

Investigating the Impact of Cyber-Attack on Load Profile of Home Energy Management System

Ugonna Anuebunwa, *Haile-Selassie Rajamani,
**Prashant Pillai and Oghenovo Okpako

Electrical Engineering and Computer Science, University of Bradford, UK. {U.R.Anuebunwa, and O.Okpako}
@bradford.ac.uk) .

*Faculty of Engineering & Information Science, University of Wollongong, Dubai, UAE
HaileRajamani@uowdubai.ac.ae

**Faculty of Technology, Design and Engineering, Oxford Brookes University, UK
ppillai@brookes.ac.uk

Abstract. Load profile for a household is key to understanding and applying automated load scheduling executed by the Home Energy Management Systems (HEMS). The provision of securing this basic domestic information as well as preventing intruders from being able to accessing and modifying them should be a matter of high priority. Any malicious attack on this data will have serious impact on the performance of the load scheduling algorithms. This paper is an investigation of how the scheduled load profile of a household can be deformed due to false data injection on the original load profile as a result of cyber-attack on the HEMS. Various incremental false data levels are introduced during an optimization process and the corresponding effect on the overall scheduled load profile is evaluated to understand the actual impact of the cyber-attack. Results show that as noise attack level increases, the optimized load profile shrinks and approaches a straight line which is equivalent to the average value of the original load profile. The implication of having such a load profile as a schedule is the obvious excessive disruption of a household's energy use which results to having appliances switched ON or OFF at highly undesired times of the day thereby exacerbating user inconvenience.

Keywords: Cybersecurity, *Demand Response*, Dynamic Pricing Home Automation and Internet of Things.

1 Introduction

On 23rd December 2015, the Ukrainian regional electricity distribution company was subject to a critical cyber-attack. On this occasion, seven 110kV and twenty three 35 kV substations were disconnected for three hours from the Ukrainian grid network resulting in a huge economic and societal impact. This attack was attributed to foreign government-sponsored cyber-criminals, who remotely controlled the SCADA distribution management system and caused a blackout for approximately 225,000 customers [1]. A similar incident is the case of cyber-attack in October 2016 when a Distributed Denial of Service (DDoS) attack knocks heating system offline in at least two housing blocks in the city of Lappeenranta, leaving their residents in subzero weather conditions. In an attempt to fight back the attack which was only short-lived, the automated systems rebooted which unfortunately got stuck in an endless loop that kept restarting and shutting down. This scenario lasted for over a week but returned to normal service by 3rd November afternoon [2]. As much as researchers and scientists are working hard every day to improve living standards as well as efficiency of system designs, criminals are also attempting and finding ways to interfering with these systems thereby sabotaging, thwarting and frustrating their operations. While cyber-attacks are a persistent threat to internet users, they are also becoming a cause for concern in other areas like power grids, healthcare networks, transportation, that are more and more using ICT technologies. The aim of this paper is to investigate the impact of a cyber-attack on Home Energy Management Systems (HEMS) and then propose means of mitigating the disruptions occasioned by these attacks, which is capable of distorting and impacting on the efficiency of the normal operations of a domestic load scheduler. This investigation is carried out by introducing noise signals on the load profile data and then observing the effect on the optimized load profile. A comparison of the outcome with the expected load profile when there is no attack is also made and appropriate deductions carried out.

The energy load profile represents the electrical load consumption of residential, commercial or industrial consumers over a period of time. The energy usage will vary over different days (weekend and weekdays) and also over different seasons (winter and summer). Such load profiles can be used to determine energy allocation and planning benefits depending on how much power is available for distribution as well as where the priority lies during peak and off-peak periods. A forecasted load profile is usually obtained from historical load profile data and it is very useful for planning the schedule for the next day. Using these load profiles, HEMS run load scheduling algorithms to propose a scheduled load usage for consumers for improved grid balancing and

reduction of consumer's energy costs. This means that load profiles are invaluable and any successful attack on it can disrupt power supply and network by producing inaccurate forecasted load profiles as well as invalidating the outcome of the proposed load allocation and efficient energy planning schedule. In this paper the forecasted load profile used is hourly-based over a 24-hour period and it is computed using moving average forecasting methods. The optimized load profile is obtained using Genetic Algorithm (GA) optimization with input variables such as pricing and occupancy data in order to determine the optimized output whose data is influenced by the amount of noise present at the forecasted load profile.

In any smart home, the attack vector to a load profile data stored in the HEMS is via the communication network that connects the HEMS to the internet as well as through smart appliances and any wireless device which connects the load to the HEMS. This connection is to enable the HEMS obtain pricing data online as they are published by the energy providers, or to communicate with the load. Unfortunately, this exposes the communication link to become a target for an attack of which cyber-criminals could break into. This is where appropriate security design should be enforced because as much as the load profile data is vulnerable; virtually any data on the HEMS can be attacked. However, this paper will limit the investigation on attack on load profile, while attack on other aspects is considered out of scope. Furthermore, it is assumed that the prices are known a day before but they could be more real time with forecasting being carried out to predict the price for the next 24 hours.

2 Related Work

Protection of vulnerable load and other related components of the smart grid from cyber-attack keeps attracting interests from researchers around the globe due to the numerous challenges facing the internet world. The authors in [3], [4] discussed the importance of detecting cyber-attacks in energy consumption data of power systems as provided by smart meters, and suggested schemes for adequate protection. Such attacks on dynamic loads known as: dynamic load altering attacks (D-LAA), was considered because, the possibility to control loads dynamically implies also the possibility to attack loads dynamically [4]. This is in contrast to Static load altering attacks (S-LAA) which is more common and is based on changing the volume of certain vulnerable loads, usually in an abrupt fashion. The paper suggested the detection D-LAAs is possible by applying frequency domain analysis of the load profile using Fast Fourier Transform (FFT) of the original load profiles via spectral analysis [5]. Another detection technique includes Real-time detection in frequency domain using Windowed-FFT (W-FFT), and detection based on both load and frequency signals [6]. The paper suggested optimization problem formulation, solution method and protection system design under uncertainty as approaches towards applying adequate protection schemes to hinder successful attacks on the load data.

As much as these authors have identified means to detecting these attacks on various types of loads which includes FFT analysis, they did not investigate or analyze the impact of such attacks on the load profile. It is acknowledged that it is important to identify that there has been an attack, but the other important issue is to understand what impact such an attack is capable of causing on the infrastructure under protection, before applying any sort of solution. This scenario can be referred to the attack in Finland as mentioned in [1] because a DDoS attack which was only short-lived was identified. But this may not be as bad as requiring a system restart because, restarting the system was what actually kept it in a perpetual reboot mode thereby making it impossible for the heating supply to continue. Therefore this paper is centered in understanding the impact of such attacks first, so that appropriate steps can be taken in attempting to solve the problem which may offer other ways to solving the problem depending on the identified impact on the system.

3 Proposed Approach

For an effective demand response (DR) system, HEMS will maintain a record of historical load profiles and will generate up-to-date forecasted load profile for daily use during optimization, using any modern forecasting techniques available. In this work, moving average forecasting technique is applied because it is easier to implement and most especially because this paper is not about implementing the bests of sophisticated load forecasting techniques. Furthermore, the attacker is assumed to have access to this data by injecting false data onto the forecasted load profile. This data is therefore simulated and the impacts analyzed. Using the load scheduling technique as proposed in [11] [12] to define the objective function, the following equation is obtained:

$$F_{j,i} = w_a * \sum A_{j,i} - w_b * \sum B_{j,i} + w_c * \sum C_{j,i} - w_d * \sum D_{j,i} . \quad (1)$$

where:

A (Change on occupants) = Change in Energy ($\Delta\mathcal{E}$) * Occupancy

As $\Delta\mathcal{E} = e - x$

B (Cost) = Optimized Load (x) * Dynamic Pricing (α)

C (Discomfort) = $\Delta\mathcal{E}$ / Standard deviation of Load Profiles (σ)

D (Optimization Factor) = Optimized Load (x) / Forecast Load (e)

e = Forecasted load profile.

i = Iteration number

j = hourly time interval in a day.

w = Weighting factor

x = randomly generated load profile for optimization.

The objective function as given by Eqn.1 is optimized using GA to find the best solution (load Profile) that satisfies the conditions as defined by the input variables. By attacking the load it is expected that a direct impact will be primarily felt on input variables A, C and D because they are the variables that have load data as a component. By modifying the affected input variable as they relate to the attack on the load, we can therefore be able to observe the impact on the forecasted scheduled load profile as the optimization process is run in order to meet the already defined objective function.

1.1 Defining Optimization Constraints

The proposed constraints for the objective function as given in Eqn.1 are defined as: energy limitation constraint and energy conservation constraint. Eqn.2 is an energy limitation equation whereby both the maximum and minimum energy level of every randomly-generated load profile sample remains within the limit of the forecasted load profile.

$$e_{min} \leq x \leq e_{max} . \quad (2)$$

On the other hand, Eqn.3 is an energy conservation equation whereby the total energy of each randomly-generated load profiles samples is equal to the total energy consumed in any given day. This samples are taken hourly over a 24-hr period in a day.

$$\sum_{j=1}^{24} x_j = \sum_{j=1}^{24} e_j . \quad (3)$$

The results from this analysis will be compared with the normal scheduling operations which is used as the control model to show an attack-free optimization with secured data, in order to ascertain the impact of the on the household as well as the grid.

1.2 False Data Injection Attack on Load Profile

The model of cyber-attack on Load Profile as presented on this paper, is defined as an injection of false data on the original load profile data with the aim to cause the generation of random and unpredictable results thereby presenting a scheduled load which is not a true reflection of the consumer's choice as well as the market events. Let us consider an attack scenario whereby the forecasted load profile e , is injected with some discrete randomly generated noise η to create some form of distortion thereby creating a new forecast load profile as shown in Fig.1. The new load profile R over a 24 hour interval is given as:

$$q_j = e_j + \eta_j . \quad (6)$$



Fig. 1: Noise Injection Attack on Forecast Load Profile

The false data signal could also be a sinusoidal wave form, or/and can also be out of phase with the original signal. The impact on load profile with a variation of false data levels is evaluated in this paper. Any amount of false data injection is possible although in this paper, it is assumed that the maximum noise that can be introduced

is up to 100% of the mean load profile value. Therefore by definition, R_j is bound by a maximum allowable proportion of the forecast load profile and for only positive load profile values. This is given as:

$$\alpha_{\min} \leq q_j \leq 2\alpha_{\max} \quad (7)$$

The load profile data was obtained from [13] and 10 iterations of increasing noise level manner from zero up till 100% of the mean load value was introduced. In order to derive the corresponding objective function, the new load profile q_j as it affects A, C and D is substituted in Eqn. 1.

Therefore;

$$F_{j,i} = w_a * \sum A_{new\ j,i} - w_b * \sum B_{j,i} + w_c * \sum C_{new\ j,i} - w_d * \sum D_{new\ j,i} \quad (8)$$

Where:

$$A_{new} = (q_j - x) * \text{Occupancy} \quad (9)$$

$$C_{new} = (q_j - x) / \sigma \quad (10)$$

$$D_{new} = x / q_j \quad (11)$$

4 Simulation and Results

Three input data which are as controlling variables are used in the optimization process and they include: the Price Profile, Occupancy and Standard Deviation of Load Profile as shown in Fig. 2. The controlled variable is given as the Original Load Profile which is attacked with false data injection, while the output is the Optimized Load Profile. The Load Profile and Price data were obtained from [13] and [14] respectively.

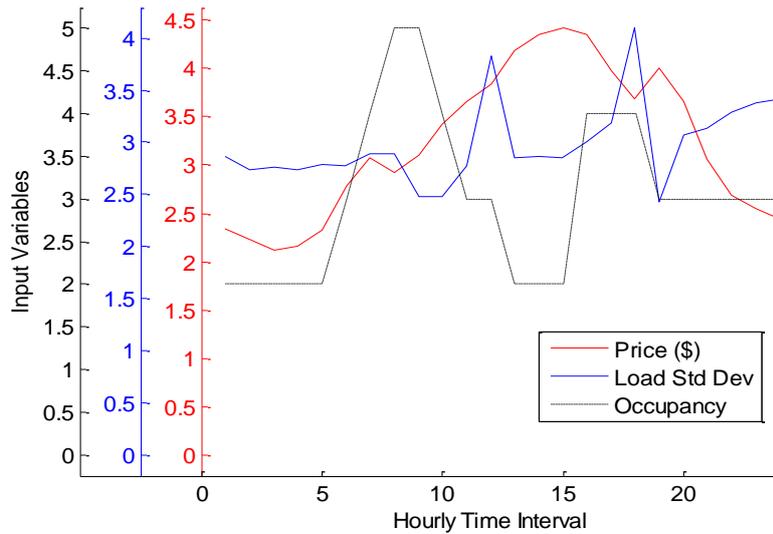


Fig. 2: Principal Input Variables for Load Scheduling

Fig. 3 to 7 shows the Original Load Profile data and various optimized Load Profile generated using Eqn. 8 as the objective function. The Original Load Profile is used as the main Load data which is subject to attack and the optimization result produced the Optimized Load Profile (With Attack) as shown in Fig. 3. The Optimized Load profile (W/out Attack) was generated using the same Original Load profile but with no false data injection. It therefore indicates the response assuming there was no attack and hence, acts as the baseline result. The Forecast Optimized Load profile is generated from Forecast Load Profile (which acts as the back-up) and is obtained from historical data of the previous 4 days of the same day of the week, as recorded within the HEMS. In this illustration, the retailer supplies the required original Load profile data, while the back-up Load Profile data was generated locally, although these positions can be interchanged as desired.

Four scenarios are shown whereby in the first one, there is no attack involved. Here, the Optimized Load Profile is exactly same for both with attack and without attack. The forecast Optimized Load Profile deviates only a bit from the two already mentioned. The second scenario as shown in Fig. 4 shows a false data injection of 20%. Here, the Optimized Load Profile (with Attack) begins to pull away from the Optimized Load Profile (without Attack) and this continues consistently at 50% as shown in Fig. 5. At 80% of false data injection as

shown in Fig. 5, it can be observed that the Optimized Load Profile (with Attack), is nearly flattened out except for the spike at 6:00 hours. This is a very key result as it clearly shows the effect of introducing false random data to the Original Load Profile, while the Forecast Optimized Load Profile shows that it is a reasonably good back-up to rely upon incase the HEMS detects irregular random or unexpected data within Load profile data. It is also appropriate to mention that the Optimized Load profile (without Attack) which is the baseline result remained the same with minimum and maximum values of about 2.5 kWh and 5.5 kWh respectively.

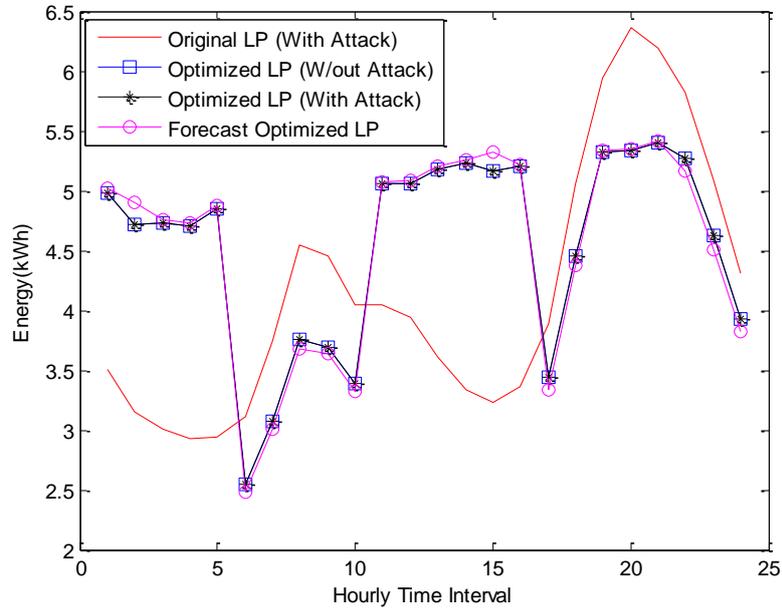


Fig. 3: Load Schedule with 0 % noise content

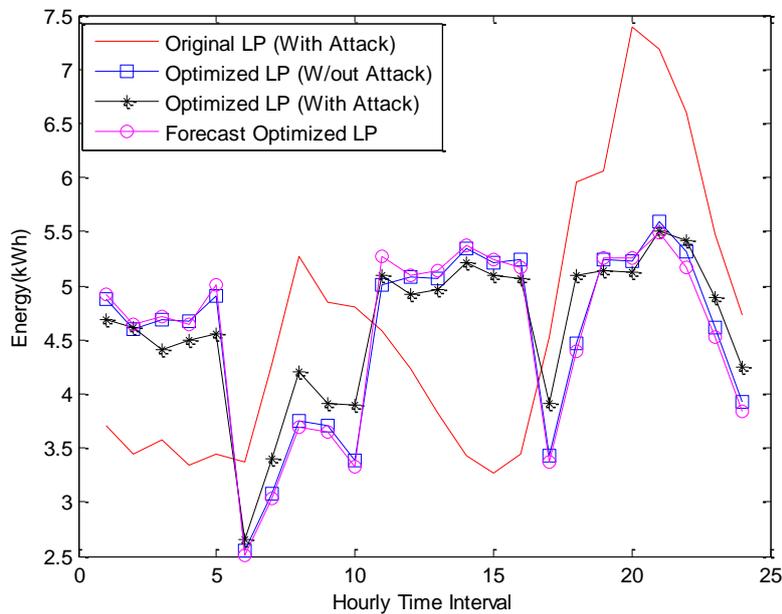


Fig. 4: Load Schedule with 20 % noise content

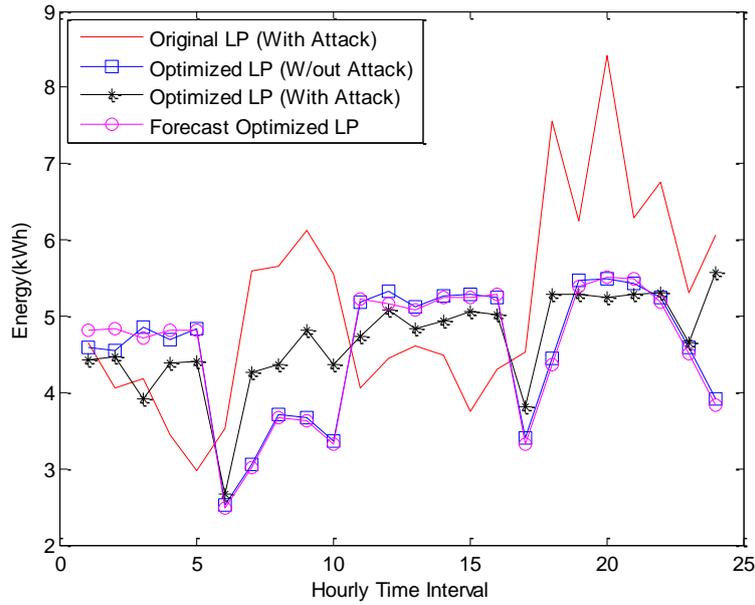


Fig. 5: Load Schedule with 50 % noise content

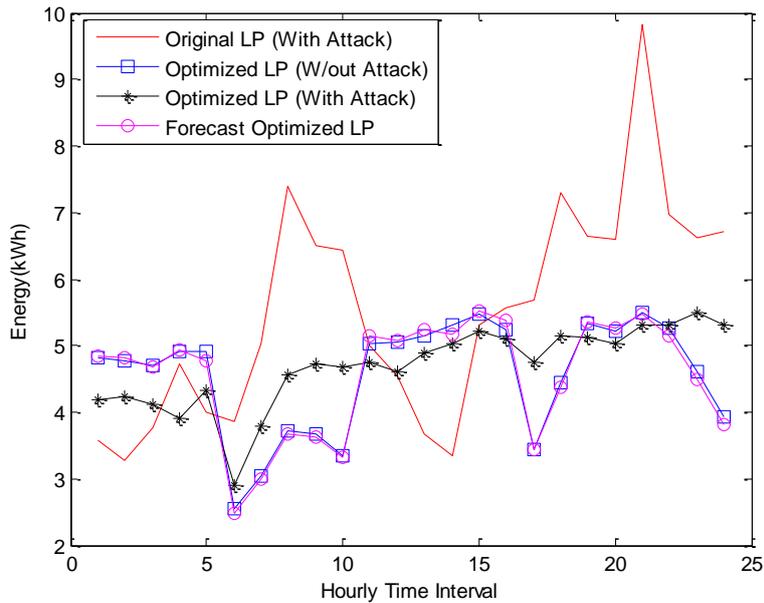


Fig. 6: Load Schedule with 80 % noise content

Two key observations are derivable from these results and they include:

- It is observable that as noise levels increases, the optimized load profile shrinks towards a straight line which represents the average value of the original load profile. This is an interesting result because we could see the effect of noise in diminishing the efficiency of the load scheduling process.
- The implications as deducible from the graphs is that such shrinking is capable of effecting significant load shifting whereby several loads could be turned ON when they are expected to be OFF and vice versa.

Therefore, this can be a worrisome scenario for consumers who participate in demand response programs and may not realize that their load profile has come under attack. They may conclude that participating in DR programs is highly discomfoting or that perhaps, their HEMS system is dysfunctional.

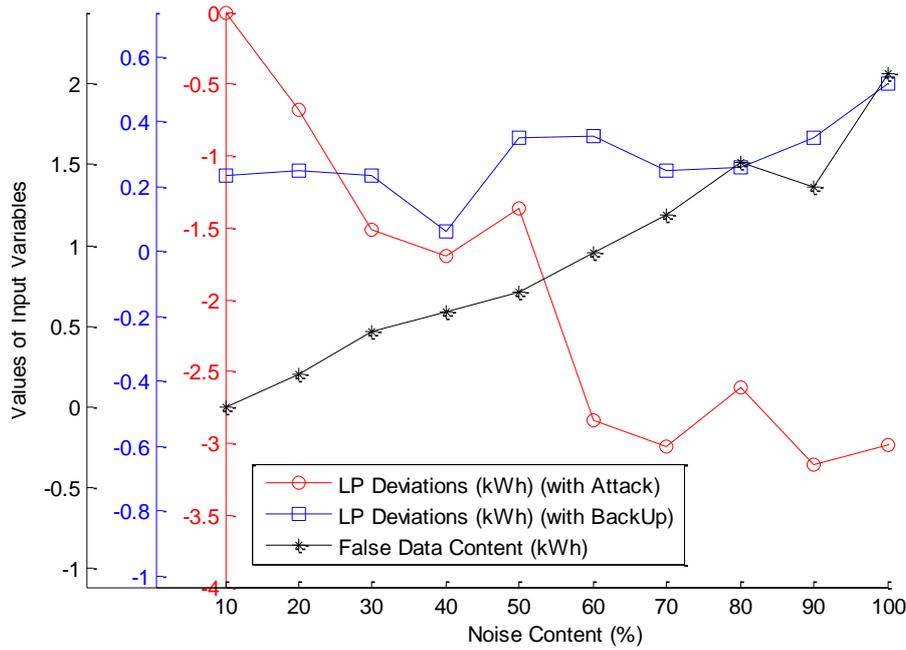


Fig. 7: Convergence of Price and Load profile Deviations as False Data Injection Increases

Fig. 7 shows the sum of deviations of Optimized Load Profile (with Attack) from the base Load Profile, which is the Optimized Load Profile (without Attack). It also shows the sum of deviations of the Forecast (Back-up) Load Profile from base Load Profile for a day, as false data content increases. It can be seen that the sum of deviations of the Back-up Load profile is fairly stable but, the Optimized Load Profile (with Attack) continues to increase significantly. This shows the impact of such an attack on Load scheduling mechanism as well as a means of mitigating such an attack, by the provision of an effective back-up system.

5 Discussion

The key to an efficient and active DR participation is on provision of a secured network with the correct and up-to-date levels of authentication and malware security applied, in order to prevent intrusion. In a case where an attack on the load profile is successfully achieved, the response by any installed security mechanisms becomes critical. It can be observed that there is no disruption of the optimization process due to the attack which means that neither the HEMS nor the users will be able to detect any anomalies by themselves since there will always be optimized load as results. It is therefore obligatory for the designers of load optimization algorithms to include means of flagging any unexpected results and as well, include means of deriving instant solutions.

The metering system could be a reliable source to detecting anomalies within the HEMS which is in view of the availability of the historical load consumption stored in the HEMS. So if an unexpected scheduling pattern which has no resemblance and differs remarkably with the historical load profile is generated, the system could call for a reassessment and vetting of all the input data. For instance in this case as presented in this paper, having an untrusted result could require the HEMS to use the last accurate load data and apply it with the current price and occupancy data, assuming they too are not affected by the attack.

Furthermore, since the attack produced results which lead to reduction in customer satisfaction, any affected consumers will most likely be discouraged to continue with their engagements and may withdraw from active participation in demand response programs. This will therefore defeat the aim for its design but with improved security, a long term benefit and advancement of the grid can be assured.

6 Conclusion

Cyber-attacks on HEMs are a real possibility and care should be taken towards ensuring the protection of the infrastructure that constitutes the network. In this paper, there has been a presentation and simulation of a cyber-attack on the HEMS which was modelled as false data injection onto the load profile data. Results obtained showed that such an attack diminishes the optimization mechanism as well as the system performance by

forcing the load profile to flatten out. Having such a flattened load demand throughout the day may seem to be the most optimal energy supply for a community from the grid perspective in terms of ensuring a supply of constant energy capabilities thereby eliminating peak load demand. But in practice, a flattened load profile is neither realistic nor comfortable for the users.

Finally, using previously known accurate data can help minimize the impact of such attacks. This means that the HEMS should keep a record of recent data and as well, perform some forecasting mechanisms on all data available. Nevertheless, preventing unauthorized access remains the best possible solution. Access authentication is naturally a key part for any proposed solution as it is important to ensure consumer confidence otherwise the dream of having a robust smart home which consumers will appreciate, will become unachievable.

References

1. R. M. Lee, M. J. Assante and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid. E-ISAC, 2016. Online. Assessed 31st December 2016.
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
2. M. Kumar. DDoS Attack Takes Down Central Heating System Amidst Winter In Finland [Online]. Available: <http://thehackernews.com/2016/11/heating-system-hacked.html> [Accessed: 21st June 2017].
3. S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Detecting Dynamic Load Altering Attacks: A data-driven time-frequency analysis."
4. S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Designs," Submitted to IEEE Trans. on Smart Grid.
5. P. Duhamel and M. Vetterli, "Fast Fourier Transforms: a tutorial review and a state of the art," Signal processing, vol. 19, pp. 259–299, 1990.
6. F. Zhang, Z. Geng, and W. Yuan, "The algorithm of interpolating windowed FFT for harmonic analysis of electric power system," IEEE Trans. on Power Delivery, vol. 16, no. 2, pp. 160–164, Apr. 2001.
11. U. Anuebunwa, H. S. Rajamani, P. Pillai and O. Okpako, Novel genetic algorithm for scheduling of appliances. in Proc. of the 2016 IEEE PES Power Africa Conference, Livingstone - Zambia, pp. 57-61.
12. U. Anuebunwa, HS Rajamani, P Pillai and O. Okpako, "Investigating the Impact of Discomfort in Load Scheduling Using Genetic Algorithm", IEEE International Conference on Power Systems Technology (IEEE POWERCON2016), Australia, 2016.
13. U.S Department of Energy, "Commercial and residential hourly load profiles for all TMY3 Locations in the United States," 2nd July 2013 ed.: OpenEI, 2013.
14. A. Illinois, "Day Ahead Pricing used for billing RTP and HSS service," 1st May 2015 Ed: Ameren, 2015.