DOI: 10.15439/2021F106
ISSN 2300-5963 ACSIS, Vol. 25

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

José Miguel Blanco, Bruno Rossi, and Tomáš Pitner
Department of Computer Systems and Communications
Faculty of Informatics, Masaryk University
Brno, Czech Republic
{jmblanco, brossi}@mail.muni.cz, tomp@fi.muni.cz

***Abstract*—Smart Grids offer multiple benefits: efficient energy provision, quicker recoveries from failures, etc. Nevertheless, there is risk of data tampering, unsolicited modification of the data of the smart meters. The main aim of this paper is to provide a model for processing the smart meter data that flags any energy consumption level that could be indication of data tampering. The proposed model is time-sensitive, allowing for tracking the energy usage along time, thus making possible the detection of long-lasting abnormal levels of energy consumption. Such model can be integrated in an anomaly detection system and in a semantic web reasoner.**

I. Introduction

SMART Grids (SGs) 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, with the overall aim to provide smart services and reduced costs for utilities and consumers [1], [2].

From the side of the connection between consumers and service operators, an important part of SGs is the Advanced Metering Infrastructure (AMI) that 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 became over time a central point for the provision of smart services to energy consumers. However, the wide diffusion has also increased several concerns for service operators, such as the needs of securing the devices, dealing with privacy concerns about data usage, and avoiding potential risks of energy theft.

In this paper, we deal with potential compromission of smart meters with the purpose of altering the power consumption readings in so-called data tampering activities with the aim to gain some benefits or to harm the overall network stability by means of data injection attack [3]. Attackers can either compromise the hardware devices locally, injecting false data packets sent to control centers or modify data exchanged in other parts of the SGs infrastructure in so-called data injection attacks [3].

The proposed model is intended to be used as the basis for the implementation of algorithms to prevent data tampering from the side of energy service providers. The main characteristics that the model offers are twofold. Firstly, it can model a minimum and maximum energy consumption thanks to the modal operators. This allows to flag any energy usage that might be too big or too small and set up an alarm. Furthermore, the model also is able to track statements regarding energy usage along the time, allowing for the implementation of time-sensitive algorithms. This aspect increases the probability of detecting a real case of data tampering, as any peak or valley in the consumption would not be enough to set off an alarm. Peaks and valleys in energy usage are to be expected, but not when they last for a long time. Finally, it is important to note that the model has been implemented from a perspective of converting the data generated by the nodes into the semantic web. This means that one could be able to use the data generated by those devices, processed by the model, and input it into a semantic web reasoner, allowing for further automation and also a much better and extensive usage of the naturally generated data.

We have the following main contributions in this paper:

- Definition of a formal model based on temporal logic for data tampering of smart meters data;
- Theoretical and practical proofs of concept of the model based on sample data from UMass Smart* Dataset [4];

The paper is structured as follows. In Section II we define the concept of SGs, the importance of smart meters and the concept of data tampering for either energy theft or for reasons of false data injection attacks. In Section III we go through several related works of modelling/detecting data tampering for smart meters. In Section IV we define the temporal logic model for data tampering for smart meters, while in section V we give both a theoretical proof and a practical one based on the publicly available datasets of power consumption data. In Section VI we provide the discussion about the formal results of the model. In Section VII we discuss the impact of the model and the results in the general context of smart metering infrastructure, while in Section VIII we provide the final conclusions of the paper.

II. Advanced Metering Infrastructure & Data Tampering

A SG is a modern power grid enabling two-way power flow and bi-directional communication between power suppliers

The research was supported from ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

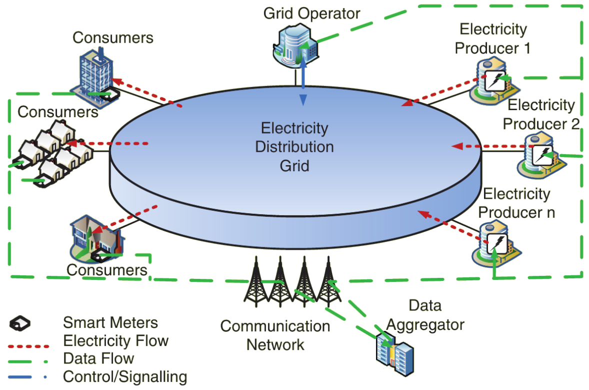


Fig. 1. Overview of the Advanced Metering Infrastructure (AMI) [5]

and consumers [2]. An efficient transmission of electricity, fast restoration in case of failures, and overall reduced costs for utilities are key aspects supported by the integration of cyber and physical systems [1]. The adoption of SGs leads to lower power costs for consumers, reduced peak demand, increased integration of large-scale renewable energy systems. Real-time monitoring and recovery of power generation and distribution is another key characteristic, as the actual state of the grid is monitored and reported to the network, adapting the power output to the real needs. SGs are also important to increase the usage of renewable sources (e.g., solar energy), as excess energy generated can be sold.

Decentralization of the SG led to the introduction of microgrids. A microgrid is an independent and small network of electricity users (consumers / prosumers) that can carry out operations independently from the centralized grid and even isolate itself from the rest of the power network in case of failure of the grid [6]. As it can be seen from Fig. 1, devices and sensors also play an important role in the context of SG, as they support smart energy scenarios, such as households using a solar-power system (with batteries and sensors) to decide about the best times to recharge Electric Vehicles (EV) [6].

Smart meters are a key element to allow bi-directional communication inside the AMI in SGs [7]–[10]. They constitute a cyber-physical device that can register power consumption and transmit back information to Distribution System Operators (DSOs). The smart meters allow one household to fully embrace the smart home concepts, by bringing several benefits to consumers / prosumers and DSOs: first of all, the availability of power consumption information allows consumers to make more reasoned choices about the best power consumption patterns allowing savings on energy costs. Furthermore, DSOs can remotely access smart meter readings, reducing the costs, and possibility of human mistakes. Additionally, wasting of energy can be reduced, by balancing the power needs where needed [8], [9]. The overall view of smart meters in the context of SGs can be seen in Fig. 2, where smart meters can be placed in the context of Home Area Networks (HAN) to integrate the different devices in a smart home. Furthermore, they can be part of Neighbourhood Area Networks (NAN) to integrate several households and make possible prosumer / consumer communication, and Wide Area Networks (WAN) to cover communication with data centers and DSOs. Data concentrators are an important component of the AMI that allows the connection between different smart meters and service providers [7], [9], [10]. All these connections and the way they are implemented, constitute the AMI [7], [9].

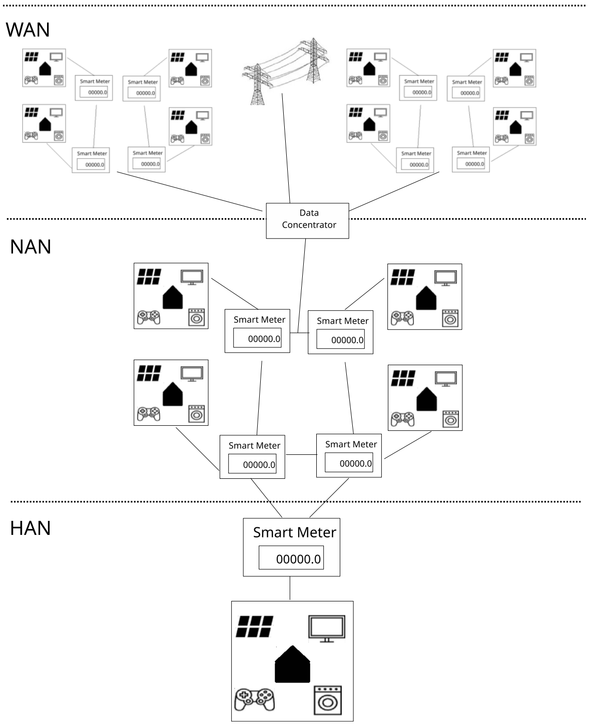


Fig. 2. Overview of Smart Meters and AMI infrastructure (adapted from [8])

Together with the benefits, there are also some potential drawbacks in the adoption of more advanced power metering devices and in general AMI. The large diffusion of smart meters and the enhanced functionalities offered increased the needs of a balance between securing the devices, keeping privacy concerns about data usage, and avoiding potential risks of energy theft.

Attacks to smart meters are often done with the aim of some data tampering activity: either on the physical device or on the data registered transmitted to achieve either some economical benefit or to harm the overall stability of the network. Data tampering activities are often referred to as false data injection attacks in the context of cyber-physical security of the SG. 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 SGs infrastructure [3].

Data tampering activities targeted at AMI can be summarized in Table I, where we can see the cyber and physical attacks that 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 AMI [11], [12]. In this paper, we are focused on the effects on power measurements, such as altering the reported power consumption to the energy provider.

III. Related Works

There are several research works that deal with data tampering in the AMI. Many of these papers focus on either energy theft detection, data tampering / data injection attacks, aggregation of data and / or frameworks for the detection / prevention of data attacks to smart meters in the AMI.

Li et al. [13] were proposing an approach to aggregate data from smart meters keeping privacy concerns in mind. A signature-based scheme, together with an incremental verification protocol is used to deal with potential dat tampering *in itinere* on data derived from the smart meters.

Hock et al. [14] were proposing an anomaly detection model using multiple sources to detect smart meters that were tampered with. The approach is based on the comparison of several time series, showing advantages over analyzing a single power consumption time series.

McLaughlin et al. [11], [12] proposed a framework for the detection of energy theft in the context of AMI, combining data from smart meters and sensors to increase detect capabilities. Combining power consumption data traces with data from logs and cyber events proved to increase the detection rate of malicious activities.

Liu et al. [15] use colored Petri net to model information flows between different components in the smart meters. Considering a threat model, authors propose a detection mechanism against false data injection attack that can be used to detect any data tampering activity.

The model proposed in the current paper can be seen as a temporal model that can be used on the inception of the data generated from smart meters. As such, it can be considered as an aggregation to the work done in Li et al. [13] rather than an alternative. Furthermore it can complement anomaly detection approaches (e.g., Hock et al. [14]) with some formal reasoning on which to base the algorithms for the detection of malicious activities for data tampering in the AMI.

IV. Model for smart meters data tampering detection

In this section, we will present the temporal logic model to be used as basis for algorithms for smart meters data tampering detection and processing of the generated data. In the upcoming sections we will discuss theoretical and practical proof of concepts of the model.

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).

By simple and complex statements we are referring to any kind of data that any device of the AMI might produce. In the current case we are focusing on the idea of implementing the model for data tampering on smart meters, but any reader would be able to identify statements that allow to reflect different aspects that give context to any action (e. g., weather data). Furthermore, while the model counts with a nice array of connectives, we have excluded any high order connectives (e. g., $\forall x$, for all x), as to keep the model to a minimum, therefore making its implementation easy as only simple operations would be required. Nevertheless, despite the simplicity of the model, it still allows for the processing of complex and interesting statements thanks to the expressiveness and variety of connectives. For example, for any reader that might be interested in using the model for patterns from a single smart meter could do so by using the recursive definition and add as many connectives to their statements as needed. Also, if a reader would be interested in aggregating multiple sources, the connective for Conjunction would allow for it. As an addition to the recursive definition of the connectives, we highlight that by $\top$ we mean constant true as customary.

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:

(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 $\exists s,\ s \in a$, with $s < t$, and $a, s \models A$, and $\forall u,\ u \in a$ if $s < u < t$, then $a, u \models A$
(8) $a, t \models FA$ iff $\exists s,\ s \in a$, with $t < s$, and $a, s \models A$, and $\forall u,\ u \in a$, if $t < u < s$, then $a, u \models A$

This model M is able to express multiple notions that are of use when considering data tampering in the SGs domain; specifically, it is based on the communication of power consumption values from the smart meters. In the first place, it is necessary to point out that the model is built under the idea that every smart meter can, and will, produce statements regarding their consumption. These statements are divided into two

TABLE I
TYPE OF DATA TAMPERING ATTACKS [11], [12]

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)

categories: simple statements, represented by lower-case letters p, q,..., and complex statements represented by upper-case letters A, B, C,...; simple statements are produced directly by the devices themselves while complex statements are to be obtained from the aggregation of simple statements. These statements are assigned either true or false according to the device where they are produced. $a \models p$ and $a \not\models p$ represent that the statement p is valid and not valid on the device a respectively. These statements are to be processed according to the classical propositional connectives of conjunction, disjunction, negation and entailment as customary. This is represented by clauses (1)-(4). (1), the clause for conjunction ($\wedge$, and), states that the conjunction of two statements is valid (in the device a) iff both statements are valid (in the device a). (2), the clause for disjunction ($\vee$, or), states that the disjunction of two statements is valid iff any of those two statements is valid. (3), the clause for negation ($\neg$, not), states that the negation of a statement is valid iff said statement is not valid. Finally, (4), the clause for entailment ($\rightarrow$, if...then...), states that a conditional statement is valid if any, the negation of the first statement or the second statement, are valid. Up to this point, the model is pretty straight forward and includes little to no novelty regarding customary processing of data.

The remaining clauses, (5)-(8), introduce the more interesting aspects. Clause (5), the clause for necessity, states that a necessary statement is true iff the argument of said statement is valid according to the minimum set by the device. That means that every device a would have a established minimum consumption m that would, in its turn, generate a statement A. This statement, therefore, is to be considered as necessarily valid, $\Box A$, iff it holds according to the minimum m. The same holds for clause (6), the clause for possibility, with the great difference that it is considered against the maximum set by the device, h.

Clause (7), the clause for "In the past", states that a statement is in the past iff there is a past temporary moment in which the statement was valid and for each temporary past moment between the first one and the present, the validity of the statement holds. This means that given a statement A is valid in a device a, in a temporary moment t, iff the statement is valid in a past temporary moment s and in the device a, and also for each temporary moment u, such that $s < u < t$, the validity of A holds in a. The same holds for clause (8), the clause for "In the future" with the great difference resides that the additional temporal moments s and u are set in the future and, therefore $t < u < s$.

All in all, this model allows us to establish a minimum consumption statement A that is to be necessary, $\Box A$, whose validity ensures that the data cannot be tampered giving back a value that is too low. Also, the model allows the establishing of a maximum that cannot be trespassed, $\neg\Diamond A$, that would be able to determine any tampering in the data consumption regarding the higher values. Both minimum and maximum are set outside of the boundaries of the formal model, as they are dictated by real-world actions, physical parts of the system (e. g., the maximum energy consumption established by contract). This further expands on the versatility of the model, as it can be set to almost anything that might be wanted, be it a simple numeric value, be it a range of values, with ease. Also, the model is not only able to consider and validate these examples, but also is able to track them along time, as it is able to determine not only if something is valid in the past or the future, PA and FA respectively, but also validate those statements according to very specific temporary points t, and therefore making the flagging of tampering much more precise. This is due to the facts that spikes over the maximum and under minimum are to be expected, but they cannot be validated for a long time.

To finalize this section there is a point that need to be addressed: the implicit comparison operator built in the validation of the statements. As m and h represent a numeric value and there are statements strictly linked to them, there has to be a comparison operator of sorts. Nevertheless, as it can be seen in the model above, the comparison operator does not exist. This is mostly due to the fact that the comparison can happen with disregard to this kind of operator: it happens but dealing on absolute values; i. e., instead of comparing two different values, it compares the validity of the statements with regard to a physically set boundary. This helps to keep the model as simple as possible, lowering its computational complexity and making it easier to implement.

A. On the relation of the proposed model with LTL

A really interesting point to be make is about the relationship of the model with LTL (Linear Temporal Logic). It could be argued that the presented model is, indeed, related to

LTL and that is, without a doubt, a correct interpretation, as both share the same kind of temporal dimension: a linear one. Nevertheless, the proposed model is more than just LTL. It should be regarded as a fragment of LTL plus an extension of said fragment; i. e., the fragment comprised of the connectives $\wedge$, $\vee$, $\rightarrow$, $\neg$, P and F, (excluding the connectives U and S) and extended with the modal connectives $\Box$ and $\Diamond$. Because this, the model is not introduced with relation to LTL, as that would be detrimental to its understanding. This reason is the same why LTL is presented as an individual model and not as just an expansion of classical propositional logic. The same could be said for any temporal or real-logics. Despite all this, any tools supporting specification and proving for existing temporal logics should be easily applicable to the common fragment of the temporal model that we have defined.

V. Proof of Concept

In this section, we will give two different proof of concepts. One based off a theoretical example, in which we will go over an ideal household a, and a practical example, for which we will use the data of UMass Smart* Dataset [4]. We begin with the theoretical one and will progress into the practical later.

To keep the proofs of concept as simple as possible we will provide simple examples with the breaching of a minimum/maximum for a long time by single datapoints. Nevertheless, the model is expressive enough to track patterns. For example, the reader might want to consider a case in which after a consumption over the maximum, the energy usage is back within the established limits and this happens up to three times with exactly the same energy consumption. This could be represented by the complex statement $(P\neg\Diamond r \rightarrow s)\wedge(P\neg\Diamond r \rightarrow s)\wedge(F\neg\Diamond r \rightarrow s))$ where $\neg\Diamond r$ is a consumption above the maximum and s a regular energy usage. As such, the model allows to design and apply customized patterns to fit the specificity of the AMI in which data tampering activities are to be detected.

A. Theoretical Proof of Concept

Let us consider a to be a small and regular household. As any household, this one has an upper limit on energy consumption at once established by the contract. This limit is established in h in the previous model (cf. clause (6) and its definition) and it is a simple statement p that equals to said upper limit; e. g., $p =$ ”the consumption is under 3kW”.

Similarly, a lower limit m (cf. clause (5) and its definition) is also established. This lower bound is not as easy to pinpoint as it is possible to not have clear data on it since its inception. Nevertheless, this problem might be solved with the advent of many smart devices, like fridges, washing machines and many other household items. These devices are expected to be able to convey their consumption in real time as statements. This would allow to calculate a minimum based on those devices that are to be running at all times; e. g., a fridge. All this items on their own should provide multiple statements regarding consumption that can be summed up in an aggregator before leaving the household; e. g., the fridge might produce $q =$ ”the consumption is 350W”, the electric heating might produce $r =$ ”the consumption is 1kW”; and therefore, the complex statement is to be $A = q\wedge r$. Obviously, this complex statement A is to be established in m as we pointed before.

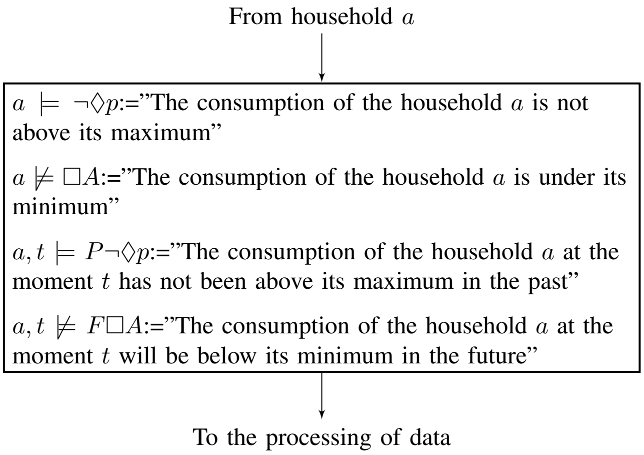
All this allows for monitoring peaks and lows in consumption. For that matter, clause (6) would allow to detect any peak higher that the maximum that we have established. When the statement $\neg\Diamond p$ is validated for the node a, $a \models \neg\Diamond p$, we know that the consumption data are being tampered, as it is impossible for the consumption to be as high: the complex statement $\neg\Diamond p$ indicates that is impossible for that to happen. In the same vein, any time that the statement $\Box A$ is not validated, $a \not\models \Box A$, it indicates that the consumption has gone under a minimum that is not expected, as there is minimal consumption that should happen constantly. With these in mind, we could track the peaks and valleys of the ideal household a that we have defined above, being able to set off an alarm when the consumption goes into abnormal territory.

It is obvious that peaks and valleys are bound to happen from time to time and not all of them should be due to data tampering. For that matter, the model introduces clauses (7) and (8) that allows to track the abnormal consumption as time goes by. The previous statements could be modified so they are read as $P\neg\Diamond p$ and $F\Box A$. This means that the abnormally high consumption from before has been going on for some time. Even more, the validation of this statement in the household that we have set should be reading as $a, t \models P\neg\Diamond p$, indicating that since the time point t the consumption has been too high. This would be able to tell us that the data of household has been tampered if t is far away enough in time. In the same sense, the not validation of $F\Box A$ would be the anticipation of some tampering in the long run: $a, t \not\models F\Box A$ means that the abnormally low consumption $\Box A$ is being constantly validated. This, in particular, rather than establishing the revision of something that has been happening for some time to set off an alarm, would be useful to indicate in which time point the alarm should be set off.

All the statements that we have used for this theoretical example can be seen summarized in Figure 3. Also, as this figure points out, the statements that are outputted by the household are to be processed in some way or another, be it a semantic web reasoner as mentioned above, be it a manual processing. One thing might draw the attention of the reader from the diagram is the explanation of $a, t \not\models F\Box A$. This is due to the fact that we are predicting what will happen in the future. Nevertheless, what this mean is that said statement is able to track the minimum consumption into the future; i. e., the statement allows for flagging a too low consumption somewhere in the future.

B. Practical Proof of Concept

Let us consider the case of HomeA from the UMass Smart* Dataset (2017 release) [4]. As we have stated before, these data are extracted directly from real smart meters and real households, so this further validation reinforces the usefulness and of the model and its real-world application. For this proof



From household a

$a \models \neg\Diamond p$:="The consumption of the household a is not above its maximum"

$a \not\models \Box A$:="The consumption of the household a is under its minimum"

$a, t \models P\neg\Diamond p$:="The consumption of the household a at the moment t has not been above its maximum in the past"

$a, t \not\models F\Box A$:="The consumption of the household a at the moment t will be below its minimum in the future"

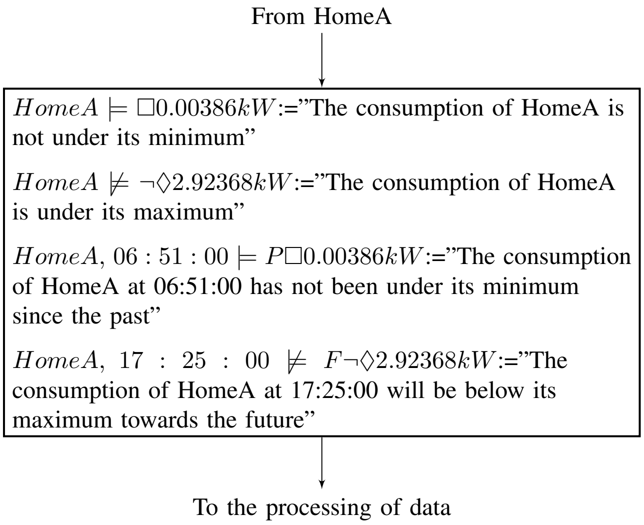
To the processing of data

Fig. 3. Household a Data Diagram

of concept, we will divide it into two different parts. The first one would be focused on showing how the model works with the preexisting data, while the second will focus on a hypothetical data injection attack.

1) Preexisting Data: For this example, we focus on the data stored in the file HomeA-meter3_2016, the one with the meter reading occurring every minute. Despite being real-world data, we are still missing some important values, like the minimum and maximum, m and h in the model respectively. Therefore, we will extrapolate this from the data we already have. As we have pointed above, we are considering single datapoints for the minimum and maximum but, nevertheless, it could be adapted to be a value equal to a standard deviation over the mean as we will show later. Since we are dealing with a regular household we will assume that there is no data tampering in the dataset and, from the file, we can assume that $m = "0.00010kW"$ and $h = "3.50000kW"$. These values are obtained from the data: there is no value under 0.00010kW as the lowest consumption can be found at Date: 2016-08-02, Time: 15:09:00 with the consumption equal to 0.00013kW; also, there is no value above 3.50000kW as the highest consumption can be found at Date: 2016-05-09, Time: 17:38:00 with the consumption equal to 3.14308kW.

Once we have set the upper and lower bound we introduce the operators of the model that allow for the description of minimum and maximum. For the case of the minimum, for the consumption p, where p is the consumption of the data from Date: 2016-10-07, Time: 06:51:00 and is $p = "0.00386"$. Then we have that $HomeA \models \Box p$, as p remains over the minimum we have set. For the case of the maximum, for the consumption q, where q is the consumption of the data from Date: 2016-05-13, Time: 17:25:00 and is $q = "2.92368"$. Then we have that $HomeA \not\models \neg\Diamond q$, as q remains below the maximum set in h. For the case of the time-sensitive connectives is easy to see how they are implemented from the time points that we have selected. Assuming that we want to check out the validity of the minimum consumption, $\Box p$, in the past, $P\Box p$, we would set the time point t as $t = "06:51:00"$ and go as back we might be interested, in this case we set $s = "04:51:00"$ for a time span of two hours. Since for every time point u between t and s the consumption does not go under the minimum, as it can be seen in the dataset, we can affirm that $HomeA, t \models P\Box p$; i. e., the consumption of HomeA has not gone under the minimum in the past at the time point t (since a time point s). Additionally, for the case of checking the maximum in regards to a future time point, we firstly set the time point t' as $t' = "17:25:00"$ and the future time point s' as $s' = "21:30:00"$ giving a time span of 4 hours and 5 minutes. Since for every time point u' between t' and s' the consumption is under the maximum we know that $HomeA, t' \not\models F\neg\Diamond q$; i. e., the consumption of HomeA has not gone over the maximum at time point t' (towards a time point s').



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"

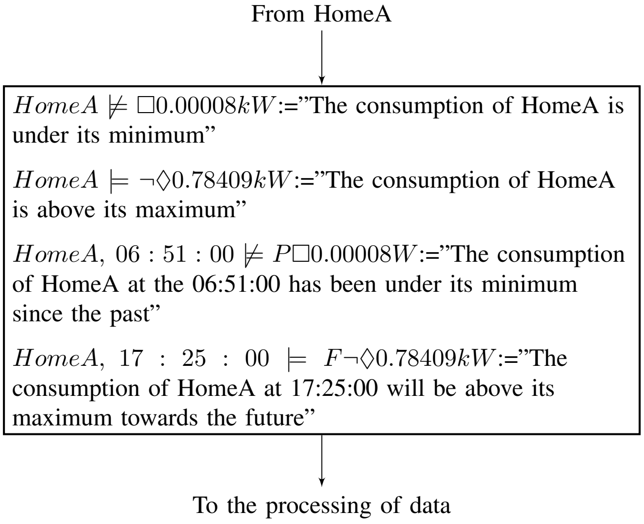
$HomeA$, $17:25:00 \not\models F\neg\Diamond 2.92368kW$:="The consumption of HomeA at 17:25:00 will be below its maximum towards the future"

To the processing of data

Fig. 4. HomeA Preexisting Data Diagram

All that has been described for this practical proof of concept based on the preexisting data can be seen in Figure 4.

2) Simulated Data Injection Attack: Now, we will show how the model works in the case that a data injection attack might happen at HomeA. For this case, we will consider two different data injection attacks and, to showcase the flexibility of the model, we will set up the maximum to be equal to the mean plus three times the standard deviation. In this case the mean is 0.02166kW while the standard deviation is 0.21316kW. The minimum would be set up to be a really low value, as the mean minus three times the standard deviation would give back a negative value, something that is impossible in this case. Obviously, this statistic approach will not work appropriately given the fact that the dataset that we are using is not normally distributed, but will suffice to show how the model works. With this in mind the minimum and maximum are as follows: $m' = "0.00009kW"$ and $h' = "0.66114kW"$. The first one would consider that the energy consumption p' at Date: 2016-07-10, Time: 04:51:00 until Time: 06:51:00



From HomeA

$HomeA \not\models \Box 0.00008kW$:="The consumption of HomeA is under its minimum"

$HomeA \models \neg\Diamond 0.78409kW$:="The consumption of HomeA is above its maximum"

$HomeA$, $06:51:00 \not\models P\Box 0.00008W$:="The consumption of HomeA at the 06:51:00 has been under its minimum since the past"

$HomeA$, $17:25:00 \models F\neg\Diamond 0.78409kW$:="The consumption of HomeA at 17:25:00 will be above its maximum towards the future"

To the processing of data

Fig. 5. HomeA Simulated Data Injection Attacks Diagram

has been tampered so it reads $p' = "0.00008kW"$. Since we know that the minimum $m' = "0.00009kW"$, it automatically follows $HomeA \not\models \Box p'$, thus flagging the consumption at any time point given of that time span as abnormal. Furthermore, since the consumption have been modified for time span, from $s = "04:51:00"$ to $t = "06:51:00"$, it allows the model flag it as abnormal in the current time point t with regards to a time point in the past s; i. e., $HomeA, t \not\models P\Box p'$. All in all, the model would detect that, at the time point t, the energy consumption has been abnormally low since the time point s.

The second simulated data injection attack would take place at Date: 2016-05-13, Time: 17:25:00 until Time: 21:30:00, tampering the energy consumption q' to $q' = "0.78409kW"$. Since the maximum has been set as $h' = "0.66114kW"$ this would allow for the model to give back the flagging of the consumption as abnormally high at any time point of the previous time span; i. e., $HomeA \models \Diamond\neg q'$. Furthermore, if we consider the time point $t' = "17:25:00"$ as the initial time point, the model would be able to track this towards a future time point $s' = "21:30:00"$ and, thus it would mark the consumption as abnormally high for the time span since t' until s'; i. e., $HomeA, t' \models \Diamond\neg q'$.

These simulated data injection attacks are available in the shape of a diagram to the reader in Figure 5. Additionally, it is important to mention that these attacks come to show how the model would work with a high tolerance, as it would detect really small differences, like in the case of the minimum, while also detecting some not so small such as the attack on the maximum.

VI. Formal Results

The fragment M_0 of the model M that includes the connectives $\wedge$, $\vee$, $\neg$, $\rightarrow$, P, F is sound, complete, decidable and satisfiable. This is due to the first four connectives being the connectives of classical propositional logic. For the last two, the temporal connectives this results also apply. This is due to the fact that the temporal dimension has been added following the work done in [16], which makes them a conservative extension of the previous model. With this said, they necessarily preserve any properties that the base model might have. Therefore, the whole fragment is, as pointed above, sound, complete, decidable, and satisfiable. This formal results guarantee that the model will not get stuck in an infinite loop, that it would be able to process any valid statement no matter what, and also the fact that well-formed statements can be validated by the model.

Also, it should be recalled that the temporal dimension added following [16] is a Linear Temporal Dimension. This implies that there is just one flow of time, not multiple as in the case of a Branching Temporal Dimension. This further expands on the simplicity of the model as, while the branching time option could be really interesting, also requires more computational power, as it creates a different flow of time for each event that we might want to track thanks to the model.

With regards to the missing fragment, the one of the connectives $\Box$, $\Diamond$, the same result should follow, but for that matter the model should be strengthened with a relational operator R. Since this model aims at being a simple model of low computational complexity, this relation should be avoided. Nevertheless, since the main validation terms of the connectives, m and h, are expected to be based on real-life events instead of theoretical ones, the same results should follow, but their proofs exceed the capabilities of a formal system.

VII. Discussion

The proposed model has been developed with the aim to deal with smart meters data tampering potentially being the basis for algorithms for anomaly detection and a semantic web reasoner. However, it is not only ideal to prevent the submission of false data, it can also constitute a validator to process regular generated data from the AMI. The model would allow for service providers to keep the whole network under surveillance to further support additional data monitoring processes. Furthermore, the definition of the model is as minimal as possible so its real-world implementation is not huge tax on any preexisting running process. Also, the fact that the model has been endowed with a temporal dimension helps when dealing with questions that might fall outside the scope of other processing tools. This is even more evident when compared with the data that is already available, like the one of UMass Smart* Dataset [4] that we used in the practical proof of concept.

A point that needs to be addressed is the integration of the model with the semantic web and therefore, with the semantic web reasoners. The statements that are part of the model are considered to be as statements from IoT devices. Generally speaking, this means that these statements are easily converted into semantic web statements, making them processable by any kind of semantic reasoner. This conversion from IoT into the semantic web is due to an Internationalized Resource

Identifier (IRI) that gives uniquely identifiable names to the thing and also specifies the location of the resource, based on the Web Ontoly Language (OWL). All in all, the model is not introduced only with the idea of detecting data tampering, but also to implement an automation of so and the AMI in general. This can be more obvious if one takes a look at all the clauses of the model, as it might be possible to have a model with only (3) and (5)-(8) to process the data tampering, but in this case, the model is extended so a semantic web reasoner has the possibility of going beyond just data tampering. It is interesting to mention that there are semantic web reasoners that have been already developed with the idea of working the energy consumption data that is the base of SGs. A good example of what these can reasoners do is [17], where the authors introduce the OEMA ontology for unifying the energy domain, which leads to the automation of the energy performance and contextual data processing. Let us add that the proposed model is independent of any ontology, it can be used to work with many different ones, as it provides the framework for the reasoning, rather than the statements that can be processed and, therefore, adding to its flexibility.

It is also worth mentioning how the model flexibility is one of its main advantages. As the model is quasi-formal, meaning that there is a part based on its interaction with the physical world, the constraints established can be bent in whatever way a service provider of a SG might need. For example, when establishing the maximum and minimum consumption for any prosumer, the aforementioned methods might not work. This is due to the fact that the minimum consumption of a prosumer might, and is expected to be, negative. Nevertheless, this can be extrapolated from the data of the energy production of the solar panels. Thus, modifying the validity of m and h, the formal notions of the model that represent the minimum and maximum consumption of the element a of the network.

Going further into the flexibility of the model, for two different households a and b, if those two households have the same minimum and maximum, m and h, then the model would be able to assign the corresponding statement to each household. Furthermore, in the case that the minimum and maximum are different, the model is not just THE model, but rather A model, meaning that there could be multiple iterations of the same model for different entities, but with the same structure. Additionally, given that both m and h are determined by the iteration of the model, the same semantic web reasoner could be used to process the data of multiple models at the same time.

To conclude this section, it is important to note how the time-sensitive aspect of the model, does not relay on accessing time points that have not already happened; i. e., time points in the future. Rather than that, what the model offers is the option of tracking changes with the passing of time, i. e., the F connective, or checking with past time points, i. e., the P connective, to ensure the validity of the statements that are happening in the current time point.

VIII. Conclusion

This paper has introduced a time-sensitive model that allows for the detection of anomalies in energy consumption from smart meters in the context of data tampering activities. The model not only offers the detection of said anomalies, but also their tracking along the time dimension, allowing for the flagging of irregularities that are sustained in time. This model has been shown to be 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 this very model has been shown through a proof of concept, at first theoretically and based on a real dataset afterwards. Furthermore, the model can be taken as the basis for the implementation of a semantic web reasoner that is not just focused on data tampering, but also allows for processing any other information produced by the smart meters that might be part of the whole advanced metering infrastructure.

There are multiple lines of investigation that can be followed from here; the main ones to be explored include the implementation of an ontology and a semantic web reasoner based upon the model described. Together with this support, the data-tampering detection model described would be tested within an anomaly detection framework, thus allowing more data to be obtained for further validation. The model also could be implemented in different domains like the communication solution that appeared in [18]. It is also of interest to modify the model so the temporal dimension may be changed from a linear one to a branching one, thus allowing for the tracking of multiple time spans of different households at the same time.

References

[1] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, *Smart grid security*. Springer, 2015.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[3] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: attacks, countermeasures and challenges," *Journal of Information Security and Applications*, vol. 54, p. 102518, 2020.

[4] "Smart - UMass Trace Repository." [Online]. Available: http://traces.cs.umass.edu/index.php/Smart/Smart

[5] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[6] R. Hebner, "Nanogrids, microgrids, and big data: The future of the power grid," *IEEE Spectrum Magazine*, p. 23, 2017.

[7] S. Chren, B. Rossi, and T. Pitner, "Smart grids deployments within eu projects: The role of smart meters," in *2016 Smart Cities Symposium Prague (SCSP)*, May 2016. doi: 10.1109/SCSP.2016.7501033. ISSN null pp. 1–5.

[8] D. B. Avancini, J. J. Rodrigues, S. G. Martins, R. A. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *Journal of cleaner production*, vol. 217, pp. 702–715, 2019.

[9] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid—challenges, issues, advantages and status," in *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–7.

[10] G. R. Barai, S. Krishnan, and B. Venkatesh, "Smart metering and functionalities of smart meters in smart grid-a review," in *2015 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 2015, pp. 138–145.

[11] S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier, “Amids: A multi-sensor energy theft detection framework for advanced metering infrastructures,” in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 354–359.

[12] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A multi-sensor energy theft detection framework for advanced metering infrastructures,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319–1330, 2013.

[13] F. Li and B. Luo, “Preserving data integrity for smart grid data aggregation,” in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012. doi: 10.1109/SmartGridComm.2012.6486011 pp. 366–371.

[14] D. Hock, M. Kappes, and B. Ghita, “Using multiple data sources to detect manipulated electricity meter by an entropy-inspired metric,” *Sustainable Energy, Grids and Networks*, vol. 21, p. 100290, 2020.

[15] X. Liu, P. Zhu, Y. Zhang, and K. Chen, “A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[16] M. Finger and D. M. Gabbay, “Adding a temporal dimension to a logic system,” *Journal of Logic, Language and Information*, vol. 1, no. 3, pp. 203–233, Sep. 1992. doi: 10.1007/BF00156915. [Online]. Available: https://doi.org/10.1007/BF00156915

[17] J. Cuenca, F. Larrinaga, and E. Curry, “A Unified Semantic Ontology for Energy Management Applications,” in *WSP/WOMoCoE@ISWC*, 2017.

[18] P. Hajder, M. Hajder, M. Liput, and M. Nycz, “Direct communication of edge elements in the industrial internet of things,” in *Communication Papers of the 2020 Federated Conference on Computer Science and Information Systems*, ser. Annals of Computer Science and Information Systems, S. Agarwal, D. N. Barrell, and V. K. Solanki, Eds., vol. 23. PTI, 2020. doi: 10.15439/2020KM194 pp. 35–42. [Online]. Available: http://dx.doi.org/10.15439/2020KM194