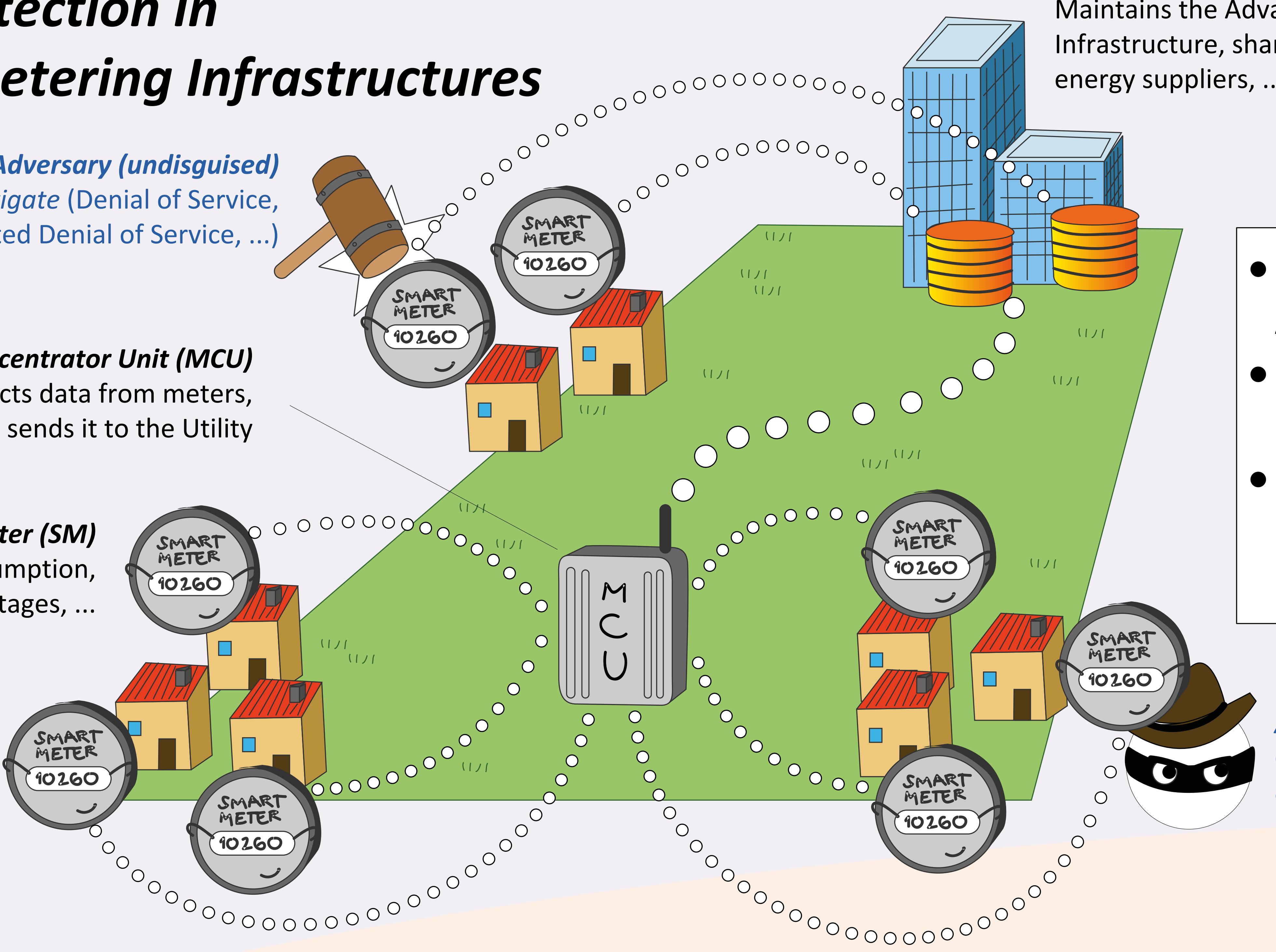
METIS: a Two-Tier Intrusion Detection System for Advanced Metering Infrastructures

Intrusion Detection in Advanced Metering Infrastructures



Utility
Maintains the Advanced Metering Infrastructure, shares data with energy suppliers, ...

Adversary (undisguised)
Challenging to *mitigate* (Denial of Service, Distributed Denial of Service, ...)

Meter Concentrator Unit (MCU)
Collects data from meters, sends it to the Utility

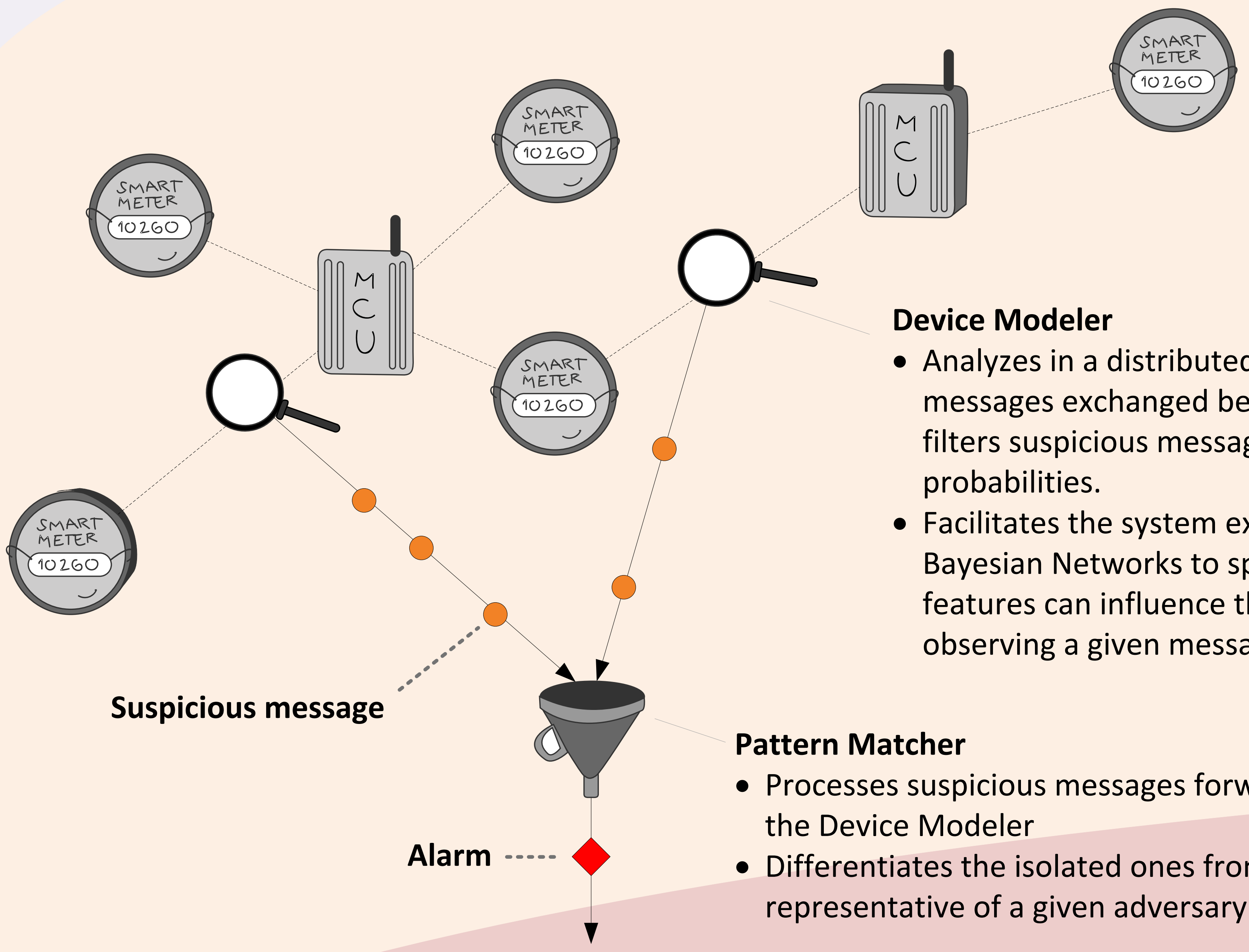
Smart Meter (SM)
Measures energy consumption, reports power outages, ...

Adversary (stealthy)
Challenging to *detect* (energy exfiltration, energy theft, ...)

CHALLENGES

- Embrace the *different networks* that compose Advanced Metering Infrastructures.
- Cope with the *large* and *fluctuating* volumes of data produced by the devices.
- Provide *intuitive ways* of specifying possible adversary goals (especially for undocumented attacks).

METIS: two-tier, streaming-based intrusion detection



Suspicious message

Alarm

Device Modeler

- Analyzes in a distributed / parallel fashion the messages exchanged between the devices; filters suspicious messages based on their probabilities.
- Facilitates the system expert interaction using Bayesian Networks to specify which traffic features can influence the probabilities of observing a given message.

Pattern Matcher

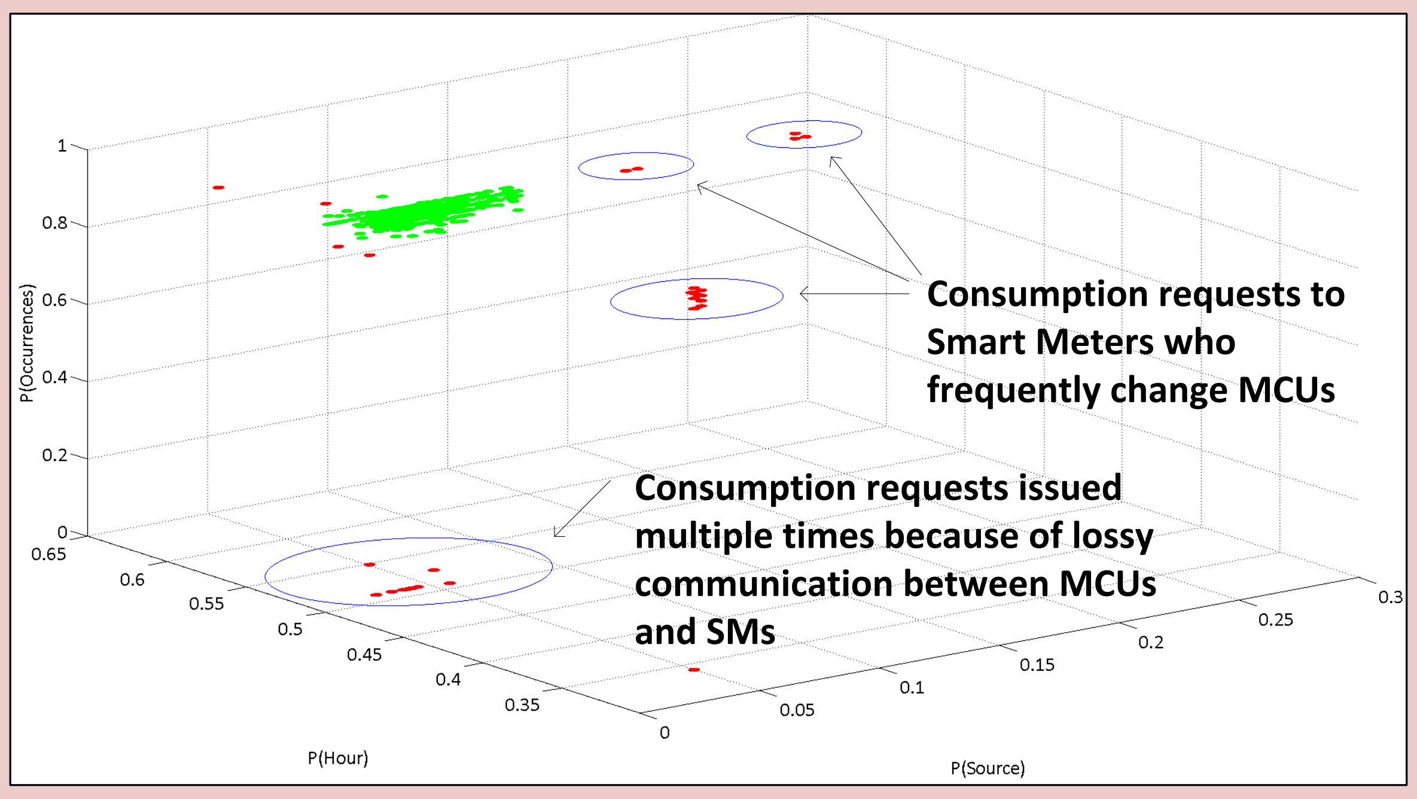
- Processes suspicious messages forwarded by the Device Modeler
- Differentiates the isolated ones from the ones representative of a given adversary goal.

CONTRIBUTIONS

- Two-tier architecture designed for a *modular* modeling of possible adversary goals and a scalable distributed / parallel traffic analysis based on the data streaming processing paradigm.
- Prototype implementation based on Storm, a state of the art Stream Processing Engine.
- Evaluation based on data extracted from a real-world Advanced Metering Infrastructure, currently focusing on *energy exfiltration* attacks, in which the adversary aims at stealing users' energy consumption information.

PRELIMINARY RESULTS

- 40 simulated energy exfiltration attacks injected.
- Small percentage (~8%) of messages exchanged between Smart Meters and MCUs considered as suspicious.
- 36 attacks (91%) detected!



Consumption requests to Smart Meters who frequently change MCUs

Consumption requests issued multiple times because of lossy communication between MCUs and SMs

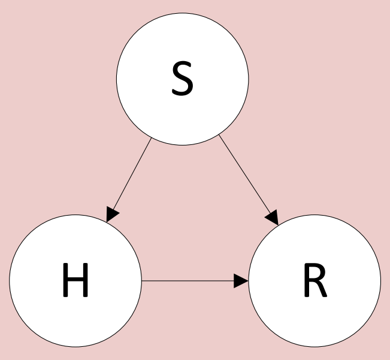
Energy Exfiltration Use-Case

Fine-grained consumption readings reveal detailed information about household activities. Such malicious activity can be carried out after successfully logging into an MCU or by deploying a (malicious) MCU replica. The subtle nature of this attack lies in that suspicious exchanges of energy consumption readings can be caused not only by the adversary, but also by legitimate factors.

Evaluation Setup

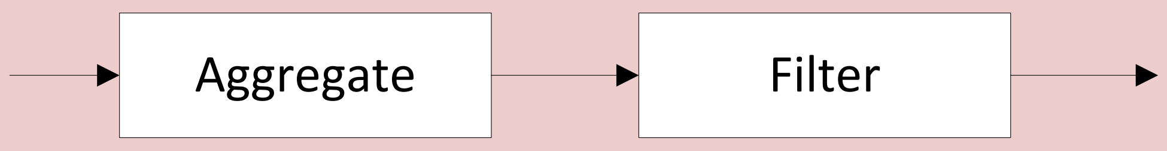
Real-world Advanced Metering Infrastructure, composed by 300,000 SMs and 7,600 MCUs. Covers a metropolitan area with roughly 600,000 inhabitants. Data extracted from a subset of 1,000 SMs and 40 MCUs, includes the messages exchanged to retrieve energy consumption during September 2012 - February 2013.

Bayesian Network for energy exfiltration



S: Smart Meter ID
H: Hour
R: # of Requests

Continuous query for energy exfiltration



Aggregate: Count # of suspicious events over 1 week
Group by smart meter

Filter: Suspicious events >= 5

Acknowledgments

This work has been partially supported by the European Comission Seventh Framework Programme (FP7/2007-2013) through the SysSec Project, under grant agreement 257007, through the FP7-SEC-285477-CRISALIS project and through the collaboration framework of Chalmers Energy Area of Advance.

References

- R. Berthier and W. H. Sanders. Specification-based intrusion detection for advanced metering infrastructures. PRDC, 2011.
- M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander. Lof: identifying density-based local outliers. ACM Sigmod Record, 2000.
- A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. BuildSys, 2010.
- M. Stonebraker, U. Çetintemel , and S. Zdonik. The 8 requirements of real-time stream processing. SIGMOD Rec., 2005.

Vincenzo Gulisano (vinmas@chalmers.se)

Magnus Almgren (almgren@chalmers.se)

Marina Papatriantafilou (ptrianta@chalmers.se)

Distributed Computing and Systems Research Group
Department of Computer Science and Engineering
Chalmers University of Technology

SEVENTH FRAMEWORK PROGRAMME
syssec
CRISALIS SECURING CRITICAL INFRASTRUCTURES