FACULTY
OF INFORMATICS
Masaryk University

A Time-Sensitive Model for Data Tampering Detection for the Advanced Metering Infrastructure

MUNI
C4E

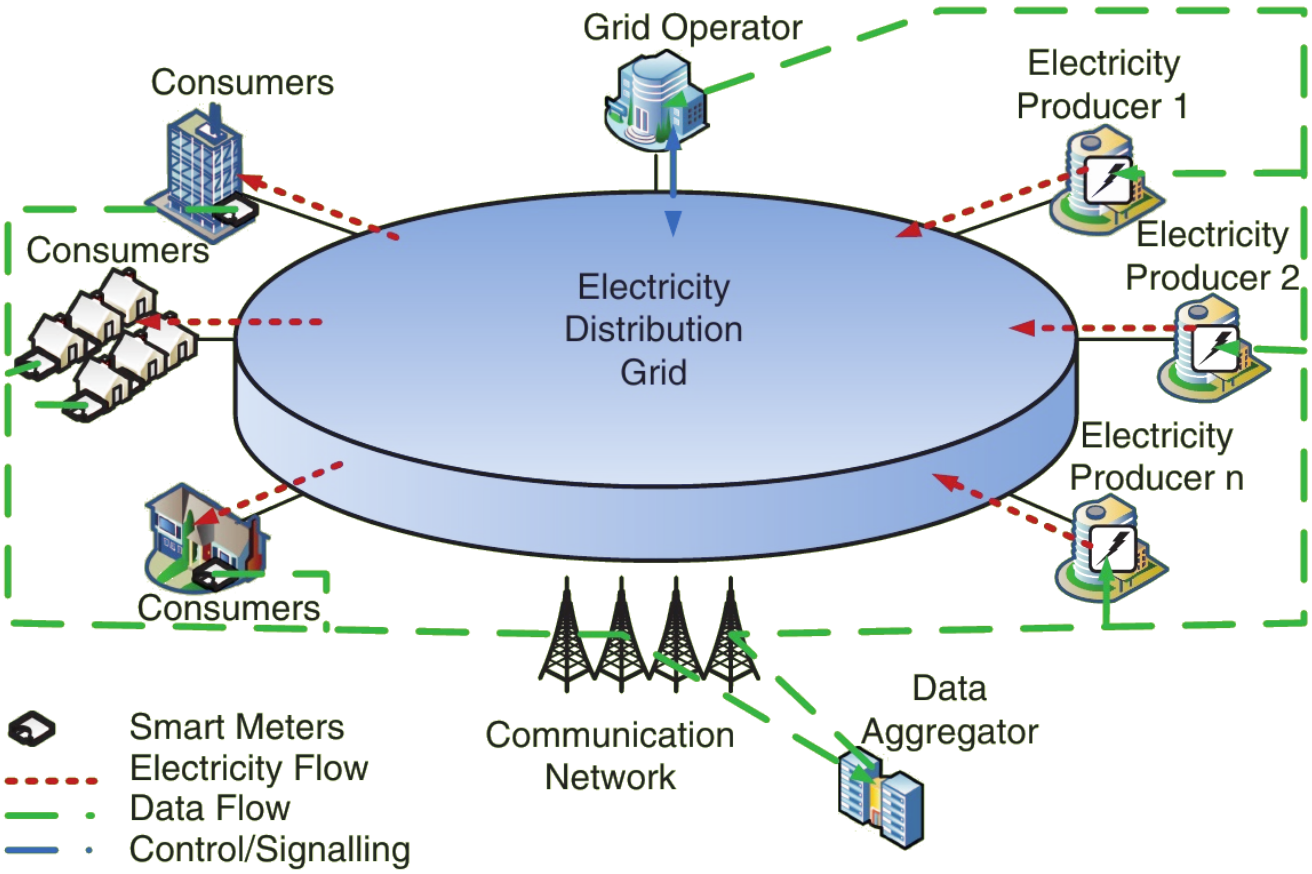
Smart Grids and Advance Metering Infrastructure

Smart Grids are modern power grids based on the integration of cyber and physical systems that enable efficient transmission of electricity, constant monitoring and self-healing properties in case of failures.

The Advanced Metering Infrastructure is constituted by smart meters and the communication infrastructure for dealing with bi-directional communication between smart meters, service operators and energy consumers/prosumers.

Smart meters are a central point for the provision of smart services to energy consumers. However, the wide diffusion has also increased several concerns for service operators.

Advance Metering Infrastructure - Diagram



Data Tampering Attacks

Data tampering activities are often referred to as false data injection attacks in the context of cyber-physical security of the Smart Grid.

Attackers can change the smart meter measurements by either compromising the hardware devices locally, injecting false data packets sent to control centers or by changing data exchanged in other parts of the Smart Grids infrastructure.

Cyber and physical attacks can lead to some effects on power measurements reported by smart meters. Compromissions can be both derived from physical or cyber aspects connected to the Advance Metering Infrastructure.

Data Tampering Attacks - Types

Cyber	Physical	Effect on Power Measurements
Compromise meters through remote network exploit	Break into the meter	Stop reporting entire consumption
Modify the firmware/storage on meters	Reverse the meter	Remove large applicances from measurement
Steal credentials to login to meters	Disconnect the meter	Cut the report by a given percentage
Exhaust CPU/memory	Physically extract the password	Alter appliance load profile to hide large loads
Intercept/alter communications	Abuse optical port to gain access to meters	Report zero consumption
Flood the NAN bandwidth	Bypass meters to remove loads from measurement	Report negative consumption (act as a generator)

Data - Statements

For any simple statements p, q, ..., any complex statements A, B, ..., the unary connectives $\neg$ (Negation), $\Box$ (Necessity), $\Diamond$ (Possibility), P (In the past), F (In the future), and the binary connectives $\wedge$ (Conjunction), $\vee$ (Disjunction), $\rightarrow$ (Entailment), the following recursive forming rules apply:

- (a) For any simple statement p, p is a well-formed statement. Furthermore, if $A = p$, then A is well-formed statement.
- (b) If A is a complex statement and $*$ is a unary connective, then $*A$ is a complex statement.
- (c) If A and B are complex statements and $*$ a binary connective, then $A * B$ is a complex statement.
- (d) There are no more statements than those defined by the clauses (a), (b) and (c).

Proposed Model for Data Tampering Detection

A model M is the structure $M = \langle K, T, \models \rangle$, where K is the set of devices (smart meters) a, b, c, ...; i. e., $K = \{a, b, c, ..\}$; each element of K is a set in itself that includes a minimum and maximum power consumption, m and h respectively, among other characteristics i_1, i_2, i_3, ...; i. e., $a = \{m, h, i_1, i_2, i_3, ...\}$. T is a set of temporal points t_1, t_2, t_3, ...; i. e., $T = \{t_1, t_2, t_3, ...\}$. Finally, $\models$ is a relation from K to the set of statements such that the following clauses apply:

Proposed Model for Data Tampering Detection

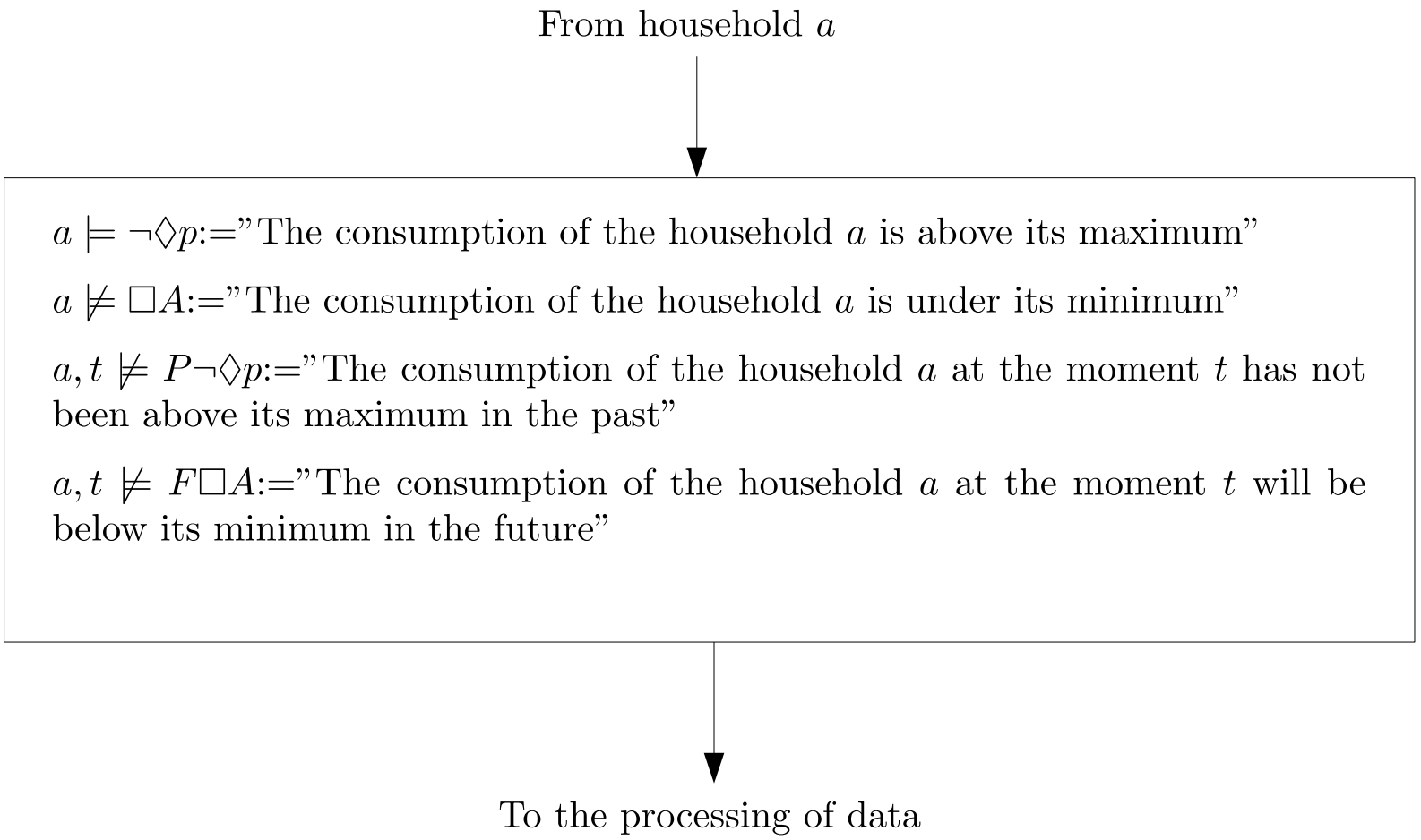
(1) $a \models A \wedge B$ if and only if (iff) $a \models A$ and $a \models B$
(2) $a \models A \vee B$ iff $a \models A$ or $a \models B$
(3) $a \models \neg A$ iff $a \not\models A$
(4) $a \models A \rightarrow B$ iff $a \models \neg A$ or $a \models B$
(5) $a \models \Box A$ iff $a \models m$
(6) $a \models \Diamond A$ iff $a \models h$
(7) $a, t \models PA$ iff $\exists s,\ s \in T$, with $s < t$, and $a, s \models A$, and $\forall u,\ u \in T$ if $s < u < t$, then $a, u \models A$
(8) $a, t \models FA$ iff $\exists s,\ s \in T$, with $t < s$, and $a, s \models A$, and $\forall u,\ u \in T$, if $t < u < s$, then $a, u \models A$

Formal Results: Soundness, Completeness and Decidability

Proof of Concept

- UMass Smart* Dataset (http://traces.cs.umass.edu/index.php/Smart/Smart)
- Theoretical Proof of Concept
- Practical Proof of Concept: HomeA-meter3_2016
  - Original Data from the dataset
    - “h” and “m” are extracted from the data
  - Simulated Data Injection Attack
    - “h” is equal to the mean plus three times the standard deviation

Proof of Concept – Theoretical Proof of Concept



Proof of Concept – Practical Proof of Concept

m="0.00010kW"
h="3.50000kW"

From HomeA

$HomeA \models \Box 0.00386kW$:="The consumption of HomeA is not under its minimum"

$HomeA \not\models \neg\Diamond 2.92368kW$:="The consumption of HomeA is under its maximum"

$HomeA$, $06:51:00 \models P\Box 0.00386kW$:="The consumption of HomeA at 06:51:00 has not been under its minimum since the past"

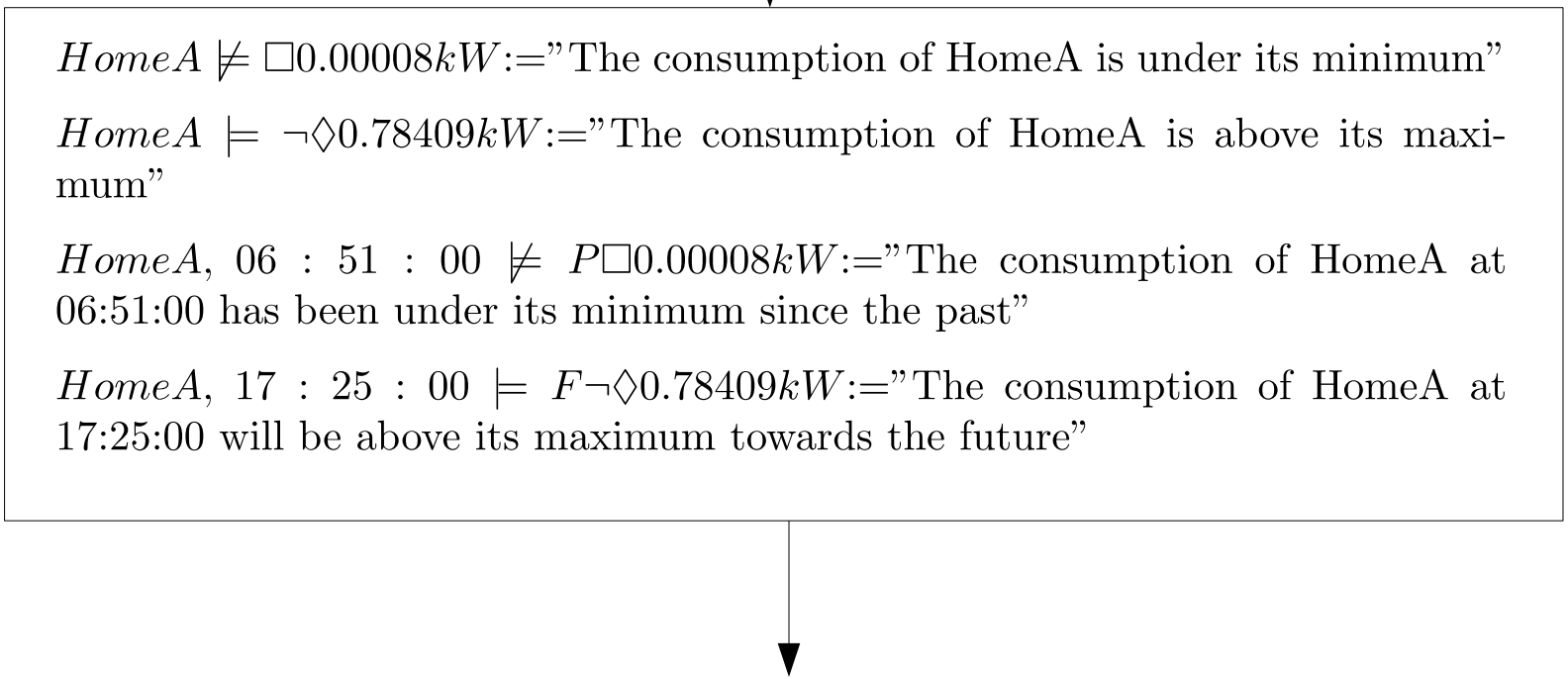
$HomeA$, $17:25:00 \not\models F\neg\Diamond 2.92368kW$:="The consumption of HomeA at 17:25:00 will be below its maximum towards the future"

To the processing of data

Proof of Concept – Simulated Data Injection Attack

m="0.00009kW"
h="0.66114kW"

From HomeA



To the processing of data

Conclusion

- The time-sensitive model allows for the detection of anomalies in energy consumption from smart meters in the context of data tampering activities.
- The model offers the tracking along the time dimension of these activities, allowing for the flagging of irregularities that are sustained in time.
- The model is able to detect any case of data tampering in smart meters, as it would not automatically target any peak or valley in the consumption, but rather those that prolong their existence over time.
- The effectiveness of the model has been shown through a proof of concept, both theoretically and based on a real dataset.

Future Works

- Implementation of an ontology and a semantic web reasoner based upon the model described.
- Testing within an anomaly detection framework, thus allowing more data to be obtained for further validation.
- Implementing the model in different domains like the communication solutions that are readily available.
- Modifying the model so the temporal dimension may be changed from a linear one to a branching one.