Security-Aware Distributed Service Composition for Wireless Sensor Networks Based Smart Metering in Smart Grid Using Software Defined Networks

Gaolei Li[1], Yang Wu[2], Jun Wu[1](✉), Jianhua Li[1],
and Chengcheng Zhao[1]

[1] School of Electronic Information and Electrical Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{gaolei_li, junwuhn, lijh888, zcc_2633}@sjtu.edu.cn
[2] Electronic Technology Information Research Institute (ETIRI),
Ministry of Industry and Information Technology (MIIT), Beijing 100040, China
wuyang02@163.com

Abstract. To monitor and control the states of surrounding infrastructures in smart grid, wireless sensor networks (WSNs) have been perceived to play an important role in connecting diverse smart meters. However, it also incurs many challenges on network security. Firstly, for WSNs, as data are stored and maintained by a large number of sensors deployed in a distributed way, it is significantly hard to ensure distributed data security by using traditional security protection technologies that only can provides guarantees for small scale centralized local networks. Secondly, more fine-grained access control should be provided for smart meters to adapt to the requirements of the multiparty communications between smart grid stakeholders. In this paper, we propose a security-aware distributed service composition scheme for WSNs based smart metering in smart grid based on software defined networks (SDN). Case studies demonstrate the feasibility of proposed scheme. To our best knowledge, this paper is the first to realize software defined security architecture for WSNs based smart metering in smart grid.

Keywords: Smart grid · Wireless sensor networks (WSNs) · Security-aware Service composition · Software defined networks (SDN)

1 Introduction

Nowadays, since smart grid is evolving towards a user-centered and time-critical application, both data security and networking security have gained increasing popularity to support for various smart grid applications. Security protection usually requires to monitor and control the states of underlying infrastructures. As a critical tool to monitor and control the underlying infrastructures, wireless sensor networks (WSNs) is supposed to have tremendous potentials for smart metering in smart grid [1].

M. Huang et al. (Eds.): WICON 2016, LNICST 214, pp. 91–97, 2018.
https://doi.org/10.1007/978-3-319-72998-5_10

The existing security issues in smart grid can be divided into two main branches roughly including cyberspace security and physical infrastructure safety [2]. In cyberspace security aspect, as a large number of smart devices are deployed in smart grid, more and more data are stored and maintained in a distributed way that enables it significantly harder to ensure distributed data security. In physical infrastructure safety aspect, security threats incurred by hardware aging and misoperations have been minimized significantly with advancement of various novel technologies [3]. Unfortunately, communication latency and network congestion limit the direct usage of existing security policies with high complexity and high time consuming [4], and high packet loss rate may lead to service interruption, even cause a chain of accidents in field-level networks of smart metering in smart grid [5].

Recently, researchers presented WSNs to monitor and control smart grid infrastructures. However, different from traditional centralized security architecture, in which firewall, traffic control software and other complex products are usually deployed at the export of an internal network. WSNs based smart metering achieves security threats by deploying distributed sensors and aggregates data from the surrounding sensors. In this paper, we propose a security-aware distributed service composition (SDSC) scheme. It exploits software defined networks (SDN) to improve WSNs based smart metering in smart grid.

2 Related Work

The existing security prevention approaches can be divided into two branches roughly: (1) centralized model, and (2) distributed model. While cloud based smart grid have better resilience, cloud itself faces many challenges on remote communication efficiency. Distributed model consumes less bandwidth and energy. Therefore, distributed model has gained increasing attention in recent years. For example, literature [6] proposed a fine-grained distributed data access control to ensure sensed data security in WSNs. However, different from traditional WSNs, it is infeasible for smart grid monitoring to deploy diverse complex security applications due to high time-consuming. Therefore, there are many challenges on WSNs based smart grid monitoring [7].

SDN is a novel paradigm that decouples logic functions from data plane, and implements them in a centralized controller. It has been perceived to have specific capability for utilization by various wireless scenes. In [8], a stateful SDN solution proposed for WSNs can reduce the amount of information exchanged between sensor nodes and make sensor nodes programmable.

The Service Composition (SC) is a popular approach to implement value-added services by combining other basic services in many application scenes (such as smart building, QoS provisioning and next-generation service overlay network [9]). And also, the prospects of SC for intelligent transportation and smart grid have traditionally been addressed separately in literature [10]. With the SC, interoperability, flexibility and reusability of a system can be improved significantly. However, due to the dynamicity and heterogeneity of the target smart meters, the security services offered by advanced metering infrastructure (AMI) cannot be composed by extending existing Service

Oriented Architecture (SOA) approaches simply. For SC in AMI, it may need the integration of a number of real-world services, which must be an security-aware process.

3 Modeling of SDSC Scheme

In this section, we describe the proposed SDSC scheme that allows networking security functions to be deployed at sides of infrastructures in a distributed way adaptively and dynamically.

3.1 Networking Model

The basic architecture is shown as illustrated in Fig. 1. With this architecture, the visibility, flexibility and scalability of the whole network for WSNs based smart grid metering can be improved significantly.

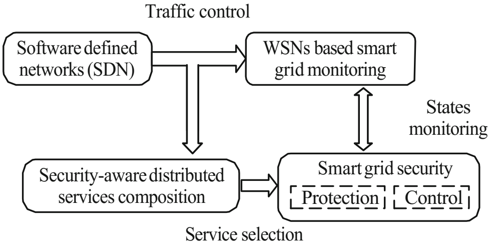
Traffic control
Software defined networks (SDN)
WSNs based smart grid monitoring
States monitoring
Security-aware distributed services composition
Smart grid security
Protection
Control
Service selection

Fig. 1. Basic logic architecture of the proposed SDSC scheme.

In smart grid, there are three constraints limiting the application of security policy for dispersive infrastructures: (1) energy; (2) and network capability. In the following, we set up a fined-grained optimization model to present proposed SDSC scheme. The basic network model L is modeled as a non-reflexive logic graph $H^L = (V^L, E^L)$, where $V^L = \{n_1, n_2, \ldots, n_N\}$ is a set N logic nodes and $E^L = \{e_{ij}\}$, with i and $j = 1, 2, \ldots, N$, is a set of logic nodes, with $\{e_{ij}\}$ connecting n_i to n_j. The security optimization model is described by a *Security Configuration Matrix*. The *Security Configuration Matrix* is defined by $AB = [AB_{ij}]$, where AB_{ij} defines the security states after security policy configured. For logic nodes V^L, it is noted as AB^V_{ij}; for links $\{e_{ij}\}$, it is noted as AB^E_{ij}. The *Used Logic Nodes Security Configuration Matrix* is defined by $ABu^V = \left[ABu^V_{ij}\right]$, where ABu^V_{ij} defines the security states of V^L already configured to logic nodes. $ABu^V_{ij} = \infty$, when $j \geq 2$. The *Used Link Security Configuration Matrix* is defined by $ABu^E = \left[ABu^E_{ij}\right]$, where ABu^E_{ij} defines the security states of $\{e_{ij}\}$ already configured to links.

3.2 The Resource-Constrained Model

The resource-constrained model is formulated by a *Energy Matrix*, a *Network Capability Matrix*. The *Energy Matrix* for logic nodes is defined by $E^V = \left[E_{ij}^V\right]$. The *Used Logic Nodes Energy Matrix* is defined by $Eu^V = \left[Eu_{ij}^V\right]$, where Eu_{ij}^V defines the energy of V^L has been occupied. $Eu_{ij}^V = 0$. The *Network Capability Matrix* is defined by $AD^E = \left[AD_{ij}^E\right]$. The *Used Network Capability Matrix* is defined by $ADu^E = \left[ADu_{ij}^E\right]$, where ADu_{ij}^E defines the total network capability of $\{e_{ij}\}$ already allocated to links.

3.3 Security Optimization

Both link security and node security are supported in our proposed scheme. The Security Request Model are shown by divisions into the link security request model and the node security request model as follows.

The Link Security Model

Let G be the number of requests that are processed simultaneously. The *g-th* request, with $g = 1, 2, \ldots, G$, is defined by a set of K_g 2-node directed virtual graph $H^{V_{kg}} = (V^{V_{kg}}, E^{V_{kg}})$, with $k = 1, 2, \ldots, K_g \cdot K_g > 1$ represents for a complex data delivery process, in which multiple source nodes and multiple destination nodes should be connected. For each k, $V^{V_{kg}} = \left\{n_s^{kg}, n_d^{kg}\right\}$ is a set of 2-nodes that consist of the source node n_s^{kg} and the destination node $n_d^{kg} \cdot E^{V_{kg}} = \left\{e_{sd}^{kg}\right\}$ denotes the virtual link connecting n_s^{kg} and n_d^{kg} with bandwidth which is equal to ad_{kg}. We define boolean $X^{kg} = \left[x_{ij}^{kg}\right]$, where:

$$x_{ij}^{kg} = \begin{cases} 1 & \text{if} \left\{e_{ij}^{kg}\right\} \text{uses} \{e_{ij}\} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

and by definition $x_{ii}^{kg} = 0, \forall i$.

The virtual-to-logic link mapping is formulated as $x_{ij}^{kg} \leq A_{ij}, \forall (i,j)$, which guarantees only existing links are assigned for link requests. The network capability of each link is usually limited, bandwidth allocated for each link should satisfy this constraint:

$$\sum_{g=1}^{G} \sum_{k=1}^{K_g} x_{ij}^{kg} \cdot \mathrm{ad}_{kg}^E \leq AD_{ij}^E - ADu_{ij}^E, \forall (i,j) \tag{2}$$

This constraint guarantees that link bandwidth will not exceed the total network capability. The link security request mapping is formulated as the following equation:

$$\sum_{g=1}^{G}\sum_{k=1}^{K_g} x_{ij}^{kg} \cdot Z_{ij}^{kg} \le AB_{ij}^{E} - ABu_{ij}^{E}, \forall(i,j) \tag{3}$$

The Node Security Model

In this paper, the energy consumption of security service on a logic node is defined by $E = [E_x]$, with $x = \{c, e, r, a\}$. For logic nodes V^L, it is noted as E_x^V. Considering the *Energy Matrix* $E^V = \left[E_{ij}^V\right]$ defined in advance, the g-th request of logic node require E_x^g energy. They should satisfy the following constraints:

$$\sum_{g=1}^{G} sum\{E_x^g\} \le E_{ij}^V \tag{4}$$

Where $sum\{\cdot\}$ is an addition operator. For example, $sum\{E_x^g\} = E_c^g + E_e^g + E_r^g + E_a^g$.

The design of the *Objective Function* is affected by multidimensional considerations. Firstly, data are usually delivered by using publisher/subscriber mode or broadcast/multicast mode. Therefore, data flows in the network often suffer from traffic fluctuation. To reduce packet loss and latency time, and guarantee the end-to-end communication efficiency, traffic control involved network applications such as multi-path transmission, rate control and congestion must try to gain the highest revenues.

4 Analysis

In this section, we will discuss how our proposed scheme applies to the WSNs based smart grid metering. We use T_x, U_x, A_x, E_x to represent traffic control, user authentication, access control and exception auditing separately. The value of each element may not be quantified. For non-quantified attributes in Table 1, classical binary-classifier can be used to build a machine learning system. Each node has to compute a a series of energy consumption E_c and computation complexity C_c. The computation equation is listed as deduced in Sect. 3.

Table 1. Security services and protection level.

Protection level	QoS services	Traffic control	User authentication	Access control	Exception auditing
1	$\le Q_1$	$\le T_1$	$\le U_1$	$\le A_1$	$\le E_1$
2	$\le Q_2$	$\le T_2$	$\le U_2$	$\le A_2$	$\le E_2$
3	$\le Q_3$	$\le T_3$	$\le U_3$	$\le A_3$	$\le E_3$
…	…	…	…	…	…
W	$\le Q_w$	$\le T_w$	$\le U_w$	$\le A_w$	$\le E_w$

Compared with other works, our work provides a multidimensional security-aware functions including priority, configuration, access control and authentication, while others work usually focusing on data aggregation. The security of WSNs based smart grid metering is enhanced at the cost of additional overhead. The SDSC scheme designed for WSNs based smart grid using SDN simplifies the logic management complexity at a price of extra implementation computation. The more sensors deployed in the network, the less average extra overhead the scheme will cost (Table 2).

Table 2. Objective value.

	Confidentiality	Encryption	Redundancy	Authorization
Energy consumption	$\leq E_c$	$\leq E_e$	$\leq E_r$	$\leq E_a$
Computation complexity	$\leq C_c$	$\leq C_e$	$\leq C_r$	$\leq C_a$

5 Conclusion

In this paper, we propose a security-aware distributed service composition (SDSC) scheme for WSNs based smart grid metering based on software defined networks (SDN). The feasibility of the proposed scheme is demonstrated by analysis. For distributed data security, SDSC scheme supports LN-aware fine-grained protection by using dynamic security policy configuration. For time-critical applications, communication latency and network congestion can be reduced significantly.

Acknowledgement. This work is supported by National Natural Science Foundation of China (Grant No. 61431008, 61571300, 61401273).

References

1. Al-Anbagi, I., Erol-Kantarci, M., Mouftah, H.T.: An adaptive QoS scheme for WSN-based smart grid monitoring. In: IEEE International Conference on Communications Workshops (ICC), pp. 1046–1051 (2013)
2. Yan, Y., Qian, Y., Shariff, H., Tipper, D.: A survey on cyber security for smart grid communications. IEEE Commun. Surv. Tutorials **14**(4), 998–1010 (2012)
3. Rashid, M.T.A., Yussof, S., Yusoff, Y., Ismail, R.: A review of security attacks on IEC61850 substation automation system network. In: Information Technology and Multimedia (ICIMU), pp. 5–10 (2014)
4. Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, R., Tan, J.-C.: Security analysis and auditing of IEC61850 based automated substations. IEEE Trans. Power Deliv. **25**(4), 2346–2355 (2010)
5. Kong, P.Y.: Wireless neighborhood area networks with QoS support for demand response in smart grid. IEEE Trans. Smart Grid **7**(4), 1913–1923 (2016)
6. Yu, S., Ren, K., Lou, W.: FDAC: Toward fine-grained distributed data access control in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **22**(4), 673–686 (2011)
7. Yassine, A., Rahimi, H., Shirmohammadi, S.: Software defined network traffic measurement: current trends and challenges. IEEE Instrum. Meas. Mag. **18**(2), 42–50 (2015)

8. Galluccioa, L., et al.: SDN-WISE: design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks. In: IEEE Conference on Computer Communications (INFOCOM), pp. 513–521 (2015)
9. Paganelli, F., Ulema, M., Martini, B.: Context-aware service composition and delivery in NGSONs over SDN. IEEE Commun. Mag. **52**(8), 97–105 (2014)
10. Dán, G., Bobba, R.B., Gross, G., Campbell, R.H.: Cloud computing for the power grid: from service composition to assured clouds. In: 5th USENIX Workshop on HotCloud (2013)