The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 4 (2018) 30–34

www.elsevier.com/locate/icte

Impact of optimal false data injection attacks on local energy trading in a residential microgrid

Shama N. Islam*, M.A. Mahmud, A.M.T. Oo

School of Engineering, Deakin University, Geelong, Australia

Received 1 December 2017; received in revised form 17 January 2018; accepted 18 January 2018
Available online 21 February 2018

Abstract

This paper illustrates the vulnerability of local energy trading to false data injection attacks in a smart residential microgrid and demonstrates the impact of such attacks on the financial benefits earned by the participants. In a local energy market, the attacker can overhear the energy generation and consumption patterns of legitimate participants and based on this, optimize its attack signal to achieve maximum benefits either as a buyer/seller, while balancing the supply–demand to remain undetected. For such a system, we have formulated an optimization problem at the attacker, to extract the maximum possible benefits from legitimate participants. The numerical results show that the false data injection from the attacker causes significant losses in the benefits of legitimate participants, up to a reduction of 94% in certain hours.

Keywords: Local energy trading; Microgrid; False data injection; Optimum attack; Smart grid

1. Introduction

The increasing penetration of renewable energy resources in power systems along with the urge for achieving better power quality in a reliable manner have resulted into widespread deployment of distributed generation technologies. Moreover, the traditional power grid is transforming from its complex and intricate nature towards systems embedded with intelligent control and communication. In this respect, the concept of a smart microgrid has attracted significant interest, especially in remote communities. To harness the maximum benefits of intermittent renewable energy generation, local energy trading among households in a residential microgrid has evolved as a highly effective approach [1].

In a residential microgrid, different houses may have different demand profiles and different capacities for renewable generation and storages. Moreover, the intermittency of renewable generation technologies can lead to energy surplus in some houses, while energy deficit in some other houses. Thus, the houses with surplus can sell the excess energy to houses with deficit, which is termed as local energy trading. However, the effectiveness of local energy trading critically depends on the availability of energy consumption/generation information, as well as the reliability of energy trading signals [2]. This becomes increasingly important with the adoption of internet of things (IoT) technologies for energy management in smart grids [3].

A number of existing studies have outlined the vulnerabilities of smart grid systems from cyber security threats, especially arising from proprietary communication protocols whose security can be breached [4]. The security objectives for different smart grid applications have been identified and to fulfill these objectives, privacy preserving authentication frameworks based on group keys are introduced in [5]. The authors in [6] have outlined a number of privacy preserving schemes for a range of applications in smart grid including data aggregation and smart home gateways.

* Corresponding author.
E-mail addresses: shama.i@deakin.edu.au (S.N. Islam), apel.mahmud@deakin.edu.au (M.A. Mahmud), aman.m@deakin.edu.au (A.M.T. Oo).

Peer review under responsibility of The Korean Institute of Communications Information Sciences.

https://doi.org/10.1016/j.icte.2018.01.015

Apart from authentication and access control mechanisms, different studies have considered intrusion detection techniques to mitigate the impact of attacks from compromised devices [7]. The authors in [8] have proposed a distributed intrusion detection technique for SCADA systems and evaluated the technique using hybrid testbed for electrical distribution network. On the other hand, [9] introduces Hidden Markov Model-based intrusion detection for SCADA systems for a range of attack vectors.

The aforementioned works have not investigated the impact of such security threats on local energy trading applications in a smart microgrid. The existing studies on local energy trading consider issues like false bids placed by legitimate participants or impersonation attacks, eavesdropping and denial of service attacks [10]. To mitigate such threats, the authors in [11] adopt privacy preserving encryption schemes. However, such schemes may not secure the local energy market from false data injection, which can cause significant financial losses.

In a local energy market, trusted third parties may act as an attacker and cause loss of benefits for the legitimate participants, whereas harnessing benefits for itself. In this respect, there has not been any investigation in the literature on how the attacker can optimally design attack signal to extract the maximum benefits from legitimate participants in the local energy market. To address the problem, we have made the following contributions in this paper:

- We have investigated the optimum attack signal design to extract the maximum benefits from legitimate participants while minimizing the supply–demand mismatch to ensure that the attack remains undetected.
- We have shown that in the absence of an attacker, the households participating in local energy trading can earn significant profits/savings, especially when a house has energy excess(deficit) and other houses are in deficit(excess).
- We have demonstrated that in the presence of an attacker, the profits/savings at the legitimate participants have significantly decreased, up to 94% at certain hours.

The rest of the paper is organized in the following manner. Section 2 describes the system model. Section 3 details the problem formulation for optimum attack generation. Section 4 demonstrates the numerical simulation results obtained for the problem under consideration. Finally, Section 5 outlines the concluding remarks.

2. System model

A residential microgrid, comprised of L number of households equipped with solar panels, battery energy storage systems (BESSs) and HEMSs is considered. Due to intermittent renewable energy generation, there might be energy excess or energy deficit at different households. These energy mismatch values will be reported by HEMSs to the central EMS. It is assumed that there are C EMSs in the microgrid and each EMS monitors the energy generation and consumption of L_c households. Based on these, the EMS manages the energy trading operation among the monitored households with non-zero energy mismatch.

Each EMS is indexed by $c \in [1, C]$ and each household monitored by the cth EMS is denoted by $\ell_c \in [1, L_c]$. The amount of solar energy generated at the ℓ_c^{th} household, the stored energy and the energy consumption are given by G_{ℓ_c}, S_{ℓ_c} and D_{ℓ_c}, respectively. The storage capacity and the minimum stored energy are S_{max} and S_{min}, respectively. We assume that among the L_c households, L_e and L_d households have energy excess and energy deficit, respectively. The households with energy excess and energy deficit are denoted by ℓ_e and ℓ_d, respectively where $G_{\ell_e} > D_{\ell_e}$, $S_{\ell_e} = S_{max}$ and $G_{\ell_d} < D_{\ell_d}$, $S_{\ell_d} < S_{max}$.

The HEMS in each household computes the energy mismatch and forwards to the central EMS, if the mismatch is nonzero. The EMS then optimizes the energy trading operation by computing the optimum amount of energy to be sold/purchased. It also computes the prices for each seller to enable the household to recover a portion of the investment cost for solar panels and BESSs. We assume that the amount of energy sold by the ℓ_e^{th} seller from its excess renewable generation and the amount of energy purchased by the ℓ_d^{th} buyer to meet its load demand are denoted by x_{ℓ_e} and x_{ℓ_d}, respectively.

The energy discharged from the ℓ_e^{th} BESS is $\beta(S'_{\ell_e} - S_{\ell_e})$ and the amount of energy charged to the ℓ_d^{th} BESS is $\frac{S_{\ell_d}-S'_{\ell_d}}{\alpha}$, where S' and S denote the storage before and after charging/discharging, α and β are the charging and discharging efficiencies, respectively. The price at which ℓ_e^{th} household sells energy is p_{ℓ_e}. The capital investment cost for solar panel and BESS installation at the ℓ_e^{th} household is C_{ℓ_e}. The energy sell/purchase and pricing information are forwarded to the HEMSs and based on this, the households initiate energy trading operation.

The effectiveness of such energy trading operation often relies on the robustness and integrity of the information exchange between the HEMSs and the EMS. We assume that the smart grid communication for energy and pricing information exchange takes place through wireless communication technologies. Wireless technologies offer better flexibility and improved scalability, however, there are limitations in terms of security and privacy. The energy mismatch information can be easily eavesdropped by third parties and this information can be utilized to predict the decisions that will be made by the corresponding EMS.

To illustrate this, let us consider an example case. The EMS is receiving the energy mismatch information from 4 households. Households 1 and 2 have excess generation of 100 W and 300 W, respectively. On the other hand, households 3 and 4 have an energy deficit of 200 W and 500 W, respectively. With optimum energy trading, household 1 can sell 100 W to household 3 and household 2 can sell 300 W to household 4. And the remaining energy deficit at households 3 and 4 will be purchased from the utility grid. Now, in the presence of an attacker, if the false injection to households 1 (3) and 2 (4) is −100 W and −300 W, respectively, the sellers will not be able to sell in the residential microgrid and cannot receive more than the feed-in tariff. On the other hand, the buyers will have to purchase energy from the utility grid at a higher utility rate. Thus, there will be loss of profit/savings for the households.

In this paper, we consider that the attacker is the nearby EMS which has either excess generation or energy deficit in all the connected households at the same time. The combined generation and combined demand of all houses under the attacker EMS is G_a and D_a, respectively. The total amount of stored energy is S_a. When the attacker EMS has excess energy (i.e., $G_a > D_a$ and $S_a = L_a S_{max}$), it can sell this energy to the households in energy deficit under the cth EMS at a rate greater than the feed-in tariff, that it would receive otherwise. Similarly, when the attacker has energy deficit (i.e., $G_a < D_a$ or $S_a < L_a S_{max}$), it can purchase this energy from the households in energy excess under the cth EMS at a rate smaller than the utility rate and thus, get the benefit of cheaper energy. The amount of energy sold or purchased by the attacker EMS is denoted by $x_{a,e}$ and $x_{a,d}$, respectively. The system model under consideration is illustrated in Fig. 1.

The attacker EMS intends to design the attack signal in such a way that its benefits as a seller/buyer are maximized. The false values injected with the signal designated for the ℓ_e^{th} seller or ℓ_d^{th} buyer are denoted by δ_{a,ℓ_e} and δ_{a,ℓ_d}, respectively. These attack signals are optimized in such a manner that the amount of energy sold/purchased from the houses under the attacker EMS is maximized, while meeting the operational constraints.

3. Optimum attack signal generation

The attacker solves the optimization problem in (1) to obtain the false injection attack signals.

$$\min_{x_{\ell_e}, x_{\ell_d}, \delta_{a,\ell_e}, \delta_{a,\ell_d}} \sum_{\ell_e=1}^{L_e} \sum_{\ell_d=1}^{L_d} |(x_{\ell_e} \beta(S'_{\ell_e} - S_{\ell_e}) + \delta_{a,\ell_e}) - (x_{\ell_d} + \frac{S_{\ell_d} - S'_{\ell_d}}{\alpha} + \delta_{a,\ell_d})| \tag{1}$$

$$x_{\ell_e} \leq |G_{\ell_e} - D_{\ell_e}| \quad \forall \ell_e \in [1, L_e] \tag{2}$$

$$x_{\ell_d} \leq |D_{\ell_d} - G_{\ell_d}| \quad \forall \ell_d \in [1, L_d] \tag{3}$$

$$S_{min} \leq S_{\ell_e}, S_{\ell_d} \leq S_{max} \quad \forall \ell_e \in [1, L_e], \ell_d \in [1, L_d] \tag{4}$$

$$x_{\ell_e}, x_{\ell_d} \geq 0 \quad \forall \ell_e \in [1, L_e], \ell_d \in [1, L_d] \tag{5}$$

$$\delta_{a,\ell_e}, \delta_{a,\ell_d} \leq 0 \quad \forall \ell_e \in [1, L_e], \ell_d \in [1, L_d] \tag{6}$$

$$\delta_{a,\ell_e} \geq -\min((G_{\ell_e} - D_{\ell_e}), u_{\ell_e}|G_a - D_a|) \quad \forall \ell_e \in [1, L_e] \tag{7}$$

$$\delta_{a,\ell_d} \geq -\min((D_{\ell_d} - G_{\ell_d}), u_{\ell_d}|G_a - D_a|) \quad \forall \ell_d \in [1, L_d] \tag{8}$$

$$p_{\ell_e}(G_{\ell_e} - D_{\ell_e}) \geq m_{\ell_e} C_{\ell_e} \quad \forall \ell_e \in [1, L_e] \tag{9}$$

$$p_{\text{feed-in}} \leq p_{\ell_e} \leq p_{\text{util}} \quad \forall \ell_e \in [1, L_e], \tag{10}$$

Here, the objective function in (1) minimizes the mismatch between energy sell and purchase to obtain the supply/demand balance in the energy market. The constraints (2) and (3) limit the energy sell and purchase values within the energy excess and energy deficit values at the households. The constraint (4) limits the stored energy between the minimum storage level and the maximum storage capacity. The constraints (5) and (6) ensure that the legitimate energy sell/purchase values are non-negative and the injections from the attacker are non-positive (so that the energy sell/purchase in the legitimate EMS is minimized).

The constraint (7) ((8)) limits the false data injection values to the minimum between the energy excess (deficit) value at the households under the legitimate EMS and the portion of the net energy excess (deficit) at the households under the attacker EMS, that the attacker EMS is willing to provide (extract) to (from) the households under the legitimate EMS. Here $u_{\ell_e} = \frac{G_{\ell_e} - D_{\ell_e}}{\sum_{\ell_e=1}^{L_e}(G_{\ell_e} - D_{\ell_e})}$ and $u_{\ell_d} = \frac{G_{\ell_d} - D_{\ell_d}}{\sum_{\ell_d=1}^{L_d}(G_{\ell_d} - D_{\ell_d})}$ are chosen in such a way that the supply/demand balance at the attacker EMS can be achieved by selling/purchasing in proportion to the energy excess and deficit values at the households under the legitimate EMS.

The constraint (9) allows to set the pricing for the legitimate sellers in such a way that the profit earned from excess energy in the residential microgrid can recover $\frac{m}{100}$% of the investment cost at the sellers. The constraint (10) ensures that the legitimate sellers receive a rate more than the feed-in tariff $p_{\text{feed-in}}$ and less than the utility rate p_{util} to make local energy trading attractive to the prospective sellers/buyers.

4. Numerical results

We consider a residential microgrid with $L = 4$ households, equipped with 1 kW, 3 kW, 2 kW, and 1 kW solar panels, respectively. Households 2 and 3 are connected to 1 kW BESS, whereas, households 1 and 2 are not equipped with BESSs.[1] The attacker EMS is also connected with 4 households with similar sizes for solar panels and BESSs. The feed-in tariff and utility rate are considered to be 11 cents/kWh and 30 cents/kWh, respectively. The charging and discharging efficiencies are 0.7. The capital investment costs for the 4 households are \$1000, \$4000, \$3000, and \$1000, respectively.

Fig. 2 shows the energy mismatch for each of the households under the legitimate EMS at different hours of the day. The positive values indicate that the households have energy deficit and the negative values indicate energy excess. The time axis represents 12 : 00 AM to 11 : 00 PM (hours 1 to 24 in the figure). It can be noted that before 10 : 00 AM, all houses have energy deficit, whereas, from 10 : 00 AM to 7 : 00 PM, most houses have energy excess (due to excess renewable generation). Households 2 and 3 have significant energy mismatch during 12 : 00 AM to 1 : 00 AM and 10 : 00 PM to 11 : 00 PM, as they are charging up the BESSs during these off-peak hours and no renewable generation is available at this time.

Fig. 3 shows the benefits achieved by the different houses in terms of profits (earned by sellers) and in terms of savings (made by buyers) when no attacker is present. The figure only shows the profits/savings from 10 : 00 AM to 7 : 00 PM, as

[1] The renewable power generation profiles and the load demand profiles are collected from http://pv-map.apvi.org.au and https://data.gov.au/dataset/electricity-consumption-benchmarks/resource, respectively.

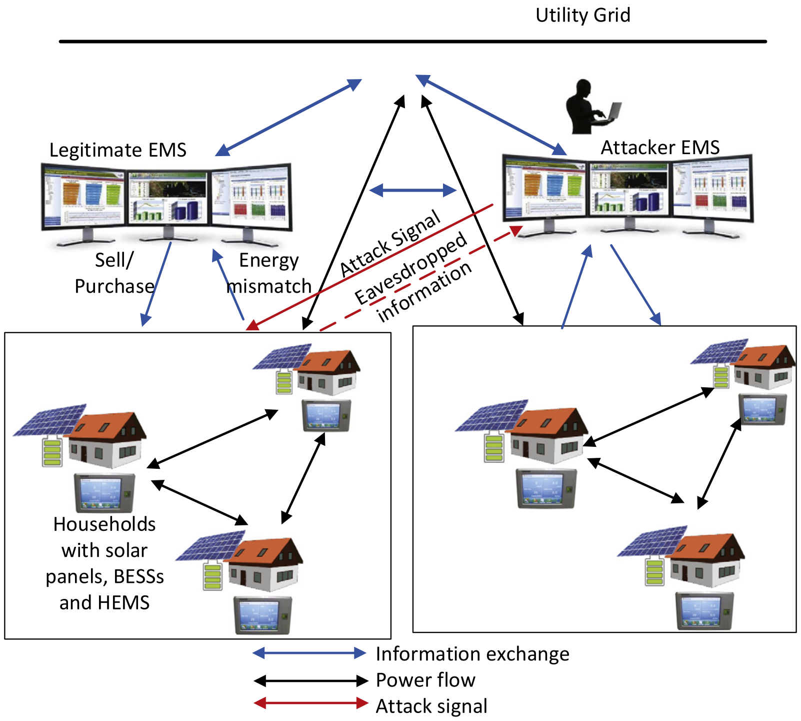

Fig. 1. System model for local energy trading in the presence of attacker, where the attacker overhears the energy consumption signals and injects false message, accordingly.

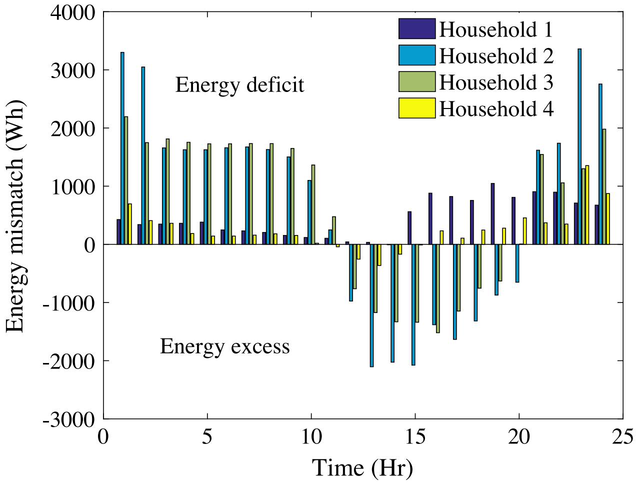

Fig. 2. Energy mismatch in the 4 households over the day.

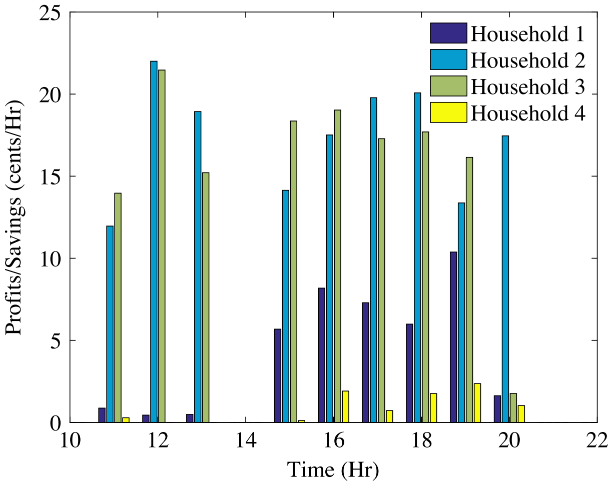

Fig. 3. Profits or savings at different households from local energy trading without attack.

the number of buyers and sellers are non-zero only during this time period. It can be seen that the households can obtain a profit/savings up to 10.38, 22, 21.5 and 2.5 cents in households 1, 2, 3 and 4 during certain hours. Households 2 and 3 have earned more benefits as they have battery storages, which they can utilize when more houses are in energy deficit. Household 4 earns small amount of profits/savings because it has small amount of mismatch compared to other houses.

Fig. 4 shows the profit/savings achieved by the houses in the presence of an attacker, as well as the profit/savings achieved by the attacker EMS. From this figure, we can see that the attacker EMS gains profits/savings from excess/deficit energy in the households under the legitimate EMS. The profits/savings at the attacker EMS can be as high as 24 cents at certain hours. The maximum loss of profits/savings at house 1, house 2, house 3 and house 4 are 94%, 86%, 93% and 86% at 4 : 00 PM, at 5 : 00 PM, at 5 : 00 PM and at 4 : 00 PM, respectively.

5. Conclusion

In this paper, we have investigated the impact of false data injections from the attacker EMS, when the attack signal is optimized to extract maximum possible benefits from legitimate participants, while maintaining supply–demand balance in the

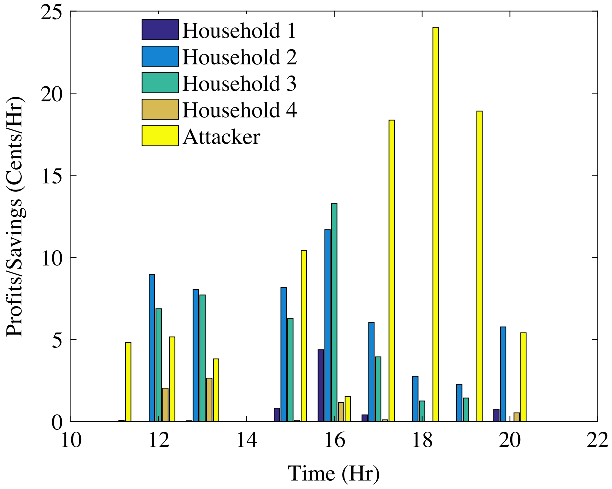

Fig. 4. Profits or savings at different households from local energy trading without attack.

local energy market. We have compared the earnings/savings from local energy trading at different houses with and without the presence of an attacker. The results show that local energy trading can result into significant benefits, especially for houses with BESSs. However, when the attacker EMS injects the optimized false signal, the profits/savings at the legitimate houses drop significantly, which illustrates the vulnerability of such systems to false data injections. Future works will focus on the inclusion of power network constraints, constraints from financial agreements in the local energy market, and the impact of communication impairments at the attacker and legitimate participants, as well as the mitigation technique for false injection attack.

Acknowledgment

This work is supported by Deakin University under the School of Engineering Small Research Grant.

Conflict of interest

The authors declare that there is no conflict of interest in this paper.

References

[1] P.G.D. Silva, D. Ili, S. Karnouskos, The impact of smart grid prosumer grouping on forecasting accuracy and its benefits for local electricity market trading, IEEE Trans. Smart Grid 5 (1) (2014) 402–410. http://dx.doi.org/10.1109/TSG.2013.2278868.

[2] R. Majumder, G. Bag, K.H. Kim, Power sharing and control in distributed generation with wireless sensor networks, IEEE Trans. Smart Grid 3 (2) (2012) 618–634.

[3] L. Maglaras, L. Shu, A. Maglaras, J. Jiang, H. Janicke, D. Katsaros, T.J. Cruz, Editorial: industrial internet of things (I2oT), Mob. Netw. Appl. 3 (2) (2017) 618–634.

[4] S.M. Amin, A.M. Giacomoni, Smart grid, safe grid, IEEE Power Energy Mag. 10 (1) (2012) 33–40.

[5] D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, M. Guizani, Secure service provision in smart grid communications, IEEE Commun. Mag. 50 (8) (2012) 53–61.

[6] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, Asurvey on privacy-preserving schemes for smart grid communications, 2016, https://arxiv.org/abs/1611.07722.

[7] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu, Securing smart grid: Cyber attacks, countermeasures, and challenges, IEEE Commun. Mag. 50 (8) (2012) 38–45.

[8] T. Cruz, L. Rosa, J. Proena, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, P. Simes, A cybersecurity detection framework for supervisory control and data acquisition systems, IEEE Trans. Ind. Inf. 12 (6) (2016).

[9] K. Stefanidis, A.G. Voyiatzis, An HMM-based anomaly detection approach for SCADA systems, in: S. Foresti, J. Lopez (Eds.), Information Security Theory and Practice: 10th IFIP WG 11.2 International Conference, WISTP 2016, Heraklion, Crete, Greece, September 26–27, 2016, Proceedings, Springer International Publishing, 2016, pp. 85–99.

[10] M.A. Mustafa, S. Cleemput, A. Abidin, A local electricity trading market: Security analysis, in: IEEE ISGT-Europe, 2016, pp. 1–6.

[11] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Trans. Ind. Inf. PP (99) (2017) 1–1.