International Journal of Engineering & Technology, 7 (4.35) (2018) 410-413

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



A New Approach for Privacy-Aware Smart Metering using the Concept of Software Defined Networking

Ahmed Al-Haiqi[1]*, Ammar Ahmed Alkahtani[2], Farah Hani Nordin[3], Mohd Zafri Baharuddin[4]

[1,2,3,4]Department of Electronics and Communication Engineering, University Tenaga Nasional, Kajang, Malaysia
[1]Institute of Power Engineering (IPE), University Tenaga Nasional, Kajang, Malaysia
[2]Institute of Sustainable Engineering (ISE), University Tenaga Nasional
**Corresponding author E-mail: ahmedmubarak@uniten.edu.my*

Abstract

The direct and two-way communication between energy suppliers and high-frequency smart meters enables the suppliers to implement dynamic pricing and manage demand response. Fine-grained monitoring of energy consumption also helps consumers improve their energy profile. This granularity, however, may impose a threat on household privacy. Detailed profile of energy usage can be mapped into detailed profile of daily activities. Many proposals attempted to mitigate this problem and introduce privacy-preserving smart metering. The main approach is to process meter data before they are sent to the energy provider, through de-identification, aggregation or encryption. This processing can take place locally on the smart meter itself, or through a trusted third party. Such solutions suffer from increased smart meter complexity or increased infrastructure complexity, which may render them unacceptable. The idea described in this paper aims to avoid those drawbacks by proposing a new architecture to implement privacy-aware metering. The proposed approach employs the concept of software-defined networking (SDN) to manage smart-meter data in a separate control layer inside the home network. Leveraging the concept of SDN puts the control back in the hands of the consumers to manage their own privacy via SDN applications, and relieves the supplier from enduring extra complexities.

Keywords: *Privacy-aware smart metering; Software defined networking; Smart meters.*

1. Introduction

Smart meters are key components in the emerging smart grid architectures. These measurement tools enable timely, accurate and reliable monitoring of electrical power consumption, which feeds into fast and efficient management of electrical power distribution on the side of energy providers. They also empower the consumers with important data to control their consumption. This precise and real-time load monitoring of user consumption makes smart meters a powerful tool for the purpose of tracing, analysing and profiling user consumption of electrical energy.

This very same ability to produce fine-grained profiles of power usage creates a new issue that is gaining more attention by the research community and privacy activists. People started to notice that the fine-grained data on the use of power can threaten the privacy of the household, because the data from load monitoring can be traced back to the type of electrical appliances they have at their home and their overall daily life routines [1]. Such data can be exploited by third party companies for their interest, either through the utility company or via hacking, without consent from smart meter users. Few research works have already shown that user activities can be exposed from smart meter data at various levels of granularity, down to the point of revealing the TV show that the household have watched [2].

Addressing this privacy issue is in the most interest of both the users of smart meters as well as the utility companies, as this concern can be one of the reasons for reluctant users and hence low deployment rates. Assuring the users of their privacy is expected to enhance their acceptance of the new meters. Indeed, the problem of smart-meter data privacy has led to the introduction of a surge of proposals under the name of privacy-aware smart metering, as well as dedicated websites to spread awareness on the issue (e.g. [3]).

Privacy-aware smart metering is a concept of managing smart meter data with various techniques to ensure that only sufficient amount of smart meter data will be exposed to utility providers. There are many available proposals to preserve privacy for smart meter data, including data aggregation, data anonymization, and data encryption. The proposed manipulations of data are usually executed on the consumer end before sending the data to utility providers for the purpose of billing and monitoring. This concept however often involves other trusted third parties (TTPs), with consumers' consent, to manage their smart meter data.

The problem with all these proposals is that they do not consider the consumers themselves when designing a solution, and hence the users have no control over the amount or type of manipulation that is applied to their smart meter data. In addition, such solutions suffer from two main issues: (1) increased smart meter complexity to cater for the required heavy processing, or (2) increased infrastructure complexity because of introducing TTPs to the meter-supplier communication. Both problems might render privacy-preserving solutions unacceptable by the industry due to complicated instalment, setup, and maintenance processes.

The aim of this paper is to introduce a new approach to address the problem of privacy-aware smart metering, and avoid the above drawbacks at the same time. The proposed approach relies on the emerging paradigm of software defined networking, SDN, to shift the task of managing smart meter data into the hands of the home user through the mechanisms defined by SDN. Software defined

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

networking allows network functions to be programmed and delivered to users via applications. Extending on this concept, smart meters can now be regarded as network devices, and users can be provided with an SDN application to select the type of manipulation to the smart meter data. This solution requires that the smart meter sends its data to the local network instead of broadcasting them to the utility network, but it avoids all other requirements by existing solutions; no TTPs are involved, no custom processing is performed on the smart meter and the users are back in control of their own data.

The focus of this paper is not on the particular manipulation techniques and implementation details. Rather, our objective here is to introduce the general idea and explain the layout of the new approach with an exemplary deployment setup that can be followed in future implementations using any available or novel data processing technique and any specific SDN controller/framework. To the best of our knowledge, this is the first proposal that exploits the power of SDN in implementing privacy-aware smart metering.

2. Background and Related Work

The theme of this paper is to address the problem of smart meter privacy issues using the concept of SDN. This section provides a brief background on the two main components, s*mart meter privacy issues* and *SDN*. In addition, selected references from the most relevant works on privacy-aware smart metering are cited.

2.1. Smart Meters and Privacy

The wide deployment of smart meters led to an increased concern on their implications to consumer privacy. High frequency smart meter data can reveal information on the energy consumption behavior of users, including complex usage patterns such as home occupancy, sleeping routines, eating routines, end even multimedia content [1], [4]–[6]. In response to these concerns, protection of user privacy in smart meter deployments became a hot problem generating a whole literature on privacy-aware smart metering.

A large number of privacy preserving techniques has been proposed, and several works have attempted to survey and classify those techniques (e.g., [7]–[10]). In general, two main approaches can be recognized [11]. One approach is to modify the energy consumption itself, for example, using storage devices, renewables and uninterrupted power supplies and then to filter or reduce sampling rate of the measurements. The other approach is to keep the real energy consumption, and modify meter data before being reported to energy providers. In this paper, we are following the latter approach.

Modifying meter data to preserve privacy can be achieved in many ways, broadly falling into one of three categories. Smart meter data can be anonymized through de-identification techniques with or without the presence of a TTP (e.g. [1], [12]–[14]), aggregated spatially over a group of users or temporally over periods with or without TTP [15]–[17], or obfuscated, e.g., by adding noise [15]. Anonymization and aggregation can be implemented with or without the presence of an independent trusted third party. Further, these techniques can also be augmented with cryptographic measures [18]–[22].

2.2. SDN

Software Defined Networking (SDN) is a new approach for computer networking that changes the way computer networks are built and controlled [23]–[25]. The concept of SDN started to be formulated in academia (by a group of Stanford researchers) in 2008 to address the challenges in managing networks today. Current network devices are typically products of proprietary vendors, and they combine the basic function of forwarding packets along with proprietary software to control that function as well as proprietary interfaces to configure the devices for higher-level policies. Consequently, the management of networks is closely bound to the individual hardware devices that make up the networks, which in turn are proprietary products of individual vendors.

Similar to the situation in the computing industry, in which the hardware that performs the actual computing (e.g. servers) is separate from the software that dictates that computing (i.e. operating systems and applications), the basic idea behind SDN is to separate the actual forwarding function, which is performed in hardware (collectively named as the forwarding or data layer of the network) from the management of those functions, which can be expressed in software (collectively named as the control plane of the network). This separation of concerns promises to create a more flexible network architecture that allows for more innovation and eases the daunting task of network management.

The core architecture of SDN is shown in Figure 1. The original design of SDN comprises three layers and the interfaces between them. The three layers are the infrastructure, controller and application layers, and are often termed as *planes*. Referring to Figure 1, the infrastructure plane at the bottom contains the network devices that perform packet forwarding, i.e. switching and routing; hence, it is also called the *forwarding* plane. The software that is used to program the forwarding plane resides in the control plane. This software implements protocols to control and manage packet forwarding as well as high-level policies. Many of these protocols require global knowledge of the network. In a traditional network, each network device such as a router has its own control plane that runs protocols to synchronize the distributed forwarding tables on different devices across the network. In SDN, the control plane is moved off the switching device onto a centralized controller.

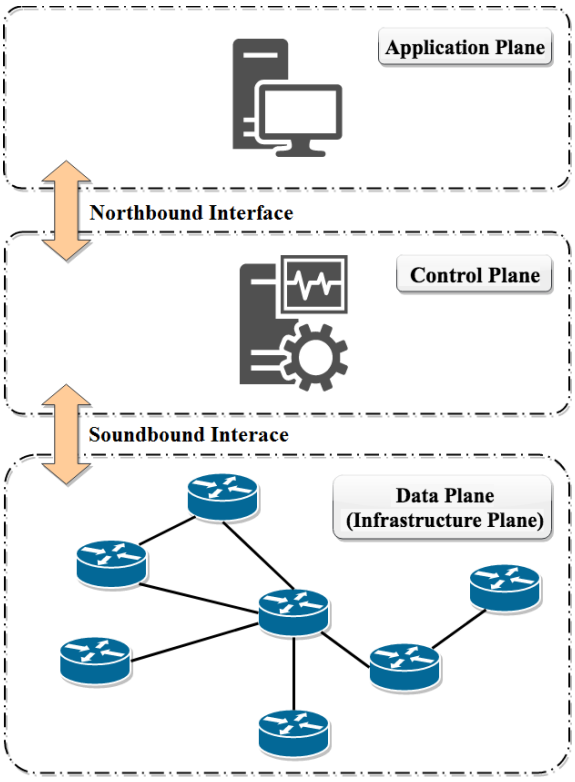


Fig. 1: Basic Architecture of SDN.

The software running on the control plane can instruct the network devices to send network packets to the controller platform before forwarding to the destination. Any kind of processing can be performed on the data in this way using software running on the controller platform (thus, the software-define notation). Controllers are very similar to the concept of an operating system in the computer industry, which introduces the possibility of running network applications on top of the controller in the same way operating systems run computer applications (the upper layer in Figure 1). This possibility allows for a diverse and flexible utilization of

the central controller to dictate different types of processing or manipulation to network traffic. The idea in this paper builds upon this basis.
Although the primary application of SDN was large networks in big datacenters, there is a growing literature on applying SDN in home networks. The application of SDN for privacy-aware smart metering perfectly fits this category of software defined home networks [26].

3. The Proposed Approach: SDN as a Solution

In this section, we present the main idea and a suggested deployment setup for the use of SDN as a solution to implement privacy-aware smart metering. This section contains the main contribution of the paper.

3.1. The Basic Concept

Unlike all other proposals, this paper suggests to (partially) put the control into the hands of the consumers besides the utility company, but not in the hands of any trusted third parties. One way to realize this vision is to consider the smart meter as one of the networked devices that belong to the household, and hence should send its data towards the home router, not outwards. In this case, the home network would manage the data traffic from the smart meter towards the utility company or any other third party.
The idea here is that the home network can somehow manipulate the smart meter data before forwarding them outward, so that only coarse-grained details can reach the outside. Further, it is desired that the type of manipulation can be selected by the household, thereby putting the control of what to send in their hands. This ability is not common in today's networks, and implies the ability to somehow *program* the network to perform the required manipulation and then forward the filtered and processed data.
Fortunately, the idea of *programmed* networks (under the name of SDN) has already emerged and gained great momentum in the networking community, where networks can be configured and controlled by software. Using software to control the network enables the ordinary user to manage certain aspects of the network through user-friendly applications. The main novelty in this proposal is to apply this very concept of SDN to the problem of privacy-aware smart metering

3.2. Overall Architecture

A basic architecture to realize the concept of using SDN in implementing privacy-aware smart metering is shown in Figure. 2. The SDN part in the figure comprises three components: an SDN-enabled router, an SDN controller, and an SDN application that can run on the same computer as the controller or on a separate PC/laptop. In an SDN environment, these components are used to manage the local home network. The smart meter now is but another node in the home network and thus connects to the home router. The utility provider receives all data through the home router.

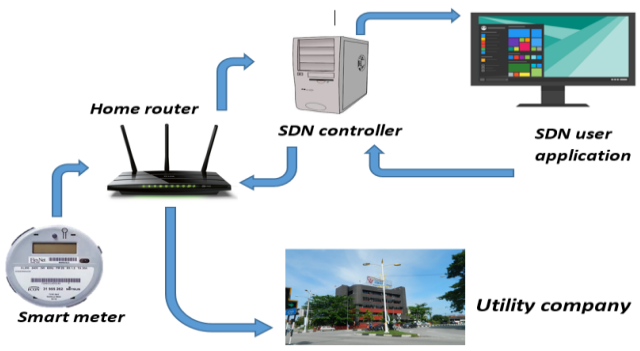


Fig. 2: The overall architecture of the proposed approach.

3.3. Suggested Implementation Setup

Based on the basic architecture in the previous section, the following setup is suggested to deploy the proposed solution:

- Connect the smart meter to the SDN router in the home, so that traffic from the smart meter will be forwarded to SDN controller not to the company network.
- Choose an aggregation algorithm to process smart meter data and write an SDN application to implement the algorithm.
- Build a GUI for the user to select what data can be sent and forward only those data to the utility company network.

This setup is illustrated in a more concrete form in Figure 3. The detailed numbered steps are listed in Figure 4.

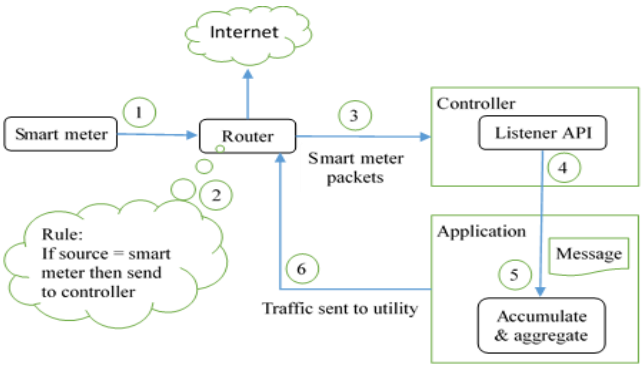


Fig. 3: How SDN application works to protect smart-meter data privacy.

1. Data packets from the smart meter are sent to the router as from any other end-user network device.
2. A flow entry in the router dictates that any packet with a source address that matches the smart meter be directed to the SDN controller.
3. Based on the flow rule above, smart meter data are forwarded to the controller.
4. A listener API in the controller notifies the SDN application of packets arriving from the smart meter. The packets are forwarded to the application as messages.
5. The application extracts the payload of the arriving packets from the smart meter. Based on a time interval, a predefined data size or number of packets, the application accumulates the smart meter readings and then applies an aggregation method on the combined data.
6. The aggregated data are sent as normal network traffic from the application directly to the utility company.

Fig. 4: How SDN application works to protect smart-meter data privacy.

4. Discussion and Conclusions

This paper introduces a novel application of SDN to the problem of preserving privacy in smart metering. The purpose of the paper is to layout and explain the general approach, leaving the actual deployment details for further implementations. This approach still utilizes smart meter data manipulation (SMDM) techniques, and can adopt any existing or new manipulation method. The novelty of the approach is to exploit the emerging paradigm of software defined networking to integrate smart metering and allow for few unique benefits.
On the one hand, deploying SDN and integrating the smart meter in the home network avoids the need for trusted third parties and all associated infrastructure to support their role in smart metering. It also avoids the requirement of physical equipment such as rechargeable batteries and uninterruptable power supplies needed by solutions that attempt to shape the users consumption to protect their privacy. For solutions that manipulate smart meter data, the proposed approach shifts the processing from the smart meter to

the SDN application, removing the need for any complexity on the smart meter itself. These benefits relate to reducing the complexity, and hence the cost, of deploying privacy-aware smart metering, and subsequently increase its acceptance by utility companies.

On the other hand, improving the protection of consumer data and enabling the users to control what data are sent on their consumption behaviour can ensure greater acceptance of smart meter deployment by the consumers. This is an important target that can accelerate the path towards the full potential of smart metering.

There are, however, a couple of limitations that can restrict the acceptance of the proposed approach. First, this solution assumes an SDN-enabled home network, which is completely feasible from a technical perspective at this point, but is still not the mainstream networking technology in homes. Second, this approach requires the utility companies to relinquish their full control over smart meter data and accept to receive the data after some processing or manipulation. This limitation, however, is not specific to the proposed approach, and is common with other privacy-aware smart metering solutions. This is not a trivial problem, and it may be subject to regulatory policies besides utilities' approval. The actual model on which everyone can agree is an open research issue.

Finally, few pointers are in order for our next steps. Validating the proposed approach can be done either via simulation, for example using the Mininet network emulator [27], or through testbed implementation. In either case, the smart meter can be replaced by a stream of metering data, which can be obtained from research-based open datasets such as [28], [29]. The SDN-enabled router can be implemented using the Open vSwitch soft switch [30] embedded in the simulator, or using one of OpenWrt-powered routers [31]. Another alternative is to use special OpenFlow (an SDN protocol) switches such as Zodiac FX [32]. Many open source controllers are available to select from, while the application has to be written against the chosen controller to implement the data manipulation algorithm.

Acknowledgement

This work is supported by project no. RJO10289176/B/1/2017/14 under Start-Up Grant from Universiti Tenaga Nasional, Malaysia.

References

[1] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, 2010, pp. 61–66.

[2] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser, "Neighborhood watch: security and privacy analysis of automatic meter reading systems," in Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 462–473.

[3] Smart Grid Awareness, "How Smart Meters Invade Individual Privacy | Smart Grid Awareness." [Online]. Available: https://smartgridawareness.org/privacy-and-data-security/how-smart-meters-invade-individual-privacy/. [Accessed: 15-Jul-2018].

[4] N. S. Grid, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," Guidel. Sep, 2010.

[5] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, "Non-intrusive occupancy monitoring using smart meters," in Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings, 2013, pp. 1–8.

[6] U. Greveler, P. Glösekötterz, B. Justusy, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in Proceedings of the International Conference on Information and Knowledge Engineering (IKE), 2012, p. 1.

[7] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1732–1745, 2014.

[8] G. Giaconi, D. Gunduz, and H. V. Poor, "Privacy-Aware Smart Metering: Progress and Challenges," arXiv Prepr. arXiv1802.01166, 2018.

[9] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart Meter Data Privacy: A Survey," IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 2820–2835, 2017.

[10] J. E. Rubio, C. Alcaraz, and J. Lopez, "Recommender system for privacy-preserving solutions in smart metering," Pervasive Mob. Comput. vol. 41, pp. 205–218, 2017.

[11] D. G. G. Kalogridis and M. A. Mustafa, "Privacy in Smart Metering Systems," 2015.

[12] R. Petrlic, "A privacy-preserving concept for smart grids," Sicherheit vernetzten Syst., vol. 18, pp. B1--B14, 2010.

[13] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 238–243.

[14] C. Rottondi, G. Mauri, and G. Verticale, "A data pseudonymization protocol for smart grids," in Online Conference on Green Communications (GreenCom), 2012 IEEE, 2012, pp. 68–73.

[15] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in Communications Workshops (ICC), 2010 IEEE International Conference on, 2010, pp. 1–5.

[16] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," Comput. Networks, vol. 57, no. 7, pp. 1699–1713, 2013.

[17] 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 Process. Mag., vol. 30, no. 2, pp. 75–86, 2013.

[18] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, 2012.

[19] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: preserving privacy in the smart grid," IEEE Commun. Mag., vol. 50, no. 5, 2012.

[20] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in International Workshop on Security and Trust Management, 2010, pp. 226–238.

[21] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "DEP2SA: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure," IEEE Access, vol. 3, pp. 2828–2846, 2015.

[22] A. Rial and G. Danezis, "Privacy-preserving smart metering," in Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, 2011, pp. 49–60.

[23] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: an intellectual history of programmable networks," ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 2, pp. 87–98, 2014.

[24] D. Kreutz, F. M. V Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, 2015.

[25] P. Goransson, C. Black, and T. Culver, Software Defined Networks: A Comprehensive Approach. Morgan Kaufmann, 2016.

[26] A. M. Alshnta, M. F. Abdollah, and A. Al-Haiqi, "SDN in the home: A survey of home network solutions using Software Defined Networking PUBLIC INTEREST STATEMENT," Cogent Eng., vol. 5, no. 1, pp. 1–40, 2018.

[27] "Mininet: An Instant Virtual Network on your Laptop (or other PC) - Mininet." [Online]. Available: http://mininet.org/. [Accessed: 15-Jul-2018].

[28] "Smart - UMass Trace Repository." [Online]. Available: http://traces.cs.umass.edu/index.php/Smart/Smart. [Accessed: 15-Jul-2018].

[29] "ACS-F2." [Online]. Available: http://www.wattict.com/web/index.php/databases/acs-f2. [Accessed: 15-Jul-2018].

[30] "Open vSwitch." [Online]. Available: https://www.openvswitch.org/. [Accessed: 15-Jul-2018].

[31] "OpenWrt Project: Table of Hardware: Ideal for OpenWrt." [Online]. Available: https://openwrt.org/toh/views/toh_available_864. [Accessed: 15-Jul-2018].

[32] "Northbound Networks." [Online]. Available: https://northboundnetworks.com/. [Accessed: 15-Jul-2018].