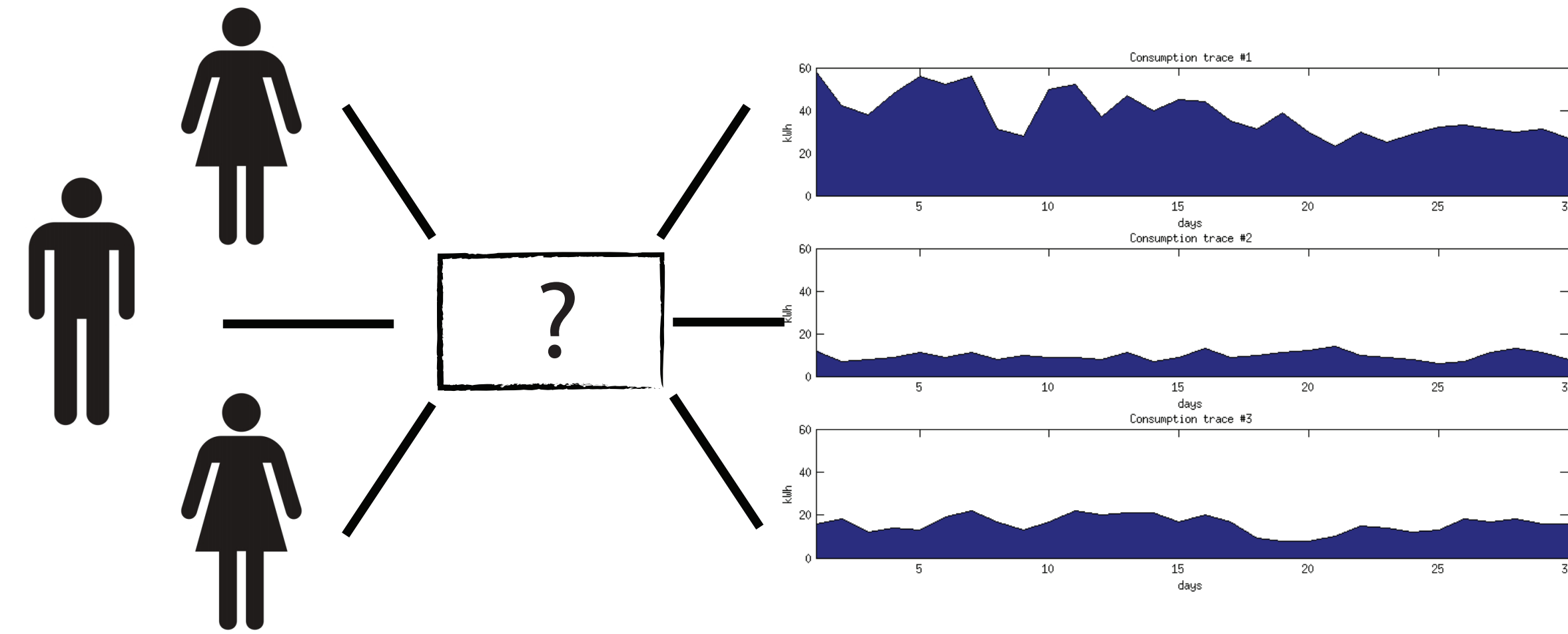
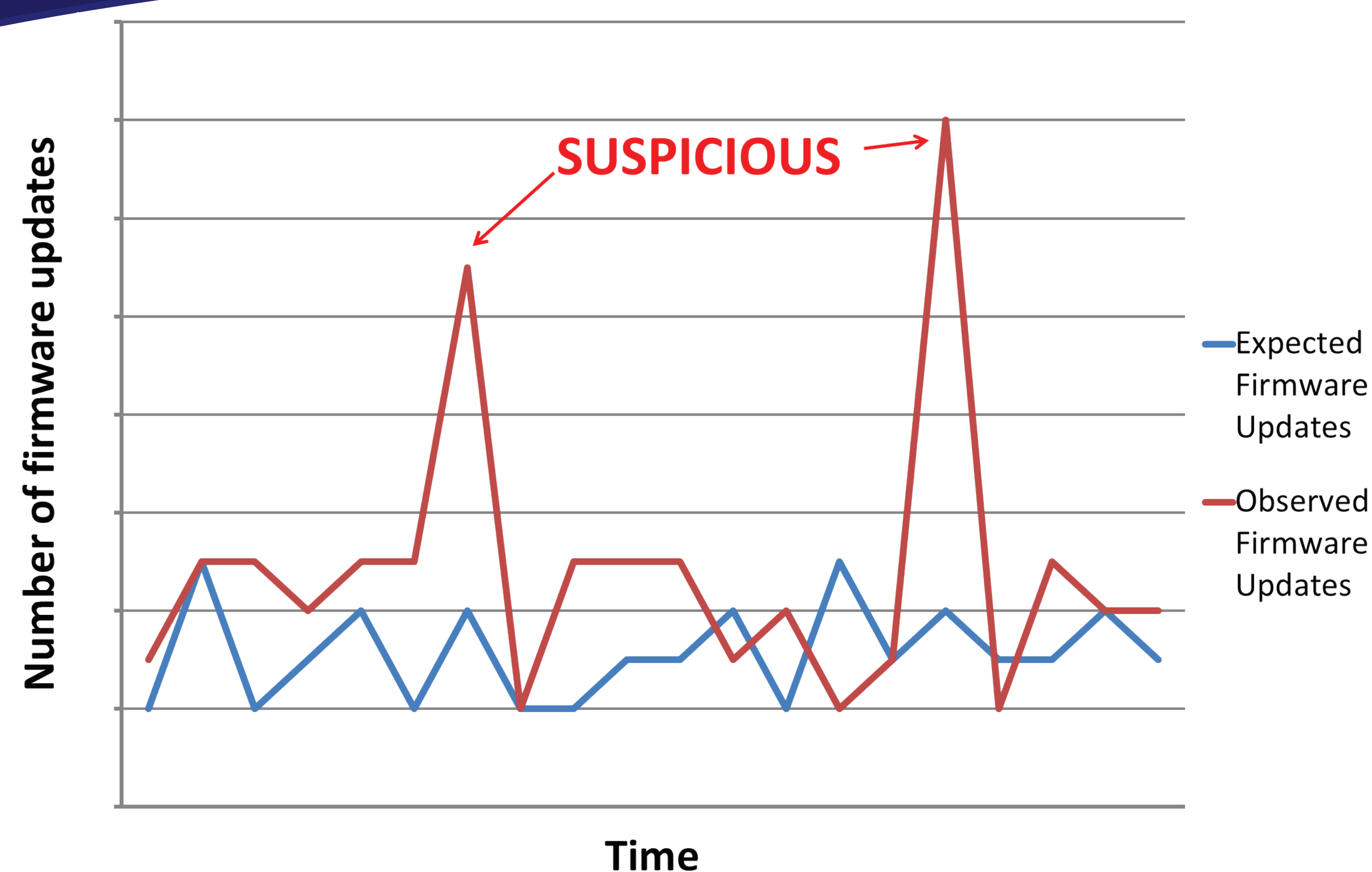


CYBERSECURITY AND DATA MANAGEMENT IN THE SMART GRID

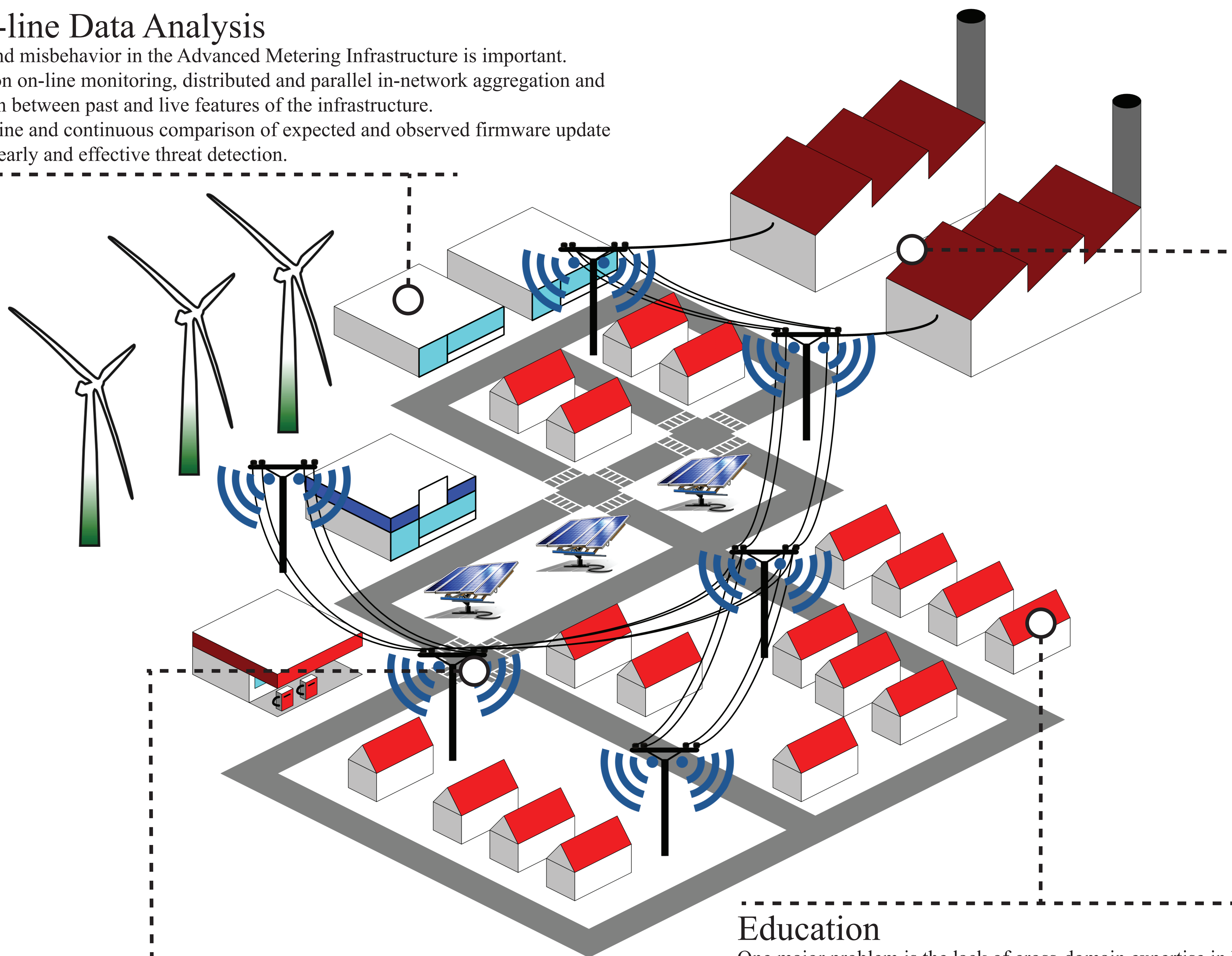


Data Anonymization

In the Advanced Metering Infrastructure, intelligent measurement devices are deployed. Data can be gathered with a high frequency and granularity, which in turn raises privacy concerns since it can be used to infer information about people's lifestyle. A challenging aspect is the study of data anonymization requirements with regards to gathered data volume and granularity.

Scalable, On-line Data Analysis

Detection of attacks and misbehavior in the Advanced Metering Infrastructure is important. Such detection relies on on-line monitoring, distributed and parallel in-network aggregation and continuous comparison between past and live features of the infrastructure. As an example, an online and continuous comparison of expected and observed firmware update rates might lead to an early and effective threat detection.



Education

One major problem is the lack of cross-domain expertise in both ICT security and power engineering.

- A new Master's course is given @ Chalmers: ICT Support for Adaptiveness and (Cyber)security in the Smart Grid, where industry partners give seminars.
- Several ongoing Master's projects cover important research topics: fuzzing, in-network aggregation and data validation, among others.

CHALMERS GÖTEBORG UNIVERSITY
Computer Science and Engineering



ICT Support for Adaptiveness and (Cyber)security in the Smart Grid DAT300

Spring semester, study period 4, 2014
(DAT300 – Masterclass in Areas of advance)

News:

- [2014-03-11] We will try to accomodate the meeting times for the course based on the students that participates. We have now booked two slots per week: Tuesdays 10–12; Thursdays 13–15, but if some of you also follow the security courses given in SP4, we will move the slots so you can also participate in this class. Just come to the first meeting.
- [2014-02-21] New draft home page created. Content will be added during February.
- [2014-02-21] The homepage from last year can be found [here](#), not that the course code has changed.

Fuzzing

By using fuzzing, the protection of equipment in the Smart Grid can be improved. In fuzzing, one checks the response of “black-box” devices against malformed input and checks the stability using protocol gnostic and agnostic tools. Joint work with Security Matters B.V., Netherlands



REFERENCES:

1. “AMI Threats, Intrusion Detection Requirements and Deployment Recommendations TCIPG: Trustworthy Cyber Infrastructure for the Power Grid.” Grochocki, D., Hub, J.H., Berthier, R., Bobba, R., Sanders, W.H., Cardenas, A., Jetcueva, J.G.
2. “Private Memoirs of a Smart Meter.” Molina-Markham, Andrés, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, 61–66. BuildSys '10.
3. “Smart Grid Privacy via Anonymization of Smart Metering Data.” Efthymiou, C., and G. Kalogridis. 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), 238–243, 2010.
4. “An Empirical Study of the Reliability of UNIX Utilities” B.P. Miller, L. Fredriksen, and B. So. Communications of the ACM 33, 12 (December 1990).



Distributed Computing and Systems
Computer Science and Engineering

MAGNUS ALMGREN, ZHANG FU, VINCENZO GULISANO,
MARINA PAPATRIANTAFILOU, VALENTIN TUDOR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CHALMERS UNIVERSITY OF TECHNOLOGY

ACKNOWLEDGEMENTS:

This work has been partially supported by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement 257007 and through the FP7-SEC-285477-CRISALIS project.

