Privacy and Security Threats from Smart Meters Technology

Matthew Robinson, Pascal A. Schirmer and Iosif Mporas
Communications Intelligent Systems Group, School of Engineering and Computer Science,
University of Hertfordshire
Hatfield, UK
m.robinson20@herts.ac.uk, p.schirmer@herts.ac.uk i.mporas@herts.ac.uk

2021 International Carnahan Conference on Security Technology (ICCST) | 978-1-6654-9988-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCST49569.2021.9717384

***Abstract*—Energy smart meters have become very popular, advantaging the general public and utility companies via instant energy monitoring, and modelling, respectively. The information available from smart metering could however be used maliciously with the use of non-intrusive load monitoring technology. In this paper, we explore the vectors for attack on the smart metering network, showing physical and logical locations from which data could be stolen; and show how socio-economic, health related, occupancy, and multi-media viewing habits can be estimated to a high accuracy, thus posing a threat to users' privacy and security.**

Keywords—consumer privacy, home security, smart meters, non-intrusive load monitoring

I. Introduction

As of December 2020, within Great Britain 12.7 million electricity smart meters have been installed into domestic homes, with an average of 2.3 million electricity smart meters being installed annually for the past 5 years [1]. The acceptance of smart meters into the home has so far been positive, with 74% of surveyed customers reporting they were satisfied with their smart meter approximately one year after installation, as reported by the UK government in 2017 [2]. The general public has also demonstrated an understanding of the benefits of smart metering, mainly relating to budgeting, energy consumption accuracy, avoiding waste, and an end to estimated billing [2].

Smart metering can also have a large positive effect on utility companies by providing inputs to grid load estimations and by helping to build long- and short-term energy forecasting models [3, 4]. This modelling may be expected and accepted by the consumer as it is in the public interest to promote future electrical applications, such as battery storage to grid and vice-versa, to be controlled intelligently; but there are possible negatives to the roll out of smart meters with regards to privacy and security [5].

An enabling technology that would allow both advances in energy monitoring and such a privacy breach to take place is energy disaggregation or Non-Intrusive Load Monitoring (NILM) [6]. NILM is the process of estimating the power consumption of multiple appliances within a household based on only the aggregate power consumption from the household's mains inlet. Smart metering technology is a convenient location for energy disaggregation algorithm processing due to its electrical location within the home, i.e., at the source of the installation. Using the outputs of NILM, sensitive information about the consumer can be inferred, such as occupancy tracking or location tracking within the home [7].

As smart metering technology improves, additional sensitive information can be estimated that could potentially lead to personal profiles being built similarly to tracked and targeted advertisement on the internet. There are measures in place with regards to smart meter installation contracts that govern the use of consumer's data by their utility company, however there are possible security breaches that could occur with the smart metering system such as decryption of the smart metering data traffic, or mains 'wiretapping' by unauthorised smart metering installations.

This paper aims to explore and explain the mechanisms that allow private information to be exposed through the use of energy disaggregation and NILM, and to discuss the security concerns that are present within the smart metering architecture. The remainder of this paper is organised as follows. In Section II the technologies that drive smart metering is introduced and explained. In Section III the prominent privacy and security threats due to information extraction from smart metering is explored with examples and case studies from literature. In Section IV the mechanisms for information theft is discussed with a proposal for both technological and policy-based interventions. The paper is concluded in Section V.

II. Smart Meter Technologies

A smart meter is a device that can be used for measuring the power/energy consumption of a household or building, while being able to transmit the recorded data via a communication channel to the consumer's utility company. The simplest smart meters may sample the supply once per second, whilst the most advanced may sample at a rate of up to 30 kHz [8]. Based on the sampled data the active power, reactive power, power factor, and multiple other metrices can be calculated. These metrices are then transmitted to the energy supplier at a lower sample rate, for example every 30 minutes, for further processing such as for accurate billing and to influence the running of the utility network [9]. In comparison, a conventional electricity meter does not send energy usage statistics to the utility company automatically. Instead, a cumulative total of the energy

consumption to date is recorded, which must be routinely recorded in person by the utility company.

Fig. 1 shows an example smart metering design, demonstrating the installation location within the home and the resulting aggregated power measurement that is made. To calculate the various power metrices explained previously, the voltage of the mains supply and the current being drawn from the supply is measured with the use of signal conditioning analogue electronics and high-speed Analogue to Digital Converters (ADCs). For the voltage measurement, isolated conversion from mains voltage to low voltage can be performed using an instrument transformer. Alternatively, non-isolating direct voltage division is possible. For the current measurement, a current transformer, Hall effect sensor, or Rogowski coil can be used to provide isolated current to low signal voltage conversion. After ADC, the sampled data is processed to calculate the metrices, and then transmitted to the energy supplier. The method of transmission depends on the country of installation. For example, in the UK, mobile cellular networks are commonly used for the transmission to the utility company, but other methods such as wireless ad hoc networks and ZigBee are also used [10]. The transmission, storage, and access to data is heavily legislated, with user contracts being required for smart meter installation and operation in domestic environments [11]. In consumer installations it is common to also install a gas smart meter and connected in-home display for user management and information.

III. Privacy and Security Threats

Within the smart metering system, and by applying smart metering technology illegally, there are several privacy and security threats that can affect the consumer and the broader electrical infrastructure. The main mechanism for privacy concerns is the novel technique of energy disaggregation.

A. Non-Intrusive Load Monitoring

NILM is a technique that aims to determine the power usage of the appliances within an electrical system when only the aggregate power usage is known. NILM can be formalised as follows, first measuring the aggregated power within a system, and then estimating the inverse of the aggregation function [12]. Considering a set of $M-1$ devices, each consuming power p_m with $1 \leq m \leq M$, the aggregated power p_{agg} measured by the smart meter will be:

$$p_{agg} = f(p_1, p_2, \dots, p_{M-1}, g) = \sum_{m=1}^{M-1} p_m + g = \sum_{m=1}^{M} p_m \quad (1)$$

where $g = p_M$ is a 'ghost' power consumption (noise) consumed by one or more unknown devices and f is the aggregation function. The goal of NILM is to find estimations for $\hat{p}_m$, $\hat{g}$ of the power consumption of each device m using an estimation method f^{-1} with minimal estimation error and $\hat{p}_m = \hat{g}$, i.e.

$$\hat{P} = \{\hat{p}_1, \hat{p}_2, \dots, \hat{p}_{M-1}, \hat{g}\} = f^{-1}(p_{agg})$$
$$s.t. \operatorname*{argmin}_{f^{-1}} \left\{ \left(p_{agg} - \sum_{m=1}^{M} \hat{p}_m \right)^2 \right\} \quad (2)$$

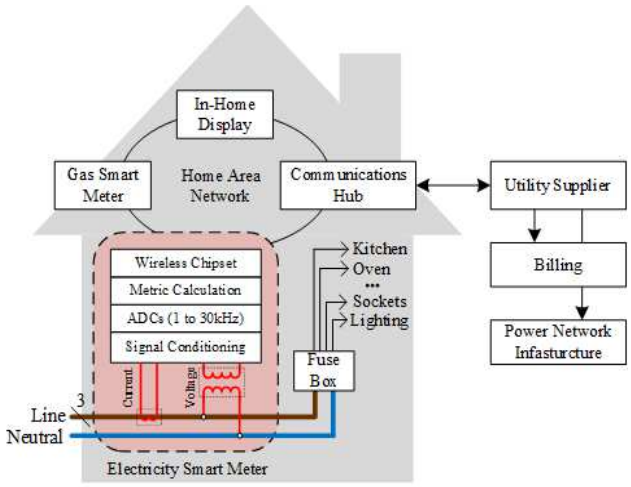

Fig. 1 Residential smart metering design, including communications link to the utility supplier

To estimate $\hat{P}$, NILM uses machine learning to estimate the inverse of the aggregation function, f^{-1}. Fig. 2 shows a NILM block diagram, featuring machine learning based regression using pre-trained appliance models. In its simplest form, there are four main steps of processing. First, the aggregated power, p_{agg}, as sampled by the smart meter is pre-processed to match the scale of the pretrained appliance models, producing p'_{agg}, and then framed into a sliding window, producing p^{τ}_{agg}, with one frame being a vector of multiple sampled measurements, containing the latest sample, and N historic values. In the next step of processing, the statistical and frequency-based features of the frame are extracted and appended to the end of the frame. For example, the standard deviation and the Fourier transform may be calculated based on the input frame; the output values of these processes are then concatenated to the frame, resulting in X^{τ}_{agg}. The features available for extraction by the smart meter is determined by the sampling rate of the ADCs. With a higher sampling rate, more detailed frequency information can be derived and metrices such as harmonic frequency content can be calculated. Table I provides details on some of the most commonly calculated features, showing their requirements for the sampling rate and whether they model steady state or transient behaviour. In detail, for sampling rates less than 100 Hz, active power, reactive power, phase angle, power factor, V-I trajectory, mean values, variance, RMS values, peak values, frequency, and power distribution can be calculated. For sampling rates between 100 Hz – 2 kHz, the 3rd, 5th, and 7th order harmonics, DC component, crest factor, and form factor can be calculated. For sampling rates from 2 kHz – 20 kHz, the harmonic spectrum, High-Frequency (HF) conductance, HF susceptance, wavelets, slope time, rise / fall time, total harmonic distortion, and transient energy can be calculated. Finally, for sampling rates above 20 kHz, wavelets, and EMI can be calculated. In the penultimate step, the resulting data is inserted as a 1-D array to a pretrained regression or classification network, which may be an artificial neural network, long- short-term memory network, or decision tree, for example. In the case of a regression network, the outputs of the network represent the estimates for the power usage for each device that the regression network has been trained in, $\hat{P}$. In the case of a classification

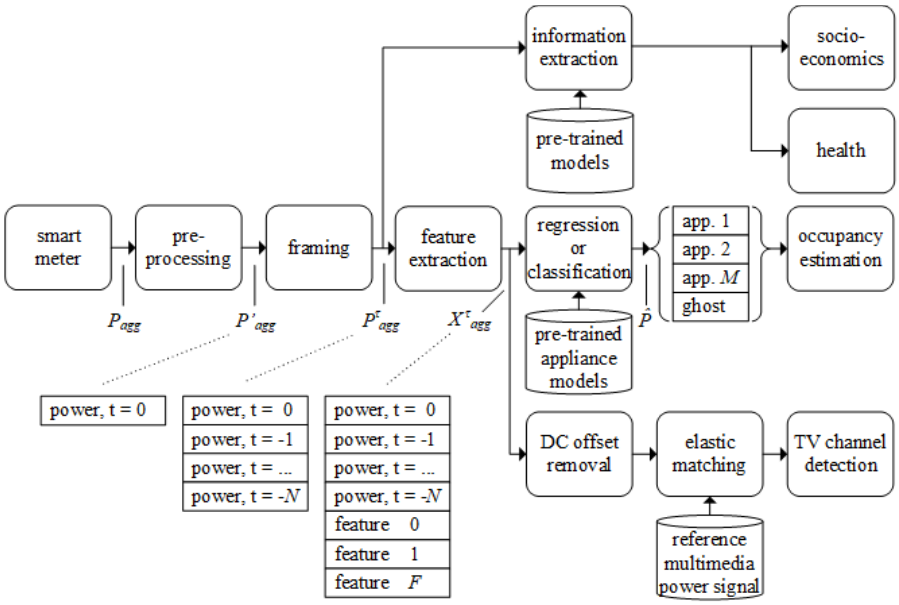

Fig. 2 NILM block diagram for the extraction of socio-economic and health scores, occupancy estimation, and TV channel detection

network, a binary output is produced per pre-trained appliance using an arbitrary threshold, corresponding to whether that appliance is estimated to be turned on or off.

In the NILM scenario, the regression or classification artificial network must be trained using a set of known appliances. This can be achieved by capturing a dataset using intrusive measurements, wherein each appliance in the home has its own smart meter installed that records that appliance's power usage only; a mains inlet power meter is used to record the aggregated power usage. The intrusive load monitors can then be used as a 'ground truth' for supervised learning, allowing the artificial network to learn the disaggregation function.

TABLE I. NILM FEATURE EXTRACTION DETAILS [13]

Feature	Modelling	Minimum Sampling Rate
Active power	Steady state	0 – 100 Hz
Reactive power	Steady state	0 – 100 Hz
Phase angle	Steady state	0 – 100 Hz
Power factor	Steady state	0 – 100 Hz
V-I tragectory	Steady state	0 – 100 Hz
Mean values	Steady state	0 – 100 Hz
Variance	Steady state	0 – 100 Hz
RMS values	Steady state	0 – 100 Hz
Peak values	Steady state	0 – 100 Hz
Frequency	Steady state	0 – 100 Hz
Power distribution	Steady state	0 – 100 Hz
3rd, 5th, 7th Harmonics	Transient	0.1 – 2 kHz
DC component	Transient	0.1 – 2 kHz
Crest factor	Transient	0.1 – 2 kHz
Form factor	Transient	0.1 – 2 kHz
Harmonic Spectrum	Transient	2 – 20 kHz
HF conductance	Transient	2 – 20 kHz
HF susceptance	Transient	2 – 20 kHz
Wavelets	Transient	2 – 20 kHz
Slope time	Transient	2 – 20 kHz
Rise/fall time	Transient	2 – 20 kHz
THD	Transient	2 – 20 kHz
Transient energy	Transient	2 – 20 kHz
Wavelet	Transient	> 20 kHz
EMI	Transient	> 20 kHz

B. *Applications of Non-Intrusive Load Monitoring*

With well-trained NILM machine learning algorithms, it has been demonstrated that more sensitive information such as household occupancy, multimedia content identification, and socio-economic status and health related parameters can be estimated with high accuracy [7, 12, 14].

Specifically, for household occupancy estimation, NILM can be used to determine the on or off binary state of particular appliances based on a predetermined power threshold. Each appliance can fall into one of three categories: appliances that operate independently of user presence, e.g. fridges; appliances with timing that can be turned on by a user and then left on while the user is not present, e.g. dishwashers; and finally appliances that can only operate with user control, e.g. microwaves. Based on the states of appliances that fall into these categories the occupancy of the house can be tracked over time [12].

For multimedia content identification, it has been shown that the multimedia content being viewed on monitors or televisions within the home can be identified with the use of NILM [12]. In comparison to the NILM architecture explained in Section III-A, a DC offset removal process and an elastic matching algorithm process is used in place of the regression or classification network. The DC offset is used to remove high power appliances within the 200 W – 2000 W range, highlighting the contour shape characteristics of the energy signal of devices with lower energy consumption such as a television or monitor. The resulting signal is then used as the input to an elastic matching algorithm comparing the measured signal with a set of reference signals. These reference signals portray the expected energy consumption for a set of known multimedia content, thus allowing identification of the multimedia source [12].

Finally, it has been shown in [12] that socioeconomic information can be extracted using a NILM setup similar to Section III-B, using a Bidirectional Long-Short-Term Memory

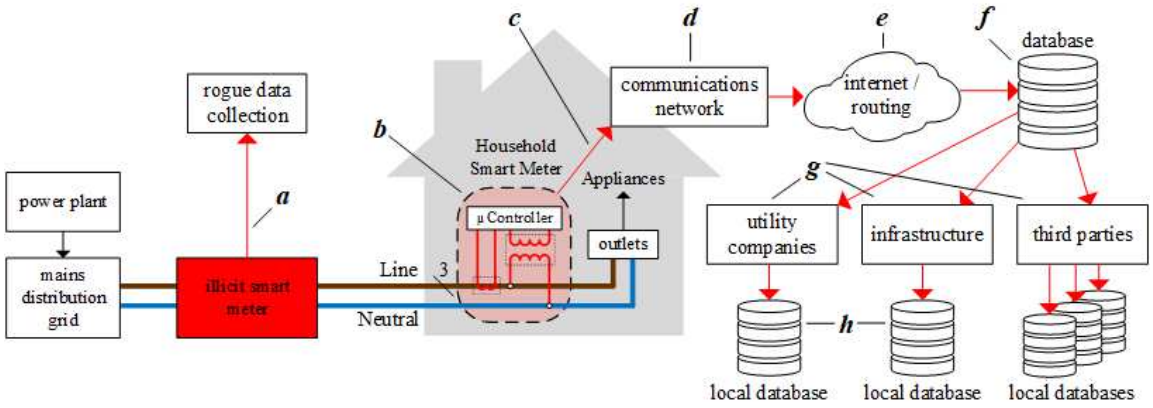

Fig. 3 Smart metering system attack vectors, ranging from physical attacks to network and database attacks

(BiLSTM) artificial neural network that has been trained with an appropriate dataset. Using this method, based on the smart meter data alone, and at a low sampling interval (30min), socio-economic features including house size, house value, resident's income, resident's savings, and social class; and health related features including smoking, exercise, life standard, eating fruits, and eating vegetables could be estimated to a standard higher than a comparable naïve predictor [12].

IV. Discussion

From the above applications of NILM, a clear impact can be seen with regards to the potential breach in privacy to residents that have a smart meter installed into their home, which when used illicitly, may then lead to security issues. For energy disaggregation to take place, first the samples from the residence's smart meter must be attained. This Section explores the possible vectors for attack for the system, or locations, both logical and physical, for theft of smart metering data, then discusses the impact that stolen data may have on the general public, and then proposes possible interventions in both policy and technology.

A. Attack Vectors for Non Intrusive Load Monitoring

Fig. 3 shows the attack vectors that could be used to access smart meter data, then enabling NILM and energy disaggregation to take place by unauthorised parties. In Fig. 3, location *(a)* represents the addition on a rogue smart meter to the property. This could be installed externally to the property without the victim's consent using minimally intrusive detectors such as 'jaw style' current clamps and solderless, clamp on wire taps, used for both powering the rogue smart meter, and for current and voltage measurement. Location *(b)* represents the presence of rogue code running on the residence's own smart meter. Using this method, the residence's smart meter could be used to either perform energy disaggregation on the device or send sampled data to a secondary destination. Location *(c)* represents the wireless communications link from the smart meter via the home area network to the communications hub and the communications and data company. This wireless link can be snooped using off-the-shelf hardware by using either dedicated radio receivers matching the wireless protocol in use, or with the use of Software Defined Radios (SDRs). SDRs have the benefit of being protocol agnostic. Additionally, they can be used to save smart meter wireless transmissions for offline processing, so unauthorised decryption (if encryption is present) can be performed without real-time constraints. Location *(d)* represents data theft from within the communications network itself, for example from within the 4G or Zigbee network infrastructure that is being used for data backhauling to the internet. Location *(e)* represents data theft from the internet. The internet uses indeterminate routing to move packetized data from source to destination; these links can be snooped promiscuously by internet vendors and network orchestrators such as by deep packet inspection. Location *(f)* represents the unauthorised retrieval of data from the data service provider's database, likely to be located on the cloud. This data could be accessed through either physical means by gaining access to the physical servers, or by using network-based attacks. Location *(g)* represents theft from the secondary set of data that is processed by the entities within the energy market. Internally at these organisations, an attack may be made by inserting malicious code to programs that are already processing the smart metering data. Finally, location *(h)* represents the local databases within each energy market entity, similarly to location *(f)*, to retrieve data either physically or via network attacks and unauthorised access.

Each location shown in Fig. 3 offers different amounts of potential data theft. In the case of tampering at locations *(a)* or *(b)*, only the residence's data can be stolen. In addition, the data being stolen is only data that is presently being detected. At location *(c)*, where wireless snooping may take place, multiple residences may be 'eves-dropped' at the same time. Due to the propagation distance of wireless transceivers, multiple smart meters are likely to be detectable from one urban location. In this case, the smart meter data being stolen is still from the present, and not retrospective. Location *(d)* offers a greater number of smart meters data to be stolen in comparison to locations *(a)* – *(c)*, as the communications network is on a local level, for example a town or county. Similarly, to locations *(a)* – *(c)*, only present data is available for theft. Location *(e)* offers a greater number of smart meters to be targeted, however does require a very large amount of data to be processed due to the requirement of filtering the packets from a very large number of irrelevant data sources. Likewise, no retrospective data can be made available. At locations *(f)* – *(h)*, all of the smart metering data may be available for the residences within a given country, including historic data. The availability of historic data is

important as this would allow more accurate profiles to be built per residence. In the case of socio-economic or health related classification, a one-time data theft may prove useful enough to profile a particular set of residences, meaning an on-going attack to the infrastructure is not necessary. In the case of occupancy tracking or multimedia detection, for a useful output to real-time systems, a real-time output of the smart meter may be necessary, requiring a long-term attack.

B. Unauthorised NILM Impact

Presuming an attack is made to the smart metering network resulting in NILM, several types of real-world applications may be attempted, from consumer profiling, to informing organised crime groups. In the case of consumer profiling, as an example, with the use of an estimated socio-economic status score of a residence, an insurance company may alter their premiums to reflect previously unknown information, such as resident's financial savings, or health features such as a resident's fruit and vegetable intake [12]. A resident with more savings and therefore likely higher earnings may be offered a higher premium than their neighbours, resulting in disproportionate pricing. With the use of multimedia elastic matching, a residence may be profiled with regards to their television genre preferences, which may in turn be used to focus advertising towards certain styles of sales tactics or influence the products that are advertised towards. In the case of informing organised crime groups, as an example, a comparison of occupancy profiles may be made to select residences that are more likely to be away from home, or to select residences with known vacationing patterns. Additionally, in the short term, the occupancy of a residence may be determined to enable burglaries to take place knowing that currently no one is home. Furthermore, with the addition of socio-economic data, an organised crime group may select their targets based on estimated wealth. A combination of occupancy tracking, vacationing profiling, and socio-economic profiling could make organised crime both more profitable, and lower in risk.

C. Existing policies

The policies for smart metering privacy and security are set out per country or jurisdiction. Reference [15] provides a summary of 157 articles relating to the privacy and security of smart metering systems, comparing the policies from Canada, France, Netherlands, Norway, the UK, and the US.

Specifically, for the case of the UK, legislation can be found in the *Smart Meters Act (2018)* [9], and the *Data Protection Act (2018)* [16], governing the limits of smart metering technology and the rules that must be followed for data storage, respectively. The *Smart Meters Act* sets the limit to the smart meter reporting interval to no more often than every 30 minutes. In terms of smart meter sampling rate, it is mandated in the UK that suppliers will have to get the customer's consent to access half-hourly data, or to use data for marketing purposes, and that suppliers can access daily data unless the customer objects [9, 17]. Sampling frequency policies for other countries can be seen in Table II. In detail, as stated in [18] the consumers have control over who can access their energy consumption data as well as how often and for what purposes the data is accessed. The only exceptions are required regulated purposes.

Based on these policies, for the countries listed in Table II, attack vectors *(c) – (h)* from Fig. 3 can only provide smart metering data at 30-minute intervals, making occupancy and multimedia detection NILM applications unfeasible, due to their more granular sampling rate requirements. However, as shown in Section III, social-economic and health related scoring is possible with a 30-minute sampling interval. To achieve occupancy estimation and multimedia channel detection, attack vectors *(a)* or *(b)* from Fig. 3 would be required. In the UK, the *Data Protection Act* summarises that data should be encrypted and stored by a reliable third party, data should be anonymized, and data should be deleted or permanently taken out of access after a period deemed reasonable to meet utility load-management goals [16]. This policy further eliminates potential attack strategies as historic data is now limited, thus reducing the amount of data that can be profiled against in retrospect, the inclusion of encryption to data stores further increases immediate access without privileges, and the anonymisation of data removes the link between sampled data and specific residences.

TABLE II. SAMPLING FREQUENCY POLICY PER COUNTRY [15]

Country	Minimum Sampling Interval
Canada	15 minutes
France	30 minutes
Netherlands	Once per month, more with consent
Norway	30 minutes
UK	More than 30 minutes
US	60 minutes

D. Interventions

The prospect of attack vector *(b)* from Fig. 3 being employed would require specific programming and compilation per device. Additionally, complete information about the smart meter would be needed, including calibration data and signal conditioning techniques. Unlike a Linux system that may use different processing applications to perform each function, such as ADC polling, energy consumption calculation, and data transmission to the energy market; the complete program that encompasses all three aspects is compiled down to one set of machine code, since microprocessors without operating systems are commonly used. This makes attack vector *(b)* unfeasible without detailed knowledge of the specific smart meter being targeted. The insertion of malicious code to a smart meter would also require either direct access to the hardware with knowledge of the programming steps, or, if there is an over-the-air update system employed for the smart meter, detailed knowledge of the updating system, or authoritative knowledge of spoofing an over-the-air update system would be needed. From a technological standpoint, to limit the possibility of attack vector *(b)* being used, the safest strategy would be to use only Read Only Memory for the instructions. Additionally, the complete machine code on the smart meter could be hashed at start-up and compared to a known hash, to ensure the machine code has not been altered. From a policy-based standpoint, smart meter hardware design companies must ensure that their IP, hardware design, and software design is kept secure. This could be mandated by law.

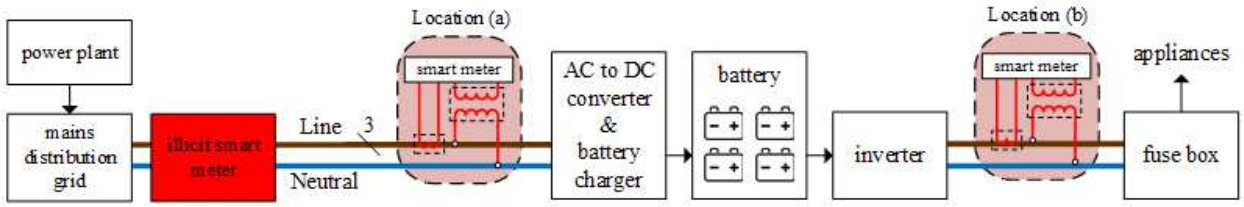

Fig. 4 Smart meter power usage obfuscation based on mains filtering via residential battery installation

For the case of attack vector *(a)*, the installation of a rogue smart meter can only be deterred by physical barriers. If a rogue smart meter is installed outside the premises, there may be no way of telling that a smart meter has been installed. For the case of all attack vectors, from a technological perspective, a potential solution would be to use signal filters on the inlet of the supply, such as a buffering battery storage unit. Fig. 4 shows this concept. In Fig. 4, a battery charging system is the only connection to the mains inlet, with all household appliances drawing from the battery, not the mains supply, via an inverter. In this case, a smart meter positioned outside of the battery powered network, for example an illegally placed smart meter or a genuine smart meter at *Location (a)* in Fig. 4, would not be able to perform energy disaggregation but would still be able to see the energy usage of the property. Additionally, with the use of a smart battery system, the battery could be charged at set times, further obfuscating the energy usage to daily energy consumption, instead of 30-minutely. For the case of *Location (b)* in Fig. 4, the complete energy usage is once again available for NILM techniques to be employed, although different appliance models, socio-economic models, and multi-media consumption detection models would need to be trained due to the particularities of the invertors being used for DC to AC conversion, which are very likely to not be as sinusoidal as the national mains supply.

V. Conclusion

To conclude, it has been shown that energy disaggregation can be used to estimate highly valuable information about the people that live within a smart metered home. Specifically, the occupancy of a home can be tracked, the multimedia consumption of a television can be determined, and the socio-economic status of a home can be estimated to a high degree. When used maliciously these applications can serve as security risks, and the NILM method as a whole can breach the privacy of smart metering users. There are policies in place to protect the general public from malicious smart metering activities from within utility companies, however, the possibility of the addition of physical unauthorised smart meters to the premises is a challenging issue to overcome.

Acknowledgement

This work was partially supported by EDIoT, an H2020 SMART4ALL subproject, funded by the European Commission.

References

[1] "Smart meter statistics in Great Britain: quarterly report to end December 2020", Department for Business, Energy & Industrial Strategy, United Kingdom, 9/03/2021.

[2] "Smart meter customer experience study: executive summary", Department for Business, Energy & Industrial Strategy, United Kingdom, November 2018.

[3] H. Cai, S. Shen, Q. Lin, X. Li, and H. Xiao, ''Predicting the energy consumption of residential buildings for regional electricity supply-side and demand-side management,'' IEEE Access, vol. 7, pp. 30386–30397, 2019.

[4] S. Althaher, P. Mancarella and J. Mutale, "Automated Demand Response From Home Energy Management System Under Dynamic Pricing and Power and Comfort Constraints," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1874-1883, July 2015.

[5] J. G. Pinto et al., "Bidirectional battery charger with Grid-to-Vehicle, Vehicle-to-Grid and Vehicle-to-Home technologies," IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society, 2013, pp. 5934-5939.

[6] G. W. Hart, "Nonintrusive appliance load monitoring", Proceedings of the IEEE, December 1992, pp. 1870-1891.

[7] R. Dong, L. J. Ratliff, Energy Disaggregation and the Utility-Privacy Tradeoff, Big data application in power systems, Elsevier, 2018, Pages 409-444.

[8] J. Gao, E. C. Kara, S. Giri and M. Bergés, "A feasibility study of automated plug-load identification from high-frequency measurements," 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2015, pp. 220-224.

[9] UK Parliament, Smart meters act 2018, [Online]. Available: https://www.legislation.gov.uk/ukpga/2018/14/data.pdf

[10] SmartMe, "Technical Information", SmartMe, https://www.smartme.co.uk/technical.html (Accessed: May 24, 2021).

[11] SMICOP, "Code of practice", https://www.smicop.co.uk/code-of-practice/ (Accessed: May 24 2021).

[12] Schirmer, P & Mporas, I 2021, 'On the Non-Intrusive Extraction of Residents' Privacy and Security Sensitive Information from Energy Smart Meters', Neural Computing and Applications.

[13] P. A. Schirmer, I. Mporas, A. Sheikh-Akbari, "Energy disaggregation using two-stage fusion of binary device detectors," Energies, vol. 13, no. 9, p. 2148, May 2020.

[14] Schirmer, P, Mporas, I & Sheikh-Akbari, A 2021, 'Identification of TV channel watching from smart meter data using energy disaggregation', Energies, vol. 14, no. 9, 2485.

[15] D. Lee, D. J. Hess, "Data privacy and residential smart meters: Comparative analysis and harmonization potential", Utilities Policy, vol. 70, June 2021.

[16] UK Parliament, Data protection act 2018, [Online]. Available: https://www.legislation.gov.uk/ukpga/2018/12/data.pdf

[17] Gov.uk, "Smart meters: a guide", Gov.uk, https://www.gov.uk/guidance/smart-meters-how-they-work#consumer-privacy (Accessed: May 24 2021)

[18] Department for Business, Energy & Industrial Strategy, United Kingdom, "Smart metering implementation programme: review of the data access and privacy framework", 2018. [Online] Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758281/Smart_Metering_Implementation_Programme_Review_of_the_Data_Access_and_Privacy_Framework.pdf, (Accessed on: 24/05/2021).