $= 0$ otherwise.

- Formulation

$$\min \sum_{j\in\mathcal{R}} \sum_{m\in\mathcal{S}} \left(p^s x^s_{i,j} + (1-p^s) y^s_{i,j}\right) c_{i,j},$$

$$\text{s.t.} \sum_{i\in\mathcal{S}} x^s_{i,n} - \sum_{i\in\mathcal{S}\cup\mathcal{R}} x^s_{n,i} = \begin{cases} -1 & \text{if } n = s \\ 0 & \text{if } n \neq s \end{cases}, \ \forall s \in \mathcal{S}, \forall n \in \mathcal{S}, \qquad \text{Flow}$$

$$\sum_{n\in\mathcal{R}} \sum_{i\in\mathcal{S}} x^s_{i,n} = 1, \ \forall s \in \mathcal{S},$$

$$x^s_{i,j} + y^s_{i,j} \le 1, \ \forall s \in \mathcal{S}, \forall (i, j) \in \mathcal{E}, \qquad \text{Disjoint}$$

$$x^s_{i,j} \le x^i_{i,j}, \ \forall s \in \mathcal{S}, \forall (i, j) \in \mathcal{E},$$

$$\sum_{i,s\in\mathcal{S}} x^s_{i,j} + y^s_{i,j} \le N_{th}, \ \forall j \in \mathcal{R} \qquad \text{Security}$$

where $p^s = \prod_{(i,j)\in\mathcal{E}} (1 - p^s_{i,j} x_{i,j})$.

ALGORITHM

- Solve RTC (NP-hard) by rounding relaxation linear programming.

Algorithm 1: Rounding Relaxation for RTC

Input: $G, \{c_{i,j}\}, \{p_{i,j}\}, N_{th}$
Output: $\{x^m_{i,j}\}, \{y^m_{i,j}\}$

while *true* **do**
  Solve LP relaxation for RTC, get optimal solution $\{x^{m*}_{i,j}\}, \{y^{m*}_{i,j}\}$;
  Set $x^s_{i,j} \leftarrow 0$ for all $x^{m*}_{i,j} = 0$, $y^s_{i,j} \leftarrow 0$ for all $y^{m*}_{i,j} = 0$;
  Set $x^s_{i,j} \leftarrow 1$ (or y) for the largest $x^{m*}_{i,j}$ (or y);
  if *all* $\{x^s_{i,j}\}, \{y^s_{i,j}\}$ *are set* **then**
    break;
  end
end
return $\{x^s_{i,j}\}, \{y^s_{i,j}\}$

FUTURE EFFORTS

- Design protocol to achieve secure and scalable data collection under failure.
- Evaluate the performance of proposed scheme on real-world dataset.
- Consider dynamic scheduling under failure.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY