Intrusion Detection in the Smart Grid Based on an Analogue Technique

Hartmut Richthammer, Sebastian Reif

▶ **To cite this version:**

Hartmut Richthammer, Sebastian Reif. Intrusion Detection in the Smart Grid Based on an Analogue Technique. International Workshop on Open Problems in Network Security (iNetSec), Oct 2015, Zurich, Switzerland. pp.56-67, 10.1007/978-3-319-39028-4_5 . hal-01445793

HAL Id: hal-01445793

https://inria.hal.science/hal-01445793

Submitted on 25 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Intrusion Detection in the Smart Grid based on an Analogue Technique

Hartmut Richthammer, Sebastian Reif*

Department Business Information Systems IV - IT Security Management
University of 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 Intrusion Detection System (IDS) based on Nonintrusive Load Monitoring (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 Smart Grid (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

* 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/).

of the *Prosumer*. The SG infrastructure is additionally threatened by external attackers [16,19].

It is eligible, to detect these attacks by suitable IDSs 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® 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 Table 1 and Table 2.

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 1. Hits per Key Word (IEEE Xplore® Digital Library).

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 [10,22,15,8,25,18], IDSs and attack vectors on SG are part of the current research [2,3,26,21,27] 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. IDSs 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 [22,23,12]. However it seems that hitherto IDS is primarily used to protect the energy service provider not the Prosumer.

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

Table 2. Hits per Key Word Combinations (IEEE Xplore® Digital Library).

Therefore we think that research with regard to the Prosumer's privacy should be intensified.

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 Figure 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 Section 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 Intrustion Detection Infrastructure

In Section 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]

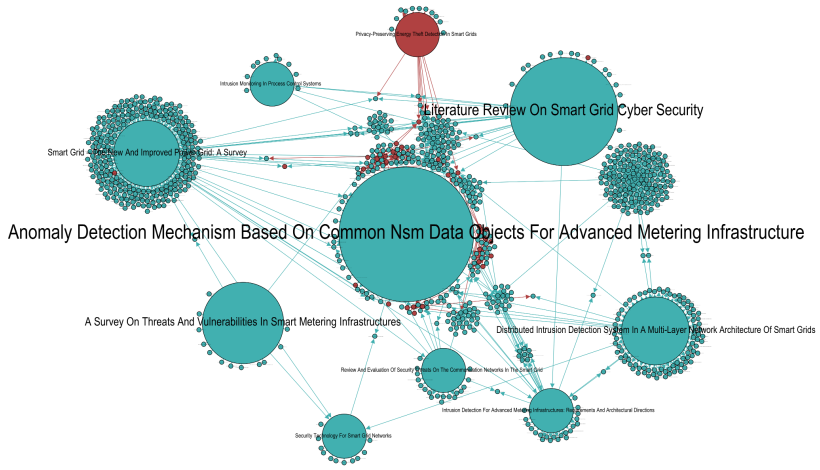

Fig. 1. Closeness Centrality of selected survey papers

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 Appliance Management System (AMS), illustrated in Figure 2. Every available appliance inside a household is therefore known by the AMS, which is also the Smart Meter (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 Energy Service Provider (ESP) is unidirectional. The data communication between every party is always bidirectional and should be encrypted in accord with the Bundesamt für Sicherheit in der Informationstechnik (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 consumpiton, ideally as historical graph.
- A Trusted Platform Module (TPM) which implements a random generator and securely handles the private keys for decryption and signing.

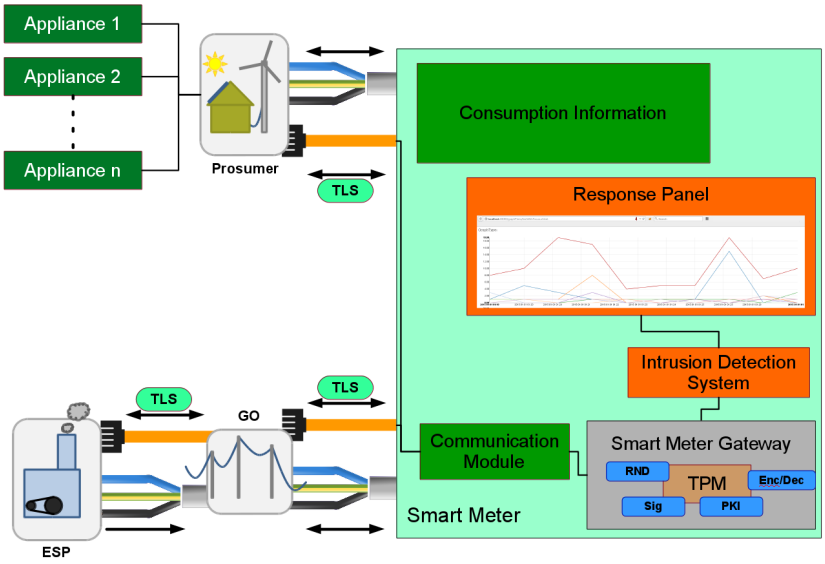

Fig. 2. Exemplary depiction of a Smart Meter Intrustion Detection Infrastructure. (Some parts of the graphic are from Marekich (Wikipedia) under the CC BY-SA 3.0 licence)

– A communication module which handles the dataflow between the parties.

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 section 3.3. The response system could be an LCD panel, a SMS or E-Mail sender, a web interface or an Application Program Interface (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 consump-

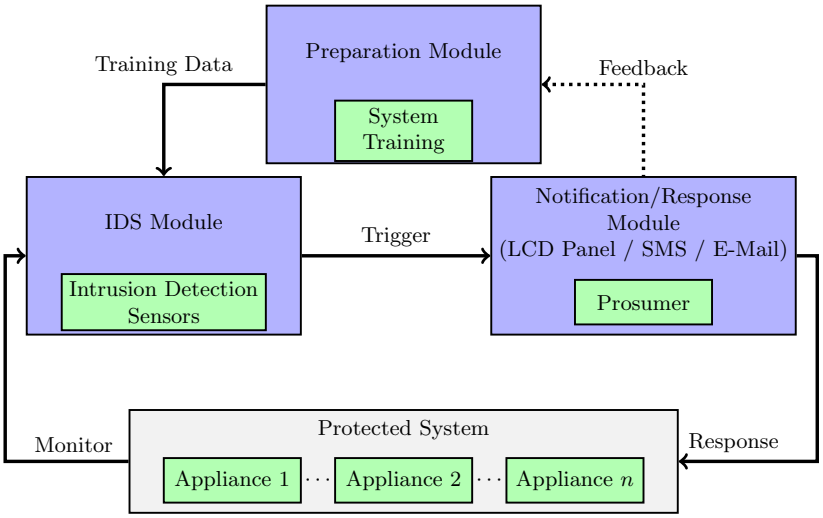

Fig. 3. Intrusion Detection System Information Flow Diagram [7].

tion and counteract it, because an attacker can not hide the irregular energy consumption from the SM.

3.2 IDS Structure

Figure 3 shows examplary the information flow for the IDS structure. A system training phase is nessesary 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 respone 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 Figure 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 *(IDS Configuration Database)* could contain IDS specific configuration information (e. g. in wich 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 seperated 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 meterological information like the temperature could be used. The *System Information* privide 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 Machine Learing (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

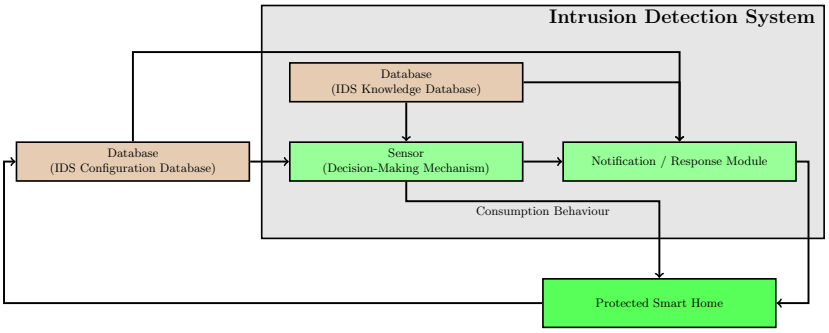

Fig. 4. Intrusion Detection System Module Details [5].

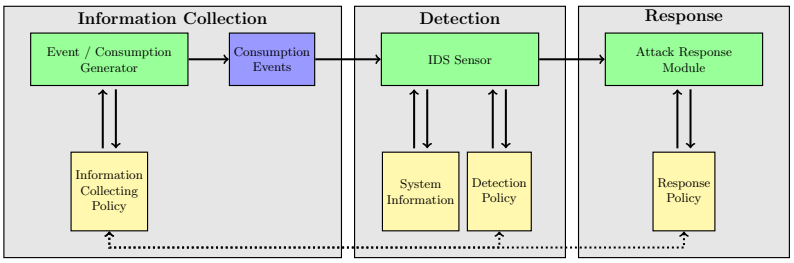

Fig. 5. Intrusion Detection System Policies [20].

example just the *Prosumer* gets informed or also a centralised database as descriped in Section 4. The information to the user could be commited over Short Message Service (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 sytem. At least an abnormal behaviour should be detected. NILM is a concept which can fulfill these requirement. 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 [30,31,24,13].

- 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 [28,9,1].
- 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 Hidden Markov Model (HMM) and variations from this model, for example Coupled factor Hidden Markov Model (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 consupmtion of every appliance, we are able to detect anomalies. Our next step will be the implementation of

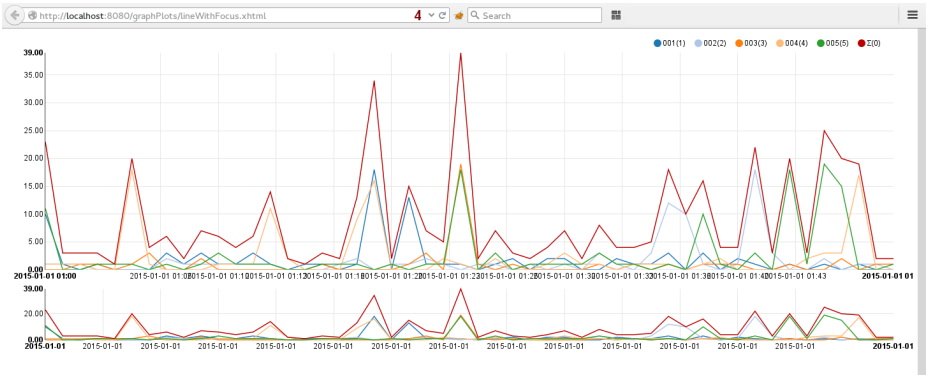

Fig. 6. Example of an energy consumption graph. The red line shows the overall consumption, the other colours show devices inside a household.

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 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 (Figure 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 IDSs of every household communicates incidents to a centralised system, false positives could be detected without revealing privacy relevant consumption data.

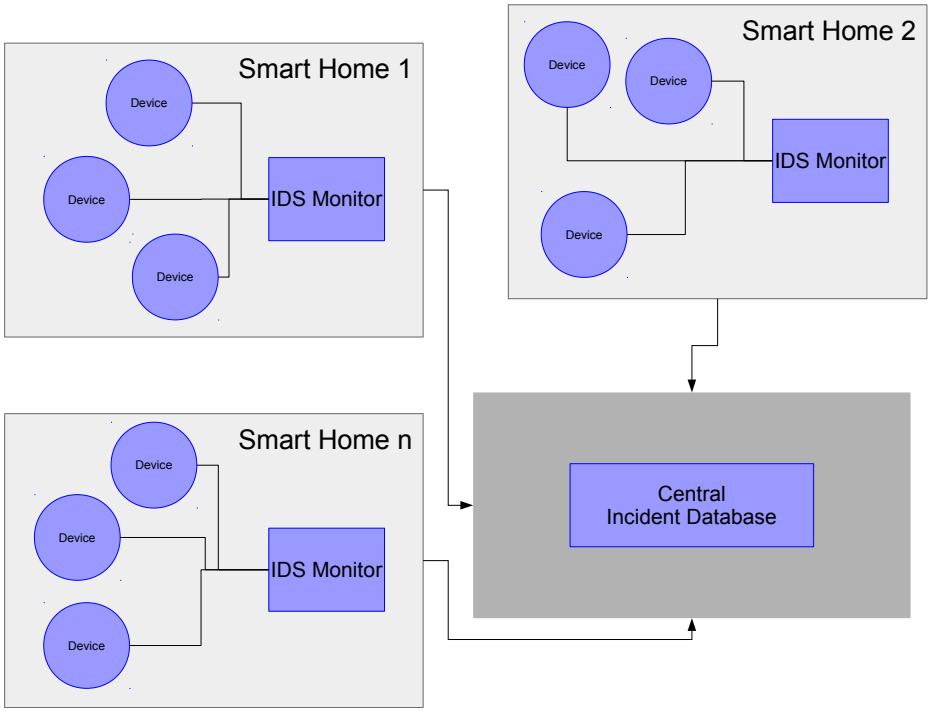

Fig. 7. Central Incident Database.

References

1. Michael Baranski and Jürgen Voss. Genetic algorithm for pattern detection in NIALM systems. In *Systems, Man and Cybernetics, 2004 IEEE International Conference on*, volume 4, pages 3462–3468. IEEE, 2004.

2. R. Berthier, W.H. Sanders, and H. Khurana. Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 350–355, October 2010.
3. Robin Berthier and William H. Sanders. Specification-based intrusion detection for advanced metering infrastructures. In *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, pages 184–193. IEEE, 2011.
4. BSI. BSI Richtlinien SmartGrid BSI TR-03109-2 - Smart Meter Gateway – Sicherheitsmodul – Use Cases, March 2013.
5. Hervé Debar, Marc Dacier, and Andreas Wespi. Towards a taxonomy of intrusion-detection systems. *Computer Networks*, 31(8):805–822, 1999.
6. Dorothy E Denning and Peter G Neumann. Requirements and model for IDES —-a real-time intrusion detection expert system. *Document A005, SRI International*, 333, 1985.
7. Piotr Dorosz and Przemys\law KAZIENKO. Systemy wykrywania intruzów. *VI Krajowa Konferencja*, 2002.
8. Costas Efthymiou and Georgios Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238–243. IEEE, 2010.
9. Marisa Figueiredo, Ana De Almeida, and Bernardete Ribeiro. Home electrical signal disaggregation for non-intrusive load monitoring (NILM) systems. *Neurocomputing*, 96:66–73, 2012.
10. Flavio D. Garcia and Bart Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In *Security and Trust Management*, pages 226–238. Springer, 2011.
11. Hugo Goncalves, Adrian Ocneanu, Mario Berges, and R. H. Fan. Unsupervised disaggregation of appliances using aggregated consumption data. In *The 1st KDD Workshop on Data Mining Applications in Sustainability (SustKDD)*, 2011.
12. Ulrich Greveler, Benjamin Justus, and Dennis Loehr. Multimedia content identification through smart meter power usage profiles. *Computers, Privacy and Data Protection*, 2012.
13. Sidhant Gupta, Matthew S. Reynolds, and Shwetak N. Patel. 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*, pages 139–148. ACM, 2010.
14. George W. Hart. Residential energy monitoring and computerized surveillance via utility power flows. *Technology and Society Magazine, IEEE*, 8(2):12–16, 1989.
15. Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim Lewis, Rafael Cepeda, and others. Privacy for smart meters: Towards undetectable appliance load signatures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 232–237. IEEE, 2010.
16. H. Khurana, M. Hadley, Ning Lu, and D.A. Frincke. Smart-grid security issues. *Security Privacy, IEEE*, 8(1):81–85, January 2010.
17. Hyungsul Kim, Manish Marwah, Martin F. Arlitt, Geoff Lyon, and Jiawei Han. Unsupervised Disaggregation of Low Frequency Power Measurements. In *SDM*, volume 11, pages 747–758. SIAM, 2011.
18. Michael LeMay, George Gross, Carl A Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 115–115. IEEE, 2007.

19. Zhuo Lu, Xiang Lu, Wenye Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. In *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, pages 1830–1835, October 2010.
20. Emilie Lundin and Erland Jonsson. Survey of intrusion detection research. Technical report, Chalmers University of Technology, 2002.
21. Steve McLaughlin, Brett Holbert, Al-Qahtani Fawaz, Robin Berthier, and Saman Zonouz. A multi-sensor energy theft detection framework for advanced metering infrastructures. *Selected Areas in Communications, IEEE Journal on*, 31(7):1319–1330, 2013.
22. Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 61–66. ACM, 2010.
23. Klaus J Müller. Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. *Datenschutz und Datensicherheit-DuD*, 34(6):359–364, 2010.
24. Oliver Parson, Siddhartha Ghosh, Mark Weal, and Alex Rogers. An unsupervised training method for non-intrusive appliance load monitoring. *Artificial Intelligence*, 217:1–19, December 2014.
25. Ronald Petrlic. A privacy-preserving concept for smart grids. *Sicherheit in vernetzten Systemen*, 18:B1–B14, 2010.
26. Maher Salem. *Adaptive Real-time Anomaly-based Intrusion Detection using Data Mining and Machine Learning Techniques*. PhD thesis, Kassel, Univ., Diss., 2014, 2014.
27. S. Salinas, Ming Li, and Pan Li. 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)*, pages 605–613, June 2012.
28. Roman Streubel and Bin Yang. Identification of electrical appliances via analysis of power consumption. In *Universities Power Engineering Conference (UPEC), 2012 47th International*, pages 1–6. IEEE, 2012.
29. Alfonso Valdes and Steven Cheung. Intrusion monitoring in process control systems. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–7. IEEE, 2009.
30. M. Zeifman and K. Roth. Nonintrusive appliance load monitoring: Review and outlook. *IEEE Transactions on Consumer Electronics*, 57(1):76–84, February 2011.
31. Ahmed Zoha, Alexander Gluhak, Muhammad Imran, and Sutharshan Rajasegarar. Non-Intrusive Load Monitoring Approaches for Disaggregated Energy Sensing: A Survey. *Sensors*, 12(12):16838–16866, December 2012.