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

Vincenzo Gulisano, Magnus Almgren and Marina Papatriantafilou

Chalmers University
of technology

Agenda

1. Why METIS?
2. Preliminaries
3. METIS overview
4. Evaluation
5. Conclusions

Agenda

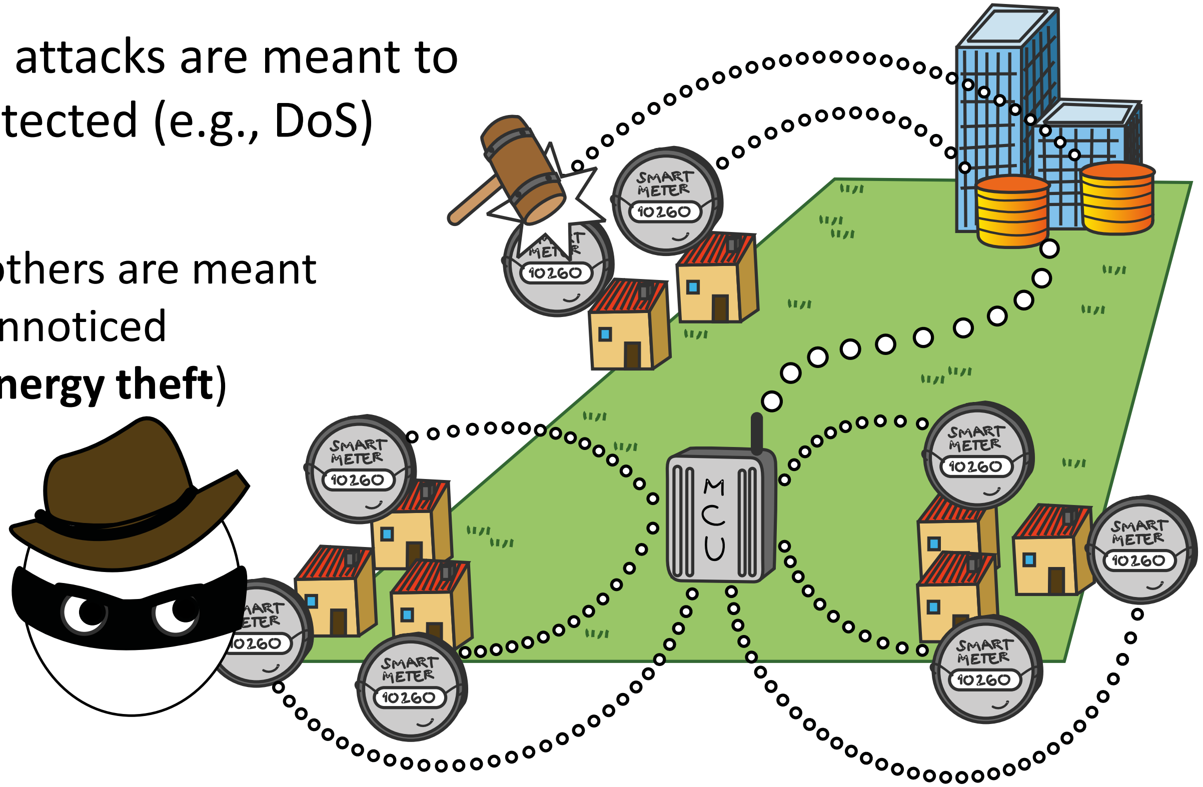
1. Why METIS?
2. Preliminaries
3. METIS overview
4. Evaluation
5. Conclusions

Why METIS?

Advanced Metering Infrastructures (AMIs)

Some attacks are meant to be detected (e.g., DoS)

Some others are meant to go unnoticed (e.g., **energy theft**)



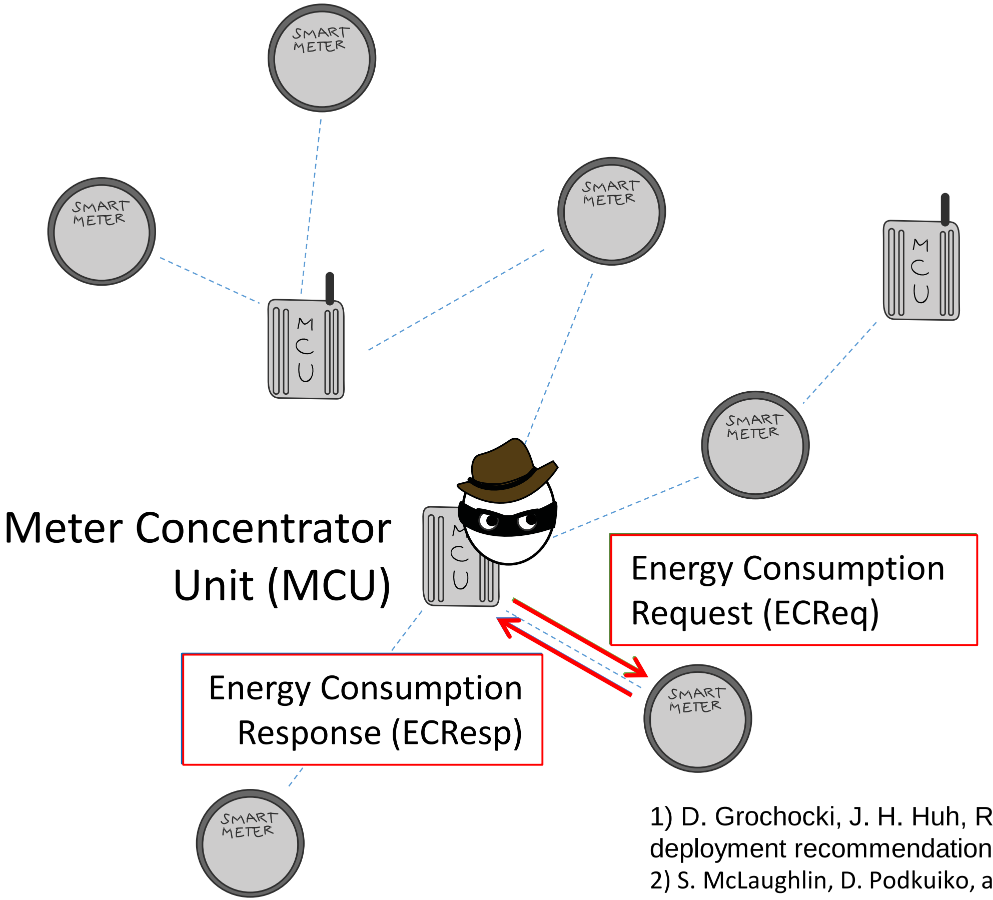
How can we detect them given that…

- … there is a large volume of *continuous* data demanding for distributed and parallel analysis
- … Most data is local to the devices
- … Such attacks are not documented
- … Each AMI relies on its brands, devices, protocols (i.e., system expert's knowledge plays a key role)

Agenda

1. Why METIS?
2. Preliminaries
    1. System / Adversary model
    2. Data Streaming
    3. Bayesian Networks
3. METIS overview
4. Evaluation
5. Conclusions

System / Adversary model


SMART METER
M C U
Meter Concentrator Unit (MCU)
Energy Consumption Request (ECReq)
Energy Consumption Response (ECResp)

Smart Meter (SM)

Attacks that could be detected by the framework:

- Installation of malicious firmware to use AMIs as communication medium[1]
- Installation of malicious firmware to lower bills[2]
- Energy Exfiltration attacks
- …

Energy Exfiltration

Fine-grained consumption readings
→ detailed information about household activities[3]

[1] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva. AMI threats, intrusion detection requirements and deployment recommendations. In Smart Grid Communications (SmartGridComm), IEEE Third International Conference on, 2012.

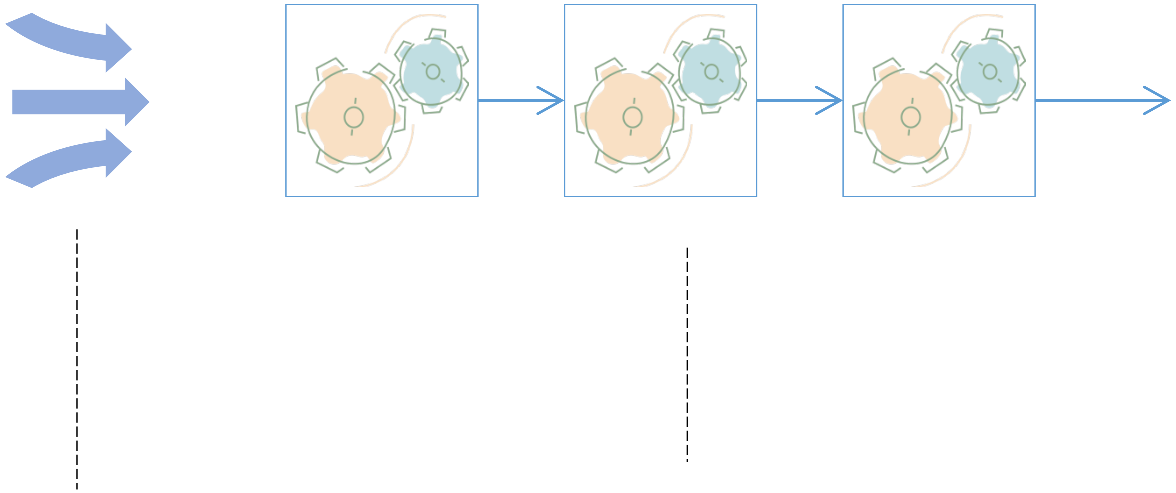
[2] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. In Critical Information Infrastructures Security. Springer, 2010.

[3] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-eciency in building, 2010.

Agenda

1. Why METIS?
2. Preliminaries
    1. System / Adversary model
    2. Data Streaming Processing Paradigm
    3. Bayesian Networks
3. METIS overview
4. Evaluation
5. Conclusions

Data Streaming Processing Paradigm

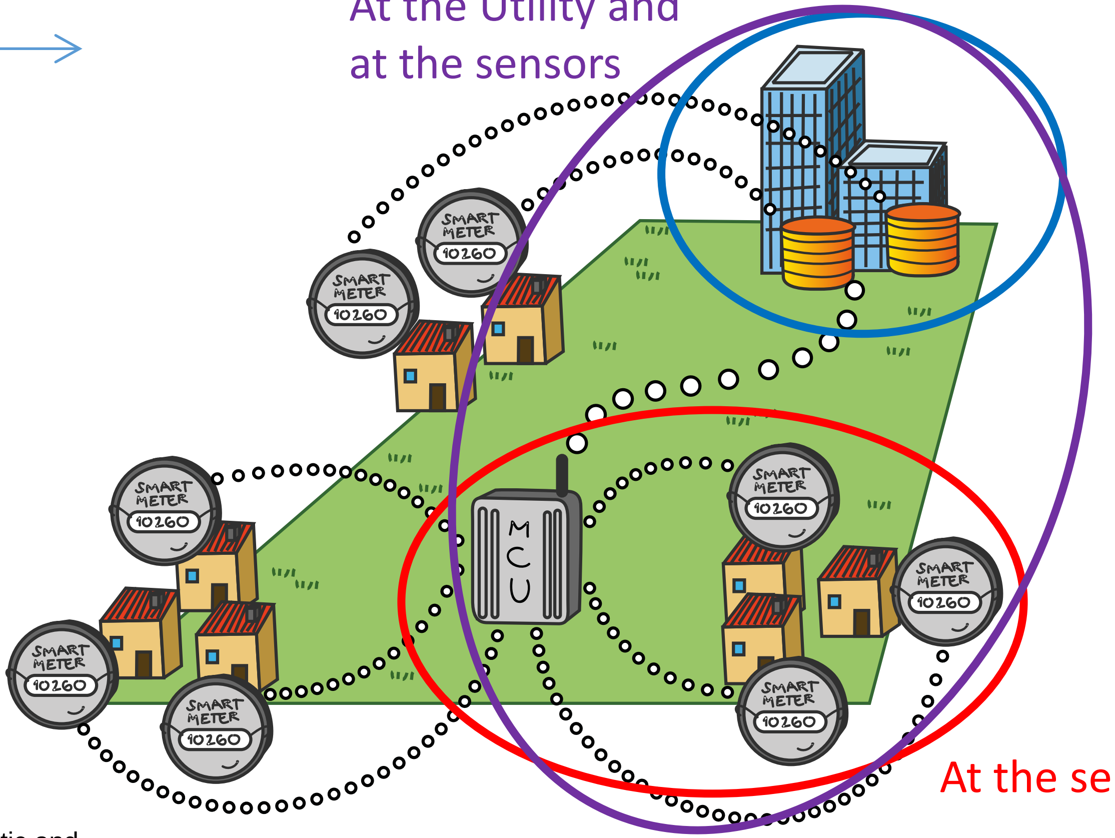


Distributed sources of data

Continuous Query (complex event processing)

Executed by Stream Processing Engines (SPEs)

Distributed and parallel deployment![1]



At the Utility and at the sensors

At the Utility

At the sensors

[1] V. Gulisano, R. Jimenez-Peris, M. Patino-Martinez, C. Soriente, and P. Valduriez. Streamcloud: An elastic and scalable data streaming system. Parallel and Distributed Systems, IEEE Transactions on, 2012.

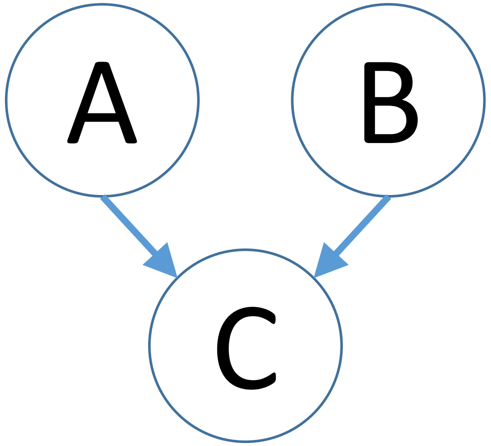
Bayesian Networks

- Probabilistic Graphical Model
- Random variables and their dependencies are represented by a Direct Acyclic Graph

A $\{a_0,a_1\}$

B $\{b_0,b_1\}$

C $\{c_0,c_1\}$



$P(c_0|a_0,b_0)$

$P(c_0|a_0,b_1)$

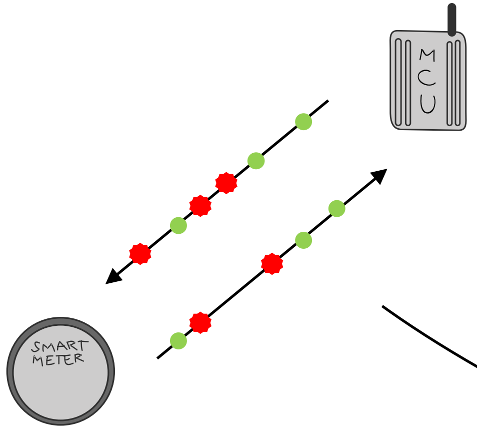
…

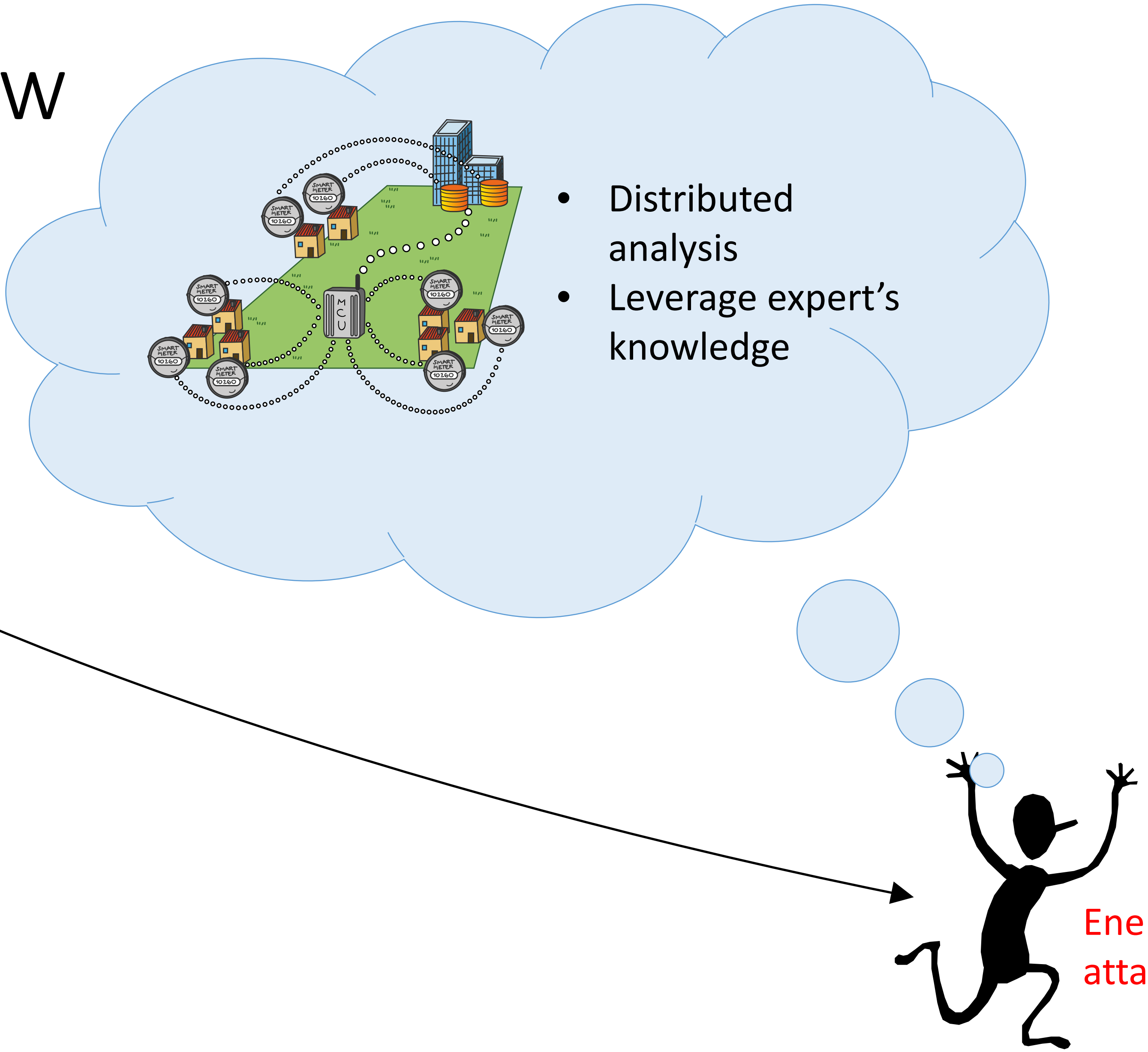
$P(c_1|a_1,b_1)$

Agenda

1. Why METIS?
2. Preliminaries
3. METIS overview
4. Evaluation
5. Conclusions

METIS overview

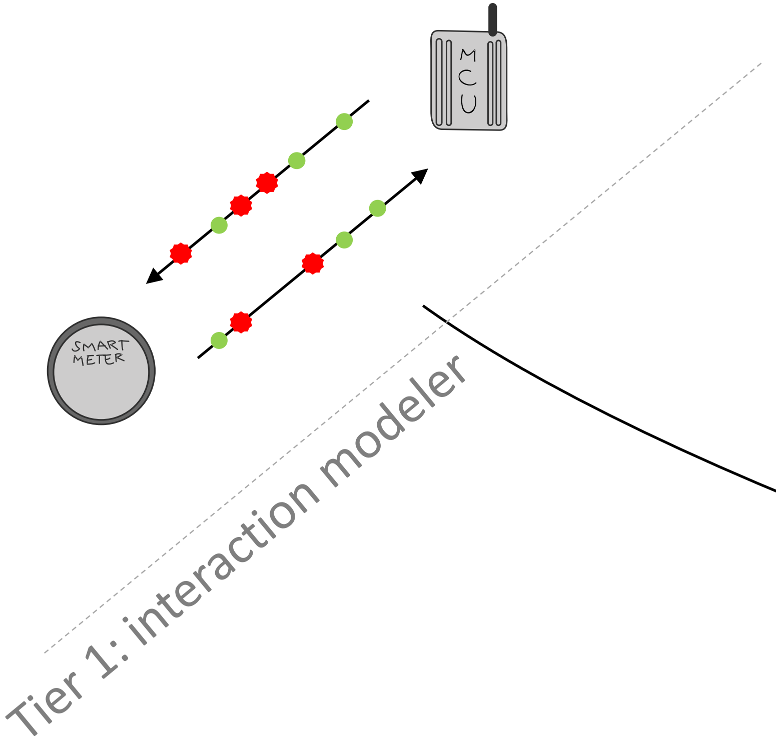




- Distributed analysis
- Leverage expert’s knowledge

Energy exfiltration attack!

METIS overview



AMIs evolve slowly and have limited heterogeneity.
Let’s learn which messages are expected and which are not!

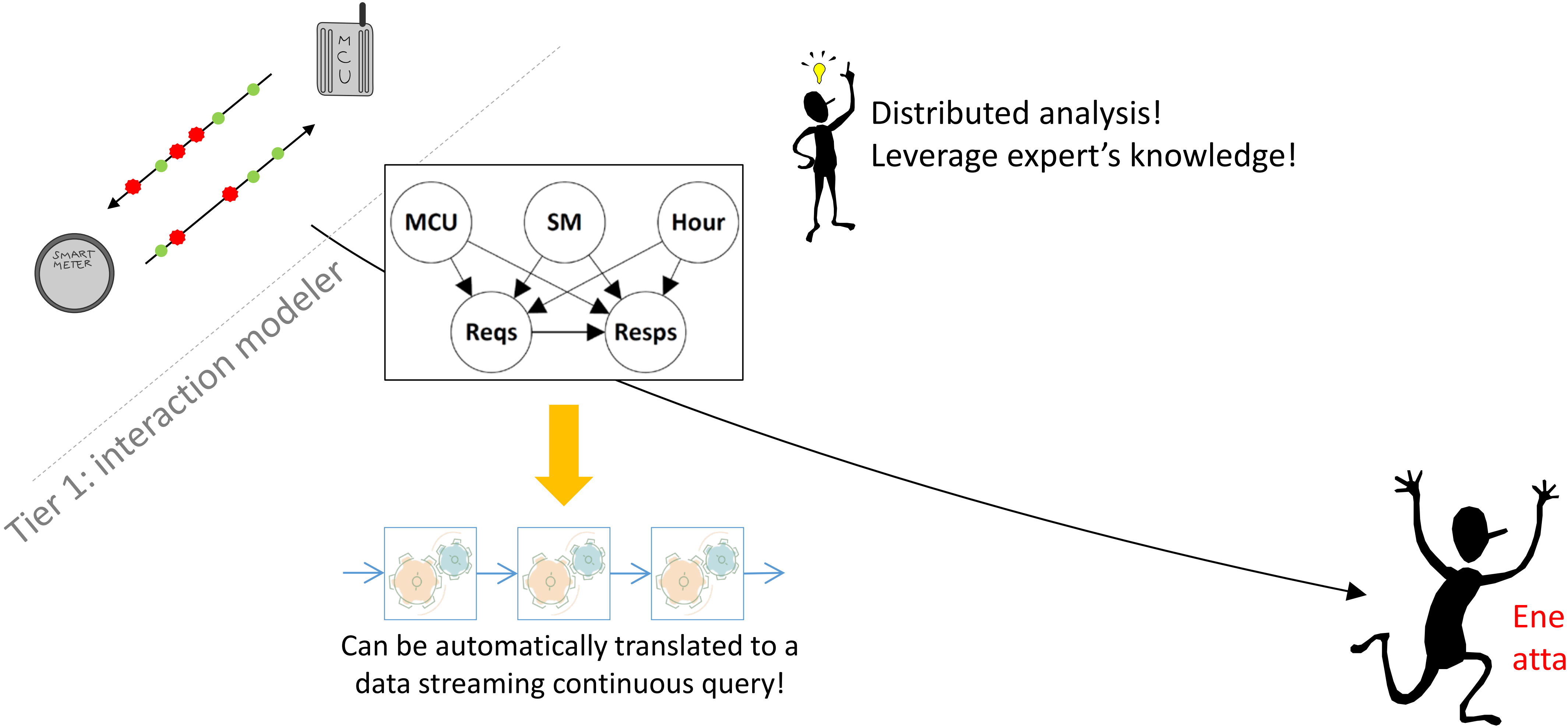
What influences an expected message?

SMART METER
MCU
…

Let’s use a Bayesian Network!

Energy exfiltration attack!

METIS overview

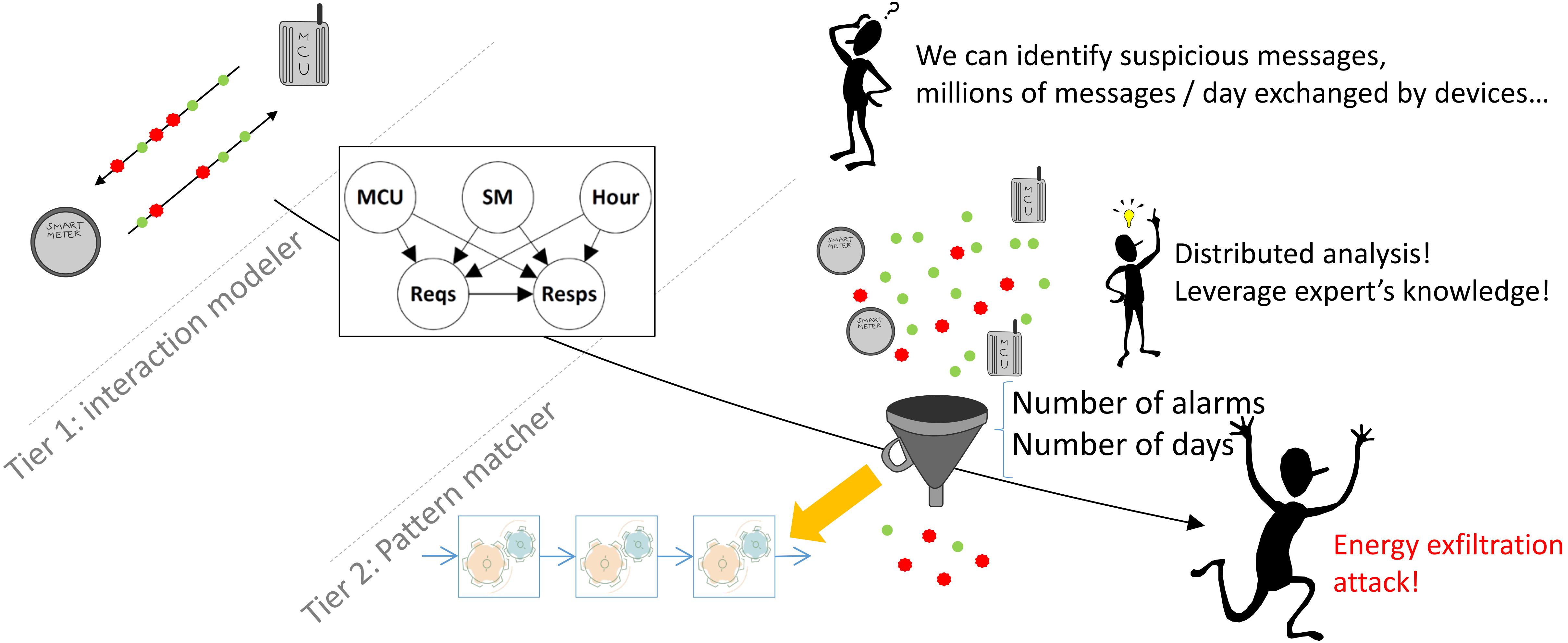


Distributed analysis!
Leverage expert's knowledge!

Can be automatically translated to a data streaming continuous query!

Energy exfiltration attack!

METIS overview



We can identify suspicious messages, millions of messages / day exchanged by devices…

Distributed analysis!
Leverage expert's knowledge!

Number of alarms
Number of days

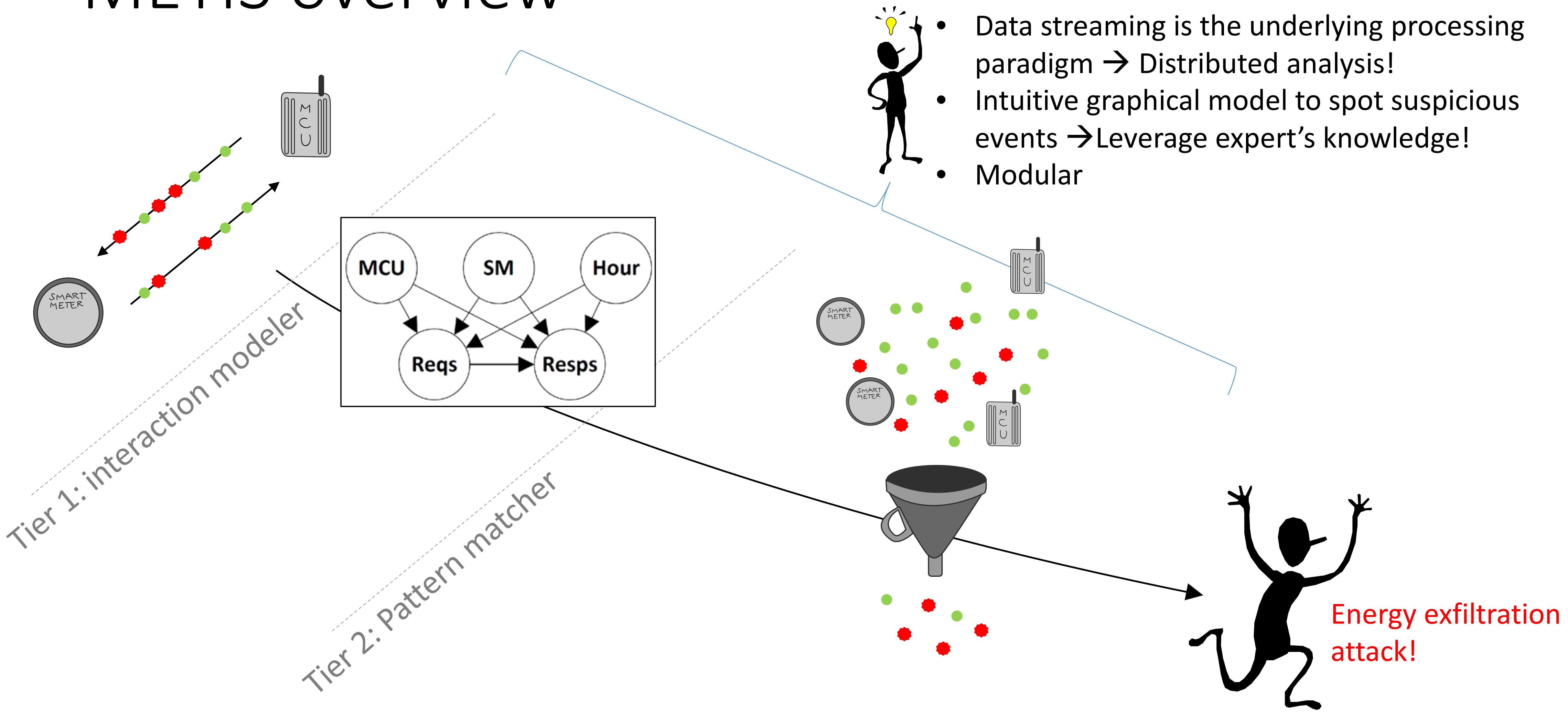
Energy exfiltration attack!

Tier 1: interaction modeler

Tier 2: Pattern matcher

METIS overview

- Data streaming is the underlying processing paradigm → Distributed analysis!
- Intuitive graphical model to spot suspicious events →Leverage expert’s knowledge!
- Modular



Agenda

1. Why METIS?
2. Preliminaries
3. METIS overview
4. Evaluation
    1. Setup
    2. Detection Accuracy
    3. Processing Capacity
5. Conclusions

Evaluation - Setup

- From a real-world AMI, data exchanged between
  - 100 MCUs
  - 6500 SMs
- Data covers September 2012 – February 2013
- No static linking SM ←→ MCU
- Wireless communication, messages get lost!

Energy exfiltration attacks:

- Randomly pick <SM,MCU>, during 7 to 10 days we inject ECReqs / ECReps
  - Malicious / Legitimate messages have the same prob. of getting lost!

- Implemented on top of Storm, a widely-used SPE (e.g., used in Twitter)

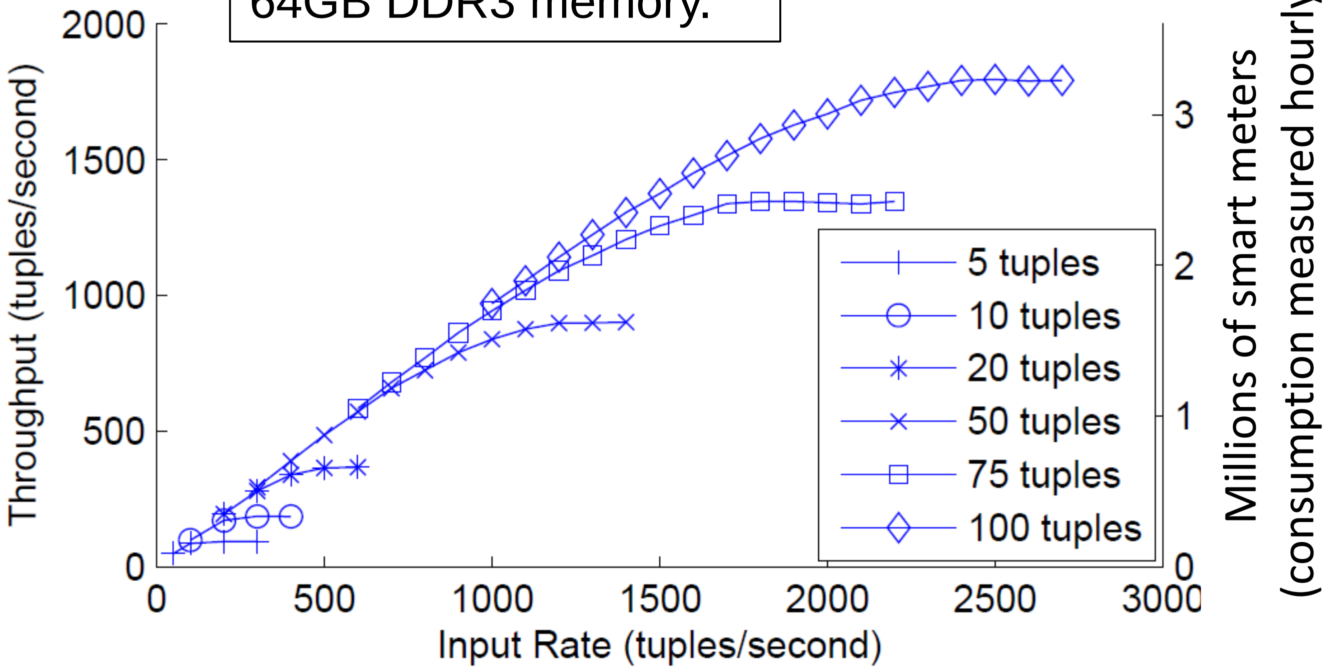
Evaluation – Detection Accuracy

AMI Data	Number of attacks	50
	Number of malicious messages	995
	Overall number of messages	4,146,327
	Messages per day (average)	23,743
Interaction Modeler	Malicious messages considered as suspicious	857 (86%)
	Malicious messages not considered as suspicious	138 (14%)
Pattern Matcher (at least 5 suspicious messages over 7 days)	Detected Attacks	45 (90%)
	False positives / day (Threshold = ~10) [1]	~ 1 or 2

1) R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das. The 1999 DARPA on-line intrusion detection evaluation. Computer networks, 2000.

Evaluation – Processing Capacity

Server specs:
16 Xeon E5-2650 cpus
64GB DDR3 memory.



Agenda

1. Why METIS?
2. Preliminaries
3. METIS overview
4. Evaluation
5. Conclusions

Conclusions

- METIS: a Two-Tier Intrusion Detection System for Advanced Metering Infrastructures
  - Eases the modelling of adversary goals
  - Scalable (distributed/parallel) traffic analysis
  - Evaluated for energy exfiltration with data from a real-world AMI

Thank You!

Questions?