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

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.

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).

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 non-zero. 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