Resilient Framework with Authentication, Key Management, and Data Collection for Energy Sensors in Energy Distribution Networks

Website: http://cred-c.org/researchactivity/authkeycollect

Researchers (Illinois): Tianyuan Liu and Klara Nahrstedt; External Collaborators (Hong Kong University): Hongpeng Guo and King-Shan Lui

Industry Collaboration:

- Currently seeking collaborators from industry, power utilities, or national labs who would like to collaborate with us on trusted sensor networks that allow access to the information about the situation awareness and health of power, oil and gas physical infrastructures (power lines, gas pipelines, refineries).
- Contact Klara Nahrstedt to discuss how we can exchange ideas or collaborate with our team.

Description of research activity: Resiliency in Energy Delivery Systems (EDS) is a big challenge. For example, in the EDS distribution system for oil and gas, since the pipelines are usually buried underground (e.g., in city gas distribution network), it is hard to perform periodic inspection without a maintenance dig. But, such digs are not scalable, and are costly in terms of human effort. Digital sensing is a promising replacement to a maintenance dig. Such sensors can be deployed inside or outside a pipeline to perform measurement of pressure, temperature, and presence of hydrocarbons, and thus detect pipeline failures. In the case of power-lines, similar challenges exist as with pipelines and gas-lines where digital sensors are deployed to enable monitoring of health of power-lines. Nevertheless, such sensors are vulnerable to failures and attacks. On one hand, it is often the case that when damage happens to the pipeline, either these sensors become unresponsive at the same time, or they send false information. Furthermore, data reported by sensors is subject to eavesdropping and tampering by attackers.

In this activity, we focus on developing a **resiliency framework for sensors networks and data collection in Energy Distribution Networks (EDN).** This is a large space since this resiliency framework includes different dimensions of the end-to-end resilience framework. The resiliency framework includes authentication protocols and real-time key management for different sensors (e.g., valves, pumps, and gas meters) and diverse O&G network topologies, as well as context-aware adaptive routing and transmission protocols for collecting control data from sensors to ensure resilient data collection under failures.

This activity is a long-term activity and will be solved in systematic phases:

Phase 1: Investigate resilience (authentication, key management, trusted data collection) for energy sensors which are wirelessly connected in a tree formation for gas, oil pipelines, and power-lines.

Phase 2: Investigate resilience for networks of energy sensors in other wireless sensor topologies and evaluate which topologies are most robust for gas, oil pipelines, and power-lines.

Phase 3: Investigate resiliency and security in the monitoring system for energy sensors, with an emphasis on authentication, provenance, and verification techniques.

The ultimate goal is to create a resiliency framework for energy sensors in energy delivery physical infrastructures. The framework considers gas, oil, and power-grid networks where the energy sensors provide the insights into the health of the energy physical infrastructures such as networks of gas & oil pipelines, and power-lines, and energy usage network, even in the presence of a cyber-attack on the EDS infrastructure. The results of the resilient framework are protocols and software functions for sensors, as well as algorithms to provide appropriate placement of sensors over different oil & gas topologies where sensor nodes have various capabilities. These results can be parts of planning tools. For example, one planning tool could be as follows. We take a pipeline topology with different sensor network capabilities and failures types, and after running the planning tool, we can visualize where weak points may occur if certain sensor

placement over given topology is employed, and what sensor measurements one can see under given failures and attacks if our resilient protocols would be deployed.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
Our resilient framework addresses the "development and implementation of new protective measures to reduce risk" as well as "sustainability of security improvements" in the road map.

New protective measures to reduce risks: With our resilient framework, we are developing *new protocols among sensor networks and new software primitives residing within sensors*, which collect sensor measurements from oil pipelines and forward these to the data collection nodes and control centers for an operator to assess the health of pipelines. The new protocols and software functions utilize new capabilities such as different ranges of wireless network technology (e.g., some of the sensors have short-range transmission capabilities, some sensors have long-range transmission capabilities) and we investigate the placement of sensors with different transmission capabilities with the ultimate goals of resiliency against physical damage or cyber-attacks on sensors. Furthermore, the new protocols and functions utilize new capabilities such as "array of things" where multiple IoT (Internet of Things) devices (e.g., temperature, pressure, GPS, wind velocity) cluster together in one sensor node (box) of the pipeline sensor network, providing auxiliary information to each other. This approach allows the sensors to achieve better resilience against failures because not all IOT devices may be attacked at the same time or fail at the same time. Hence, each sensor node with multiple IoT devices has diverse contextual information to make advanced decisions how to route if some IoT devices fail.

Security improvements: One important aspect of introducing *array of things as a sensor node* is that one can upgrade the sensor node gradually by replacing individual IoT devices and sustain security improvements as IoT device technology advances.

Summary of EDS gap analysis: Although sensors are widely deployed in EDS (transmission and distribution, oil & gas networks), the sensors, i.e., energy-specific cyber-metadata collectors, are themselves vulnerable to failure and attacks. If the EDS is attacked, these sensors become unresponsive, with the result that either the incident cannot be reported to the control center, or they reveal false information.

This activity addresses physical failures and cyber-attack-induced failures in EDS sensor and secure data collection networks by designing an authentication and data collection framework so as to enhance the responsiveness of EDS sensors (e.g., valves and pumps in transmission O&G networks and SCADA gas meters in distribution O&G networks).

Full EDS gap analysis: Tree-based Data collection in sensor networks has been actively studied [1], [6], and [7]. Most work aims at optimizing energy usage or sensor lifetime while reducing data reporting latency. Due to the massive number of sensors, a hierarchical data collection structure is usually adopted. Cluster heads are selected to collect data from sensors within their neighborhoods, and then report the data to the data sink. Some recent studies on how to select cluster heads to balance energy and latency can be found in [8], [9]. As energy harvesting has been proposed to prolong the lifetime of a sensor, some researchers study data collection with this emerging technology [10], [11]. To reduce traffic, compression techniques are studied to improve the data collection performance [2], [12]. To the best of our knowledge, there is no representative study on resilient data collection in sensor networks that can be applied in our EDS data collection scenario when considering topologies in refineries or other oil & gas infrastructure settings. Data collection in smart grids has been studied from the security and data aggregation aspects. Nevertheless, there are not many studies on resiliency identified. [13] Studies where to put extra relay nodes to provide fault tolerance in the overhead transmission lines. Since the topology of the transmission grid is linear, the mechanism cannot be applied in the tree structure. [14] Considers the robustness of data collection in advanced metering infrastructure. Similar to our work, data are collected through a tree structure. A primary tree is first built and then backup links are identified to provide resilience. The proposed algorithm aims at finding the minimum set of links to form the resilience tree. The authors in [15] study the performance of different backup parent selection mechanisms. Our work differs from these works in two aspects: first, [14], [15] focus on backup selection in single tree structure and assume that tree root does not fail. However, in our approach, we aim at selecting backup parents among multiple trees, i.e., we consider a forest of trees, and we assume tree roots can be faulty. Second, besides the connectivity issue, we also consider other objectives

and constraints in backup mechanisms such as security and latency. In our prior TCIPG work [16], we considered secure protection approaches against attacks on sensor networks that monitor power lines for a smart grid and collect data from these sensor networks. However, power lines create simpler 2D topologies for sensor networks than 3D topologies in oil refineries, hence enhanced secure data collection framework needs to be developed.

Regarding failures for oil and gas sensor network, we consider scenarios ranging from single failures/attacks on a single tree to cascaded failures of the outdoor sensing infrastructure (e.g., in refineries). From the operator's point of view in the control center, the failure of multiple outdoor sensors due to, for example, a fire, and the failure of multiple outdoor sensors due to cascaded cyber-attacks looks the same. Often, from the control center it is not clear if sensor failure cause is due to physical phenomena or to a cyber-attack. The DOE Roadmap and the NESCOR failure scenarios are not sufficient as foundations to promote resilience in O&G sensing and data collection. Our failure models consider physical phenomena that can cause sensor failures of the cyber-physical sensing infrastructure. It would be interesting if a similar document as the document with NESCOR failure scenarios were to appear for oil & gas infrastructures.

Bibliography:

1. O. D. Incel, A. Ghosh, B. Krishnamachari, and K. Chintalapudi, "Fast data collection in tree-based wireless sensor networks," IEEE Transactions on Mobile computing, vol. 11, no. 1, pp. 86–99, 2012.
2. Y. Yao, Q. Cao, and A. V. Vasilakos, "Edal: An energy-efficient, delayaware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks," Networking, IEEE/ACM Transactions on, vol. 23, no. 3, pp. 810–823, 2015.
3. J. D. Rhodes, C. R. Upshaw, C. B. Harris, C. M. Meehan, D. A. Walling, P. A. Navr´atil, A. L. Beck, K. Nagasawa, R. L. Fares, W. J. Cole et al., "Experimental and data collection methods for a large-scale smart grid deployment: Methods and first results," Energy, vol. 65, pp. 462–471, 2014.
4. Q. Chen, D. Kaleshi, and Z. Fan, "Reconsidering the smart metering data collection frequency for distribution state estimation," in Proc. of IEEE SmartGridComm, 2014.
5. H. Gao, X. Fang, J. Li, and Y. Li, "Data collection in multi-application sharing wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, Frebuary 2015.
6. C.-T. Cheng, N. Ganganath, and K.-Y. Fok, "Concurrent data collection trees for iot applications," IEEE Transactions on Industrial Informatics, 2016.
7. J. Fei, H. Wu, and W. Y. Alghamdi, "Lifetime and latency aware data collection based on k-tree," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on. IEEE, 2015, pp. 1–6.
8. R. Zhang, J. Pan, D. Xie, and F. Wang, "NDCMC: A hybrid data collection approach for large-scale wsns using mobile element and hierarchical clustering," IEEE Internet of Things Journal, to appear.
9. Z. Xu, L. Chen, C. Chen, and X. Guan, "Joint clustering and routing design for reliable and efficient data collection in large-scale wireless sensor networks," IEEE Internet of Things Journal, to appear.
10. A. Mehrabi and K. Kim, "Maximizing data collection throughput on a path in energy harvesting sensor networks using a mobile sink," IEEE Transactions on Mobile Computing, vol. 15, no. 3, March 2016.
11. C. Wang, S. Guo, and Y. Yang, "An optimization framework for mobile data collection in energy-harvesting wireless sensor networks," IEEE Transactions on Mobile Computing, to appear.
12. X.-Y. Liu, Y. Zhu, L. Kong, C. Liu, Y. Gu, A. V. Vasilakos, and M.-Y. Wu, "Cdc: Compressive data collection for wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 8, August 2015.
13. K. Wang, X. Qiu, S. Guo, and F. Qi, "Fault tolerance oriented sensors relay monitoring mechanism for overhead transmission line in smart grid," Sensors Journal, IEEE, vol. 15, no. 3, pp. 1982–1991, 2015.
14. J. Kamato, L. Qian, W. Li, and Z. Han, "Biconnected tree for robust data collection in advanced metering infrastructure," in Proc. of IEEE WCNC, 2015.

15. J. Silber, S. Sahu, J. Singh, and Z. Liu, “Augmenting overlay trees for failure resiliency,” in Proc. of IEEE Globecom, 2004.
16. H. Jin, S. Uludag, K.-S. Lui, and K. Nahrstedt, “Secure data collection in constrained tree-based smart grid environments,” in Proc. of IEEE SmartGridComm, 2014.
17. R. C. Prim, “Shortest connection networks and some generalizations,” Bell system technical journal, vol. 36, no. 6, pp. 1389–1401, 1957.