

# Intrusion Detection in the Smart Grid Based on an Analogue Technique

Hartmut Richthammer and Sebastian Reif<sup>(✉)</sup>

Department Business Information Systems IV - IT Security Management,  
University of Regensburg, Regensburg, Germany  
{Hartmut.Richthammer,Sebastian.Reif}@ur.de

**Abstract.** In Smart Grid a customer’s privacy is threatened by the fact that an attacker could deduce personal habits from the detailed consumption data. We analysed the publications in this field of research and found out that privacy does not seem to be the main focus. To verify this guess, we analysed it with the technique of directed graphs. This indicates that privacy isn’t yet sufficiently investigated in the Smart Grid context. Hence we suggest a decentralised IDS based on NILM technology to protect customer’s privacy. Thereby we would like to initiate a discussion about this idea.

**Keywords:** Smart grid · Smart meter · Intrusion detection system · IDS · NILM · Privacy

## 1 Introduction

During the last years power supply was subject to fundamental changes. In the course of the energy revolution the percentage of fossil fuels and nuclear power decreases and in return the percentage of renewable energies, such as wind and sun, increases. Therefore the energy production is more and more decentralized and the availability changes from static to dynamic. In this context not only a few actors of the infrastructure, e.g. the energy service provider, produce power but also private customers are able to act as producers by installing their own power supplies, e.g. photovoltaics, at their houses. It is also possible to store the power, e.g. in accumulators of electric cars. The former consumer acts as a producer and energy provider as well. We call him *Prosumer*.

To face these new challenges the SG infrastructure concept was established. Due to the increased number of producers it has to be ensured, that the network is not damaged by big deviations of power. In this context detailed consumption data of the *Prosumers* are recorded and sent by the smart meters to the energy service provider. This recorded data threatens the privacy of the *Prosumer*. The SG infrastructure is additionally threatened by external attackers [16, 19].

---

S. Reif—The research leading to these results was supported by “Bavarian State Ministry of Education, Science and the Arts” as part of the FORSEC research association (<http://www.bayforsec.de/>).

It is eligible, to detect these attacks by suitable IDS considering *Prosumer's* privacy. In this paper a new approach is introduced.

## 2 Related Work

We investigated the number of available publications searched by Key Word and Key Word combinations. The queries were based on the IEEE Xplore<sup>®</sup> Digital Library. We think that this database is a quite important one for the research on SG. Nevertheless this restriction is a drawback of our work. In future analyses the search should be extended to other libraries such as Springer or Google Scholar.

### 2.1 Quantitative Analysis

The results gives us a first impression about the focus of actual research on SG and are illustrated in Tables 1 and 2.

The tables show that Smart Grid and privacy with over 10,000 and 20,000 hits respectively are important fields of research besides security.

To find interconnections between different Key Words, we searched for combinations of these terms, Table 2 shows hits on such combinations.

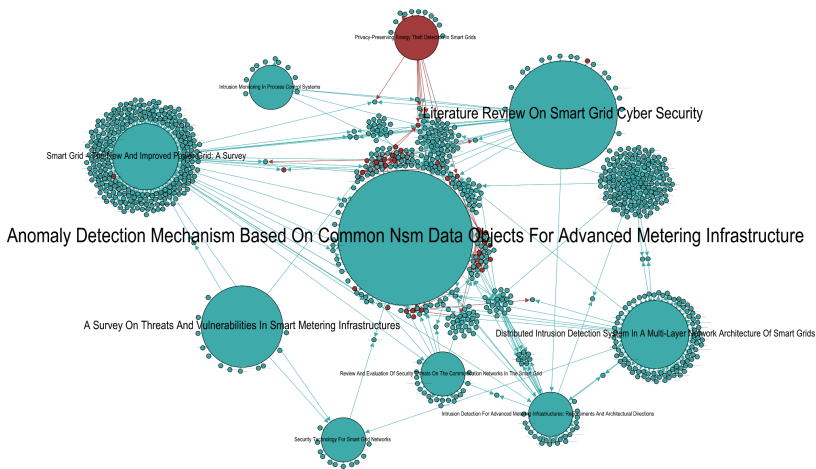
It could be concluded that the research on Smart Grid is mainly focused on security, but privacy is discussed less. Nonetheless protection of privacy in the context of SG is well analysed by many publications [8, 10, 15, 18, 23, 25], IDS and attack vectors on SG are part of the current research [2, 3, 21, 26, 27] as well. The combination of the Key Words *Smart Grid*, *Intrusion Detection* and *Privacy* yields just five publications. It seems that especially privacy in connection with Intrusion Detection for the Smart Grid is not considered sufficiently. IDS aggregate and analyse a lot of data [6] and in addition this data is highly privacy relevant. The consumption data reveals details about the daily routine, consumer behaviour and habits of the residents [12, 22, 23]. However it seems that hitherto IDS is primarily used to protect the energy service provider not the Prosumer. Therefore we think that research with regard to the Prosumer's privacy should be intensified.

**Table 1.** Hits per Key Word (IEEE Xplore<sup>®</sup> digital library).

Key Word	Hits
Smart Grid	10,702
Privacy	20,952
Fraud	1435
Theft	1071
Intrusion detection	9,088
Advanced metering infrastructure	400
Security	126,852

**Table 2.** Hits per Key Word combinations (IEEE Xplore<sup>®</sup> digital library).

Key Word combination	Hits
Smart Grid, Security	1,502
Smart Grid, Privacy	288
Smart Grid, Advanced Metering Infrastructure, Security	84
Smart Grid, Intrusion Detection	52
Smart Grid, Advanced Metering Infrastructure, Privacy	30
Smart Grid, Advanced Metering Infrastructure, Privacy, Security	22
Smart Grid, Advanced Metering Infrastructure, Intrusion Detection	7
Smart Grid, Intrusion Detection, Privacy	5
Smart Grid, Intrusion Detection, Theft, Security	4
Smart Grid, Advanced Metering Infrastructure, Theft, Security	4
Smart Grid, Advanced Metering Infrastructure, Privacy, Theft	4
Smart Grid, Advanced Metering Infrastructure, Theft, Security, Intrusion Detection	4
Smart Grid, Advanced Metering Infrastructure, Theft, Privacy, Security	4



**Fig. 1.** Closeness Centrality of selected survey papers

## 2.2 Qualitative Analysis by Directed Graphs

To measure the impact of single publications we generated a network with directed graphs that shows the interconnections between different papers and their references. Thereby we tried to verify the assumptions we made above. For this purpose the results were processed to more meaningful graphs. We used the “Closeness Centrality” metric, which measures how far a node is away from other ones. A high value means that the publication and their references use lot

of third party references. This suggests that they are survey papers and it is confirmed by a close look. These papers are represented by the nodes shown in Fig. 1. The node size visualises the closeness centrality value. The red coloured nodes represent publications that are related to privacy. As you can see, there is just one node of relevance, which is related to the topic privacy. This affirms our assumptions that privacy is not yet sufficiently investigated.

### 3 NILM Based IDS

NILM was first proposed by Hart [14] in the year 1989. The idea behind this concept is to use only one measurement device to gather consumption data of the whole household. It will be described in Sect. 3.3.

First we will introduce the infrastructure, the interconnection from a household with the SG itself and the IDS components in detail.

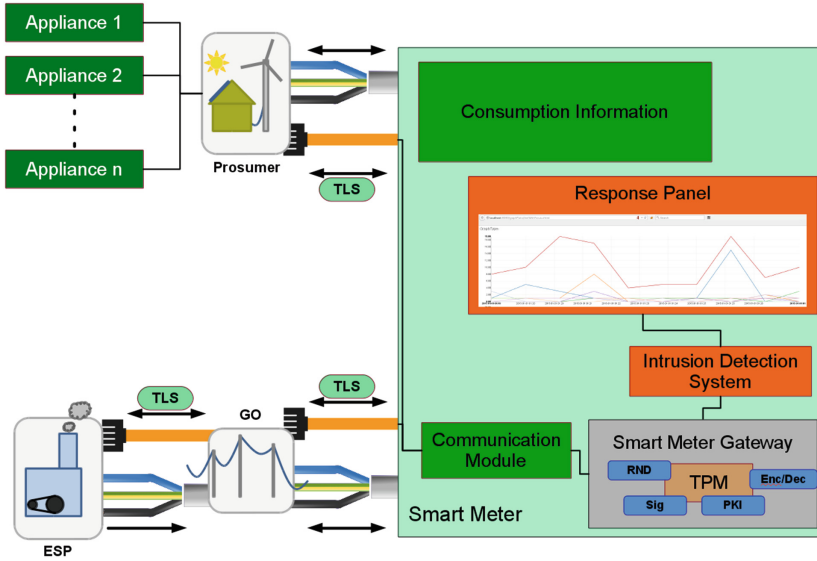
#### 3.1 The Smart Meter Intrusion Detection Infrastructure

In Sect. 2 we have shown that privacy seems not to be an important part for IDS in the SG. The suggested concepts only analyse network traffic [29] and gather information outside the household [2]. Energy fraud and malicious devices which produce unusual consumption of energy are not detected. Salinas et al. [27] introduced an interesting concept for privacy-preserving energy theft detection, where the neighbourhood is involved in the fraud detection. But this concept does not consider the attacker inside a household.

Our approach is a privacy friendly inhouse IDS and was inspired by this idea. We want to reach this goal by developing a decentralized IDS where all relevant energy consumption data is aggregated by a device inside the household. This device should act as central AMS, illustrated in Fig. 2. Every available appliance inside a household is therefore known by the AMS, which is also the SM. Thus it can be avoided that sensitive data is permanently transferred to the energy service provider. The *Prosumers* produces and consumes energy which is depicted as a bidirectional energy flow in the figure. The energy flows through the SM and also bidirectional into the grid. Only the energy flow from the ESP is unidirectional. The data communication between every party is always bidirectional and should be encrypted in accord with the BSI [4].

All appliances consume energy and hence are directly connected with the SM over the powerline. Which leads to that the SM knows the energy consumption behaviour of the household. Inside the SM the following components should be included as it is recommended by the BSI:

- Some kind of user interaction component, where the consumer can monitor his energy consumption, ideally as historical graph.
- A TPM which implements a random generator and securely handles the private keys for decryption and signing.
- A communication module which handles the dataflow between the parties.



**Fig. 2.** Exemplary depiction of a Smart Meter Intrusion Detection Infrastructure. (Some parts of the graphic are from Marekich (Wikipedia) under the CC BY-SA 3.0 licence)

Our approach is to include the IDS and a response mechanism inside the SM. The user now has the possibility to get Informations about security incidents and react on them. How the data is collected and processed will be described in Sect. 3.3. The response system could be an LCD panel, a SMS or E-Mail sender, a web interface or an API where a third party device (e.g. Smartphone App) can connect to.

To detect, categorize and manage all energy consuming household appliances, an analogue technique like NILM could be used. Every device is identified by its individual energy consumption signature. The idea is, when every appliance can be identified inside a household and the normal energy consumption behaviour of a device or the whole system is known, an irregular acting device can be identified. For example a possible attack on an SG could be that high energy consuming devices (e.g. a air conditioning) in a specific region are compromised by a virus. What if all these devices are activated at the same time? A sharply rising energy consumption in this region would be the consequence. If we have a large region and the peak is high enough or the consumption goes over a long period of time, the grid structure could be overstressed and damaged. The data link communication between the malicious device and an attacker can be disguised in the normal internet traffic or over a encrypted communication. But an AMS with an integrated IDS could detect such an irregular energy consumption and counteract it, because an attacker can not hide the irregular energy consumption from the SM.

### 3.2 IDS Structure

Figure 3 shows exemplary the information flow for the IDS structure. A system training phase is necessary before the system can be deployed. A preparation module with a initial dataset trains the IDS. When this phase is finished, the protected system is monitored by an *IDS Module* which is inside the SM. For every incident the response and notification module is triggered. The user can now interact with the system and give response in an appropriate manner. To deal with *false positives* or *false negatives* a feedback channel to the preparation module could be used to adjust the IDS. A detailed structure of the *IDS Module* itself is shown in Fig. 4. The *IDS Knowledge Database* contains the normal behaviour pattern of the household and the appliances. It provides the *Sensor* with information about the normal and abnormal behaviour. A second database

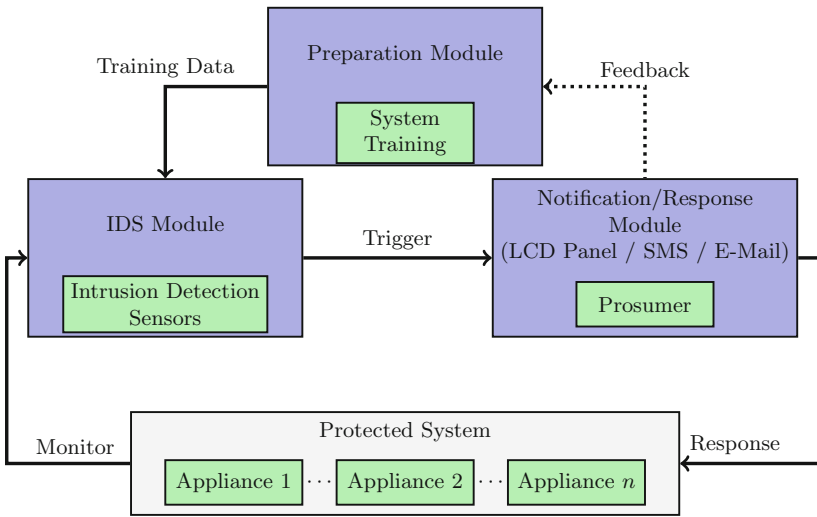


Fig. 3. Intrusion detection system information flow diagram [7].

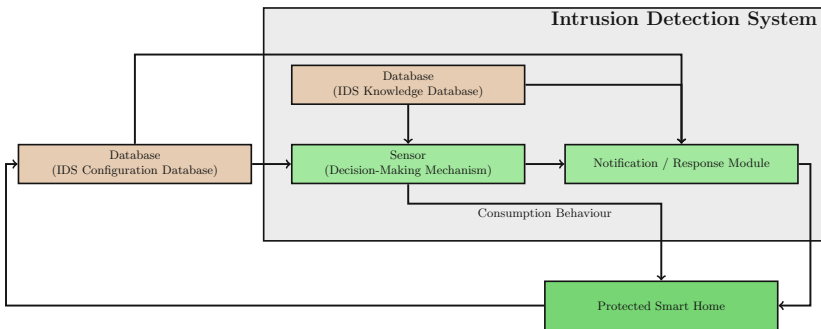


Fig. 4. Intrusion detection system module details [5]

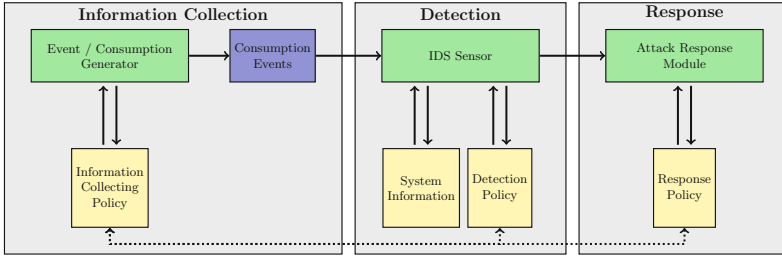


Fig. 5. Intrusion detection system policies [20].

(IDS Configuration Database) could contain IDS specific configuration information (e.g. in which time frame the system should be active). The *Attack Response Module* was already described.

Figure 5 gives an overview about the policy structure from the IDS. The structure is separated in three parts.

**Information Collection**

- **Event / Consumption Generator:**  
The generator is the physical device which collects the real world data. It uses the *Information Collecting Policy* to decide how the information and which information should be collected.
- **Consumption Events:**  
The *Consumption Events* are the resulting data which are generated by the *Event / Consumption Generator*. The events are handled by a storage process and stored in a central location such as a database.
- **Information Collecting Policy:**  
The *Information Collecting Policy* defines how information and which information will be collected. For example the collection intervall which characterizes the period between every collected energy consumption measurement. An external information such as meterological information could also be collected, for example the ambient temperature and general weather information. And of course the timestemp, when the information is collected.

**Detection**

- **IDS Sensor:**  
The *IDS Sensor* analyse the preserved information and tries to detect suspicious or abnormal behaviour. How the collected data is processed is defined by the *Detection Policy*. Also additional *System Information* can be considered for the data analysis by the sensor.

- **System Information:**

To support the *IDS Sensor* during the detection process and the to decide if an anomaly is an attack or a false positive / false negative, additional information for example actual meteorological information like the temperature could be used. The *System Information* provide such kind of information.

- **Detection Policy:**

The *Detection Policy* specifies to which extent the energy flow will be monitored and stored. The *Detection Policy* could also define a value how detailed the collected data is analysed. The policy could also define which algorithm (for example which ML algorithm) is used to process the data. The policy also contains information how the determined results should be interpreted.

## Response

- **Attack Response Module:**

This module contacts the *Prosumer* and informs him or her about an incident. The user can now react on this event and can decide the next steps.

- **Response Policy:**

The policy defines how, when and who gets informed about incidents. For example just the *Prosumer* gets informed or also a centralised database as described in Sect. 4. The information to the user could be committed over SMS, as an E-Mail, over a web interface or an API and a connected Smartphone Application.

The policies could be connected to attach conditions or to sum them up.

### 3.3 How NILM Works

As described before, every device should be identified and be known by the system. At least an abnormal behaviour should be detected. NILM is a concept which can fulfill these requirements. The idea of NILM is over 25 years old and there were many different NILM algorithms and concepts developed since.

We will give a short overview about NILM and how it works. The functionality can be classified in three main principles:

- In the *first* step, characteristic consumption or production data of appliances has to be collected. This means that the overall energy consumption of a household is measured and collected. The collection can be realised by external hardware or within a smart meter. The actual research distinguishes between two different collection methods, the high-frequency and low-frequency data collection. Though there is no exact definition of high-frequency and low-frequency [13, 24, 30, 31].

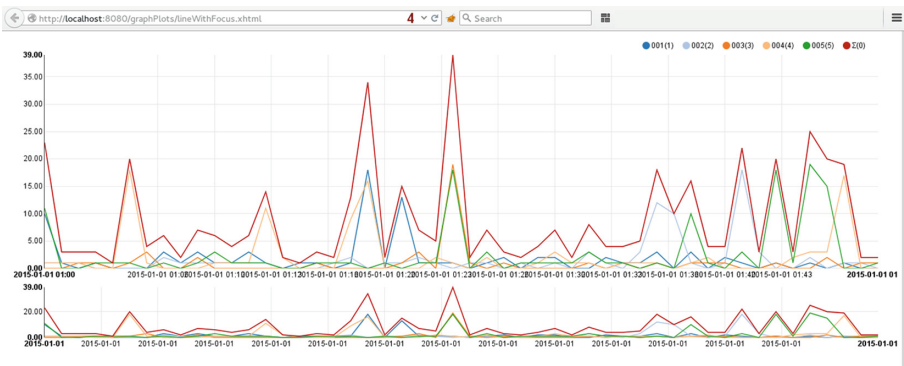


- In the *second* step, collected raw data has to be processed. This process is called *feature extraction*. Its goal is to generate an individual signature for every device [31]. A signature should be unique and describes a characteristic temporal change of consumption of each device. As a data base the real power and reactive power for a device can be used [1, 9, 28].
- After the raw data is analysed and signatures are generated, classification methods are used to disaggregate appliances in a *third* step. The classification can be separated in supervised and unsupervised classification. For the supervised method, labelled datasets are produced. This means that every generated signature is related to a device designation label which is set manually.

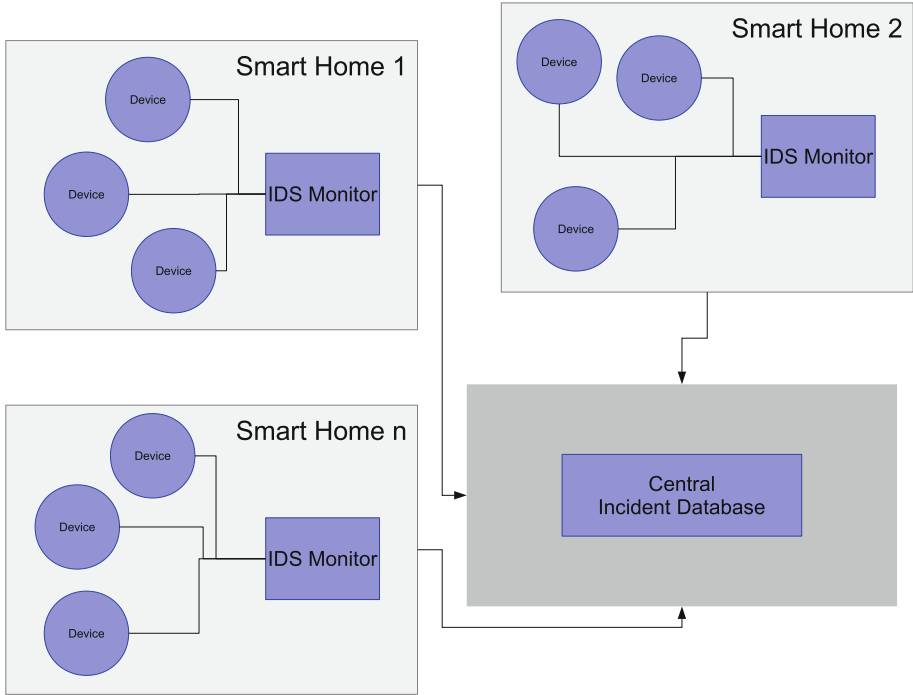
In contrast, the unsupervised classification needs no external influence. This means that the device designation labels are already present in a pre-delivered database [11], are generated from the real power and reactive power plot or use a HMM and variations from this model, for example CFHMM [17].

## 4 Next Steps

Figure 6 depicts an example consumption trace. The red coloured graph shows the overall consumption of a household over a period of time. This trace is known by the SM. The other coloured traces symbolise the energy consumption of appliances inside a household and are inaccessible for the SM. The accumulated consumption of every device inside a household is represented by the overall consumption. If we are able to determine the consumption of every appliance, we are able to detect anomalies. Our next step will be the implementation of AMS, based on NILM technology. We want to find out which NILM concept works best for our IDS idea. Some NILM algorithms and concepts are based on ML algorithms. Our next research steps will go in this direction. We will



**Fig. 6.** Example of an energy consumption graph. The red line shows the overall consumption, the other colours show devices inside a household (Color figure online).



**Fig. 7.** Central incident database.

implement, train and test different ML concepts, based on energy consumption traces gathered in the real world.

For future ideas, the decentralised IDS could be combined with a centralised evaluation and analysis system, for example to detect false positives (Fig. 7). To come back to the air conditioning example, this could also be a false positive, caused by an unusual warm day. If the decentralised IDS of every household communicates incidents to a centralised system, false positives could be detected without revealing privacy relevant consumption data.

## References

1. Baranski, M., Voss, J.: Genetic algorithm for pattern detection in NIALM systems. In: 2004 IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3462–3468. IEEE (2004)
2. Berthier, R., Sanders, W.H., Khurana, H.: Intrusion detection for advanced metering infrastructures: requirements and architectural directions. In: 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 350–355, October 2010
3. Berthier, R., Sanders, W.H.: Specification-based intrusion detection for advanced metering infrastructures. In: 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 184–193. IEEE (2011)

4. BSI. BSI Richtlinien SmartGrid BSI TR-03109-2 - Smart Meter Gateway Sicherheitsmodul Use Cases, March 2013
5. Debar, H., Dacier, M., Wespi, A.: Towards a taxonomy of intrusion-detection systems. *Comput. Netw.* **31**(8), 805–822 (1999)
6. Denning, D.E., Neumann, P.G.: Requirements and model for IDES - a real-time intrusion detection expert system. Document A005, SRI. International, vol. 333 (1985)
7. Dorosz, P., Kazienko, P.: Systemy wykrywania intruzw. VI Krajowa Konferencja (2002)
8. Efthymiou, C., Kalogridis, G.: Smart grid privacy via anonymization of smart metering data. In: 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 238–243. IEEE (2010)
9. Figueiredo, M., De Almeida, A., Ribeiro, B.: Home electrical signal disaggregation for non-intrusive load monitoring (NILM) systems. *Neurocomput.* **96**, 66–73 (2012)
10. Garcia, F.D., Jacobs, B.: Privacy-friendly energy-metering via homomorphic encryption. In: Cuellar, J., Lopez, J., Barthe, G., Pretschner, A. (eds.) *STM 2010*. LNCS, vol. 6710, pp. 226–238. Springer, Heidelberg (2011)
11. Goncalves, H., Ocneanu, A., Berges, M., Fan, R.H.: Unsupervised disaggregation of appliances using aggregated consumption data. In: *The 1st KDD Workshop on Data Mining Applications in Sustainability (SustKDD)* (2011)
12. Greveler, U., Justus, B., Loehr, D.: Multimedia content identification through smart meter power usage profiles. In: *Computers, Privacy and Data Protection* (2012)
13. Gupta, S., Reynolds, M.S., Patel, S.N.: ElectriSense: single-point sensing using EMI for electrical event detection and classification in the home. In: *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, pp. 139–148. ACM (2010)
14. Hart, G.W.: Residential energy monitoring and computerized surveillance via utility power flows. *Technol. Soc. Mag. IEEE* **8**(2), 12–16 (1989)
15. Kalogridis, G., Efthymiou, C., Denic, S.Z., Lewis, T., Cepeda, R.: Privacy for smart meters : Towards undetectable appliance load signatures. In: 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 232–237. IEEE (2010)
16. Khurana, H., Hadley, M., Ning, L., Frincke, D.A.: Smart-grid security issues. *Secur. Priv. IEEE* **8**(1), 81–85 (2010)
17. Kim, H., Marwah, M., Arlitt, M.F., Lyon, G., Han, J.: Unsupervised disaggregation of low frequency power measurements. In: *SDM*, vol. 11, pp. 747–758. SIAM (2011)
18. LeMay, M., Gross, G., Gunter, C.A., Garg, S.: Unified architecture for large-scale attested metering. In: 40th Annual Hawaii International Conference on System Sciences, HICSS 2007, pp. 115–124. IEEE (2007)
19. Lu, Z., Lu, X., Wang, W., Wang, C.: Review and evaluation of security threats on the communication networks in the smart grid. In: *Military Communications Conference, MILCOM 2010*, pp. 1830–1835, October 2010
20. Lundin, E., Jonsson, E.: Survey of intrusion detection research. Technical report, Chalmers University of Technology (2002)
21. McLaughlin, S., Holbert, B., Fawaz, A.-Q., Berthier, R., Zonouz, S.: A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE J. Sel. Areas Commun.* **31**(7), 1319–1330 (2013)
22. Müller, K.: Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. *Datenschutz und Datensicherheit-DuD* **34**(6), 359–364 (2010)

23. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, pp. 61–66. ACM (2010)
24. Parson, O., Ghosh, S., Weal, M., Rogers, A.: An unsupervised training method for non-intrusive appliance load monitoring. *Artif. Intell.* **217**, 1–19 (2014)
25. Petrlc, R.: A privacy-preserving concept for smart grids. *Sicherheit vernetzten Systemen* **18**, B1–B14 (2010)
26. Salem, M.: Adaptive Real-time Anomaly-based Intrusion Detection using Data Mining and Machine Learning Techniques. Ph.D. thesis, Kassel, Univ., Diss. (2014)
27. Salinas, S., Li, M., Li, P.: Privacy-preserving energy theft detection in smart grids. In: 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 605–613, June 2012
28. Streubel, R., Yang, B.: Identification of electrical appliances via analysis of power consumption. In: 2012 47th International on Universities Power Engineering Conference (UPEC), pp. 1–6. IEEE (2012)
29. Valdes, A., Cheung, S.: Intrusion monitoring in process control systems. In: 42nd Hawaii International Conference on System Sciences, HICSS 2009, pp. 1–7. IEEE (2009)
30. Zeifman, M., Roth, K.: Nonintrusive appliance load monitoring: Review and outlook. *IEEE Trans. Consum. Electron.* **57**(1), 76–84 (2011)
31. Zoha, A., Gluhak, A., Imran, M., Rajasegarar, S.: Non-intrusive load monitoring approaches for disaggregated energy sensing: a survey. *Sensors* **12**(12), 16838–16866 (2012)