Investigating the Impacts of Cyber-Attacks on Pricing Data of Home Energy Management Systems in Demand Response Programs

Ugonna R. Anuebunwa
School of Electrical Engineering & Computer Science
University of Bradford
Bradford, UK
u.r.anuebunwa@bradford.ac.uk

Haile-Selassie Rajamani
Faculty of Engineering &Information Science,
University of Wollongong,
Dubai, UAE
HaileRajamani@uowdubai.ac.ae

Raed Abd-Alhameed
School of Electrical Engineering & Computer Science
University of Bradford
Bradford, UK
R.A.A.Abd@bradford.ac.uk

Prashant Pillai
School of Mathematics and Computer science Faculty of Science and Engineering,
University of Wolverhampton,
Wolverhampton, UK
ppillai@wlv.ac.uk.

Abstract— Provision of security involves protecting lives and properties, and properties in this context include data and services. This paper investigates the impact of cyber-attacks on load scheduling applications by simulating various possible modes for these attacks while observing possible effects on the users. The attack modes used are in the form of denial of service (DoS) and phishing attacks whereby the attacker is able to interfere with data intake to the Home Energy Management Systems (HEMS) or a modification of critical data to the HEMS. The dynamic pricing information and load profile data is the target here although other types of data utilized by the central controller for load scheduling purposes can also be targeted. The test-bed uses load scheduling applications based on genetic algorithm optimization. Results show the impact on optimized load profiles and how they can discourage active demand response participation if such attacks are not properly managed.

***Index Terms*-- Cybersecurity, *Demand Response*, Dynamic Pricing, *H*ome Automation and Optimization**

I. INTRODUCTION

Cyber-attack is a familiar experience to internet users since the commercialization of internet services and operations. As in the real world, similar criminal activities are carried out by people who have capitalized on the vulnerability of data transferred over the internet for their own selfish needs. The realization that information transferred via the internet can be hacked, harvested and compromised, has offered intruders alternative ways to invading peoples' privacy without having to physically step into their premises. As a result, evolution of traditional power grid network system to a smart grid network which primarily utilizes communication and data transfer infrastructure, requires adequate security in order to deter intruders from disrupting the network.

The focus of this paper is on consumer side of the smart grid within a liberalized energy market, in particular on the emerging Home Energy Management Systems (HEMS) that may be linked to other external entities such as Virtual Power Plants, Distribution Network Operators (DNOs) and micro-grid operators in order to provide for load balancing services, renewable energy integration and ultimately financial benefit to the consumer. Although a survey by promotional marketing firm Parago, suggests that only about 14% of consumers in the US currently participate in demand response programs, security of the HEMS still remains important [1]. Several factors can encourage cyber-criminals to consider hacking into people's privacy but the commonest reasons seem to be just for fun, intending to prove a point that they can hack a new system or simply because they just want to bring down an organized system [2]. Sometimes information harvested from unsuspecting victims are sold to a third party for some monetary value, and this is one of the occasions whereby cyber-criminals trade directly the personal details of online users in the so called "dark web" [3]. This therefore leaves the energy grid itself as a matter of national security if it becomes subject to attack.

The aim of the work is to demonstrate the possible impacts on the performance of a load scheduler which came under specific and successful cyber-attack on the HEMS. As a result, appropriate proactive defense mechanism can be provided which is capable of preventing the effectiveness of any such attack. Although authentication, firewalls, antivirus and other conventional protective mechanisms are absolutely necessary, it is also important to incorporate other protective mechanisms which act as the last line of defense in securing the HEMS. This is incorporated in the algorithm that runs the program such that required actions can be taken.

II. RELATED WORK

On December 23 2015, there was a recorded incidence of cyber-attack on the Ukrainian reginal electricity distribution company whereby seven 110kV and twenty three 35 kV substations were disconnected for three hours [4]. This attack was attributed to foreign government-sponsored cyber-criminals who remotely controlled the SCADA and caused blackout on approximately 225,000 customers. This shows an example of the numerous threats which cyber criminals oftentimes, pose to the smart grid network and the disturbing disadvantages of being all connected via the internet. In trying to understand how to identify cyber-attack patterns and

preventing their occurrence, several authors have contributed through several experiments to this effect.

Authors in [5] investigated the attack vectors on smart HEMS analyzed on a digitalSTORM installation using solution-based analysis. This was done by identifying and ranking possible attack vectors or entry points into a smart home systems with suggested ways of thwarting such attacks. Those entry points included: the server, communication bus, smart control device (e.g. smartphone or control station) and remote third party services which provides monitoring and control services. A malicious app was surreptitiously installed on the home owner's android smart-phone and was used as entry vector which can turn appliances ON or OFF. Results shows various vulnerabilities via the attack entry points on the HEMS while suggesting authentication from authorized users as a reliable means of preventing such attacks.

Authors in [6] improved mesh network security used within various smart grid domains against cyber-attack by introducing a dynamically updating key distribution strategy on network protocols. The proposed method was mainly designed against DoS attack by utilizing a 4-way Merkle-tree based handshaking scheme. The reliability of the model was verified using Proverif and they were able to demonstrate the effectiveness of key refreshment strategy in thwarting DoS attack on the smart grid network.

Authors in [7] [8] proposed means of detecting cyber-attacks in HEMS by alterations on the load profiles. Two models of attacks were considered which includes: Dynamic Load Altering Attacks (D-LAA) and Static Load Altering Attacks (S-LAA). D-LAA was considered because the possibility to control loads dynamically implies also, the possibility to attack loads dynamically. S-LAA is more common and is based on changing the volume of certain vulnerable loads, usually in an abrupt fashion. The paper suggested possible D-LAAs detection by applying frequency domain analysis of the load profile using Fast Fourier Transform (FFT) of the original load profiles [9] via spectral analysis. Another technique includes Real-time detection in frequency domain using Windowed-FFT (W-FFT), and detection based on both load and frequency signals [10].

Several other forms of cyber-attack are possible and may include communication system failure which could originate from the utility or from the localized HEMS [11]. The next section is a description of the method applied in analyzing possible attacks within the HEMS and suggested ways of preventing possible impacts on the load profile generated.

III. PROPOSED METHOD

The impact of security breaches on homes that engage actively in demand response programs can be investigated by modeling possible attack scenarios which may affect the home network in order to analyze possible impacts due to these attacks. Unsecured or poorly secured communication links within the household are usually the target and the focus here is on communication links that send pricing information from the retailer to the HEMS. Each model of the various possible cyber-attacks is simulated in order to investigate the impact on the localized scheduler. Pricing is an important variable but also vulnerable due to energy cost savings capabilities thereby making them an attacker's target [12]

In this analysis, a household whose occupants are active demand response (DR) participants are presumed to receive a forecast load schedule of which they are prepared to abide with. Thereafter, an attack on the pricing data was encountered which affected the components of the objective function that has price information as a variable. The objective function is given as the following equation:

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

Where:

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

Here, A represents the effect of absolute change in energy use on all occupants. However when nobody is in house, the change has no effect. This is why $\Delta\mathcal{E}$ is multiplied by the occupancy to give A, which offers a better measure than $\Delta\mathcal{E}$. A low impact of such change is favorable to the consumer.

B represents change that effects energy cost reduction. Cost is a major incentive to the adoption of demand response programs, hence its inclusion on the fitness function equation.

C represents the discomfort experienced due to scheduling which is expected to be minimized in order to reduce drastic reassignments of loads from the original forecasted load profile to other times for the new day.

D represents optimization factor which attempts to scale the optimized load to the magnitude of the forecast load profile at every iteration during optimization. A high effect of this application is considered favorable to the consumer.

Various scenarios are therefore simulated in the next section by nullifying or modifying the affected variable with respect to the attack. Hence, impact of the respective cyber-attack on the forecast scheduled load profile is observed.

A. Genetic Algorithm-Based Model

Genetic Algorithm (GA) is the optimization tool used mainly due to the ease in appending variables to the fitness function in order to accommodate any desired objective. Due to the dissimilarities of the variables in Eqn.1, each variable is converted to the per unit scale in order to allow additions of the variables while the weightings places more emphasis on any variable considered more important that the other. Eqn.2

and Eqn.3 shows the constraints applied whereby Eqn.2 is an energy limitation equation, and 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.

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

Eqn. 1 is a minimization of the fitness function. This means that the variables with positive signs are minimized while those with negative signs are maximized.

B. Cyber-Attack Models and Impact on HEMS

I. Denial of Service Attack

A typical DoS attack can be initiated when an attacker deliberately generates multiple requests from his device to a target via a single protocol, thereby causing an impediment on data traffic and preventing the target from accessing their data online. Alternatively, the attacker can generate multiple requests through some master to slave computers while pretending to be the victim computer. The slave computers not recognizing the source of the request command presumes that all requests came from the victim computer and in an attempt to respond to those requests, they end up causing an unprecedented traffic and delays on the victim computer. Such requests are usually massive for the server to withstand and this type of attack is known as Distributed DoS (DDoS).

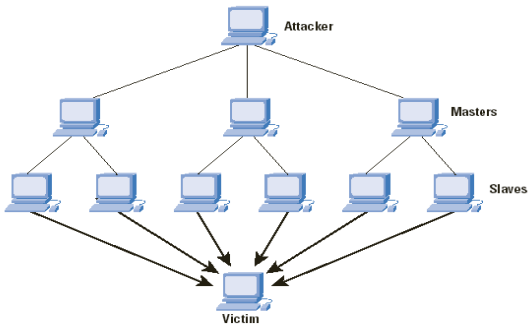

Fig. 2: Distributed Denial of Service Attack on a Victim [13]

Any such attack on the pricing information as shown in Fig. 2 is capable of preventing the load scheduling algorithm from accessing the pricing data required for load scheduling. The consequence of this attack is the non-availability of the pricing function to the fitness function of Eqn. 1. Mathematically, given the cost B, as a variable of the fitness function F, total Energy Cost per day is given as:

$$B_{Total} = w_b * \alpha * \sum x_{j,i} \quad (4)$$

For a DoS attack, Price = nil (data is delayed or unavailable)

Then from Eqn. 4,

Total Energy Cost per day = $w_b * 0 * \sum x_{j,i}$

Therefore for a DoS attack, Eqn. 1 becomes:

$$F_{j,i} = w_a * \sum A_{j,i} + 0 + w_c * \sum C_{j,i} - w_d * \sum D_{j,i} \quad (5)$$

II. Constant- Pricing Attack

Reducing a dynamic pricing regime to a fixed pricing signal can be a consequence of an unsecured network hijacked by a cyber-attacker. In order to model this attack;
Let Constant Price factor = ΄Y,
Then from Eqn. 4, total Energy Cost per day = $w_b * ΄Y * \sum x_{j,i}$

Therefore for a fixed pricing attack, Eqn. 1 becomes:

$$F_{j,i} = w_a * \sum A_{j,i} + w_b * ΄Y * \sum x_{j,i} + w_c * \sum C_{j,i} - w_d * \sum D_{j,i} \quad (6)$$

III. False Data Injection Attack

A cyber-attack on the dynamic pricing information can occur in form of false data injected on the actual pricing signal. The aim of this sort of attack can be to cause the generation of random and unpredictable results thereby presenting a scheduled load which is not a true reflection of the market events. The result is important because this type of attack can be difficult to detect since different types of results can be generated each time the algorithm is run.

Fig. 3: False data Injection Attack on Actual Price Signal

Let us consider an attack scenario whereby the actual dynamic price signal α is injected with some discrete randomly generated false data η to create distortion thereby creating a new price profile R as represented in Fig. 3. The new price profile R over a 24 hour interval is as given in Eqn.7.

$$R_j = \sum_{j=1}^{24} \alpha_j + \eta_j \quad (7)$$

A variation of false data levels introduced is evaluated and a maximum false data level of up to 20% of the peak dynamic price value is assumed. Therefore R_j is bound by a maximum allowable proportion of the actual pricing signal for only positive pricing values. This is as given in Eqn.8.

$$\alpha_{min} \leq R_j \leq 1.2\alpha_{max} \quad (8)$$

The actual day-ahead pricing data was obtained from [14] and 20 iterations of increasing false data level was incremented in a step-wise manner from 0 up till 20% of the maximum price value. In order to model this attack, Let Noisy Price = R_j .

Then from Eqn. 4, total Energy Cost per day = $w_b * R_j * \sum x_{j,i}$
Therefore for a fixed pricing attack, Eqn. 1 becomes:

$$F_{j,i} = w_a * \sum A_{j,i} + w_b * R_j * \sum x_{j,i} + w_c * \sum C_{j,i} - w_d * \sum D_{j,i} \quad (9)$$

IV. SIMULATION AND RESULTS

In order to perform load scheduling, the controlled variable is given as the Forecast Load Profile obtained from [15] while the three principal input data used as controlling variables include: Price Profile, Standard Deviation of Load Profile and Occupancy.

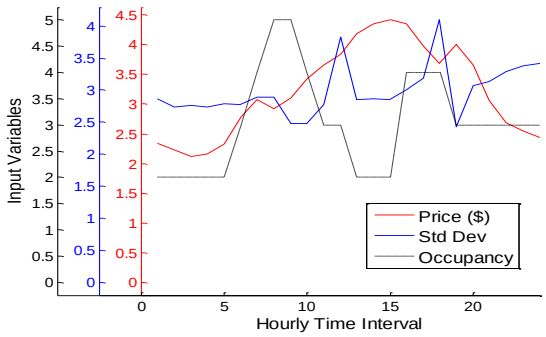

Fig. 5: Principal Input Variables for Load Scheduling

The output is the Optimized Load Profile generated due to the effect of the controlling variables shown in Fig. 5. The results of the three attack scenarios are presented as well as means of mitigating each of the attacks encountered.

Case 1. Impact of DOS Attack

Here, Eqn. 5 is applied whereby the price data is not available for load scheduling optimization due to DOS attack. From Fig. 6, four events were carried out which includes: load profile with attack on price; load profile with actual day-ahead price; load profile with forecast load profile (generated locally) and load profile without scheduling (which acts as a control).It is observable that the optimized load profile during attack re-traces the forecast load profile. This is because when pricing information is not available the optimized load profile retains approximately same profile as the original forecast load profile. In other words, such an attack will render the scheduling operation temporarily dormant and ineffective.

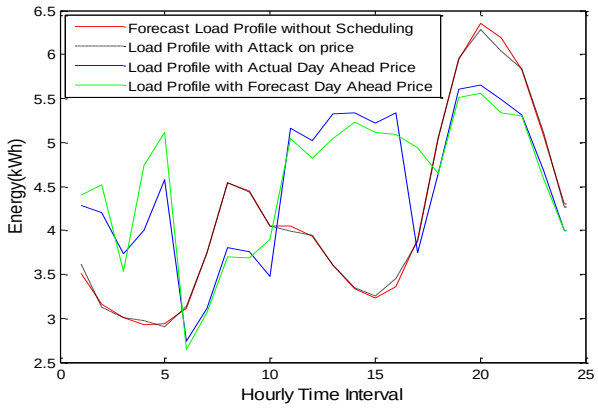

Fig. 6: DOS Impact on Load Profile and Possible Correction

A reliable solution for this attack is to locally generate price forecast which uses historical prices to estimate the day-ahead price, if the use of previous day's data is not acceptable. This outcome is also demonstrated in Fig.6 and it is impressive to observe how much of a good job the forecasted price did in providing a price profile that can be used as an approximate data to substitute a DOS attack on a pricing data.

Case 2. Impact of Constant-Pricing Attack

Here, Eqn. 6 is applied by replacing the dynamic pricing model with a fixed pricing system for different fixed pricing levels. This is as shown in Fig. 7a-c whereby the higher in magnitude of the fixed pricing value, the greater the deviation of the optimized load profile from the forecast load profile. If the constant pricing line goes below the minimum day-ahead price which is \$0.02125/kWh in this illustration, the optimized load profile becomes almost indistinguishable from the forecast load profile. If the fixed pricing value becomes zero, DOS attack as shown in Fig. 6 becomes replicated.

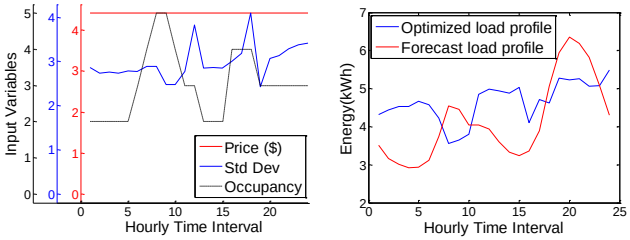

Fig. 7a: Scheduled Load Profile for high Constant Price

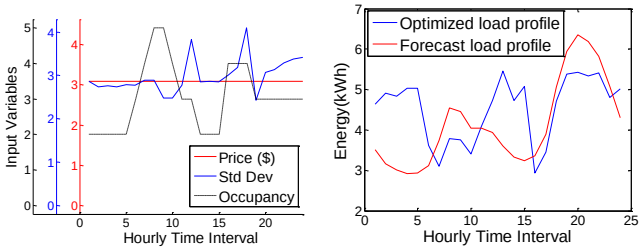

Fig. 7b: Scheduled Load Profile for Medium Constant Price

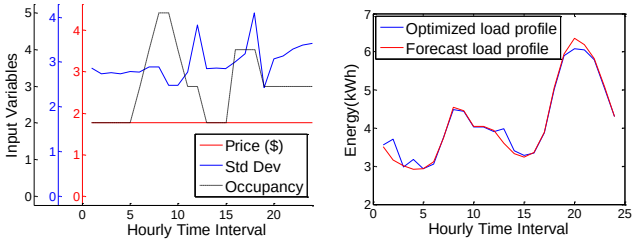

Fig. 7c: Scheduled Load Profile for low Constant Price

This type of attack is considered to be relatively easy to detect especially because constant-valued pricing data is an anomaly in a dynamic pricing system hence, the HEMS can easily flag such as an error. It is therefore possible for the HEMS to find ways to nullifying its impact by requesting for a second update on the pricing information or by relying on a localized forecasting mechanism as discussed in Case 1.

Case 3. Impact of False data-Injection Attack

This attack is modelled using Eqn. 9 and the impact on the optimized load profile is examined assuming the pricing data contains some randomly generated false data As this is gradually introduced to the price variable, the scheduled load responds in different ways. The graphs in Fig.9a-c represent the graphs of load schedules at some selected proportions of price and increasing false data signal combinations from a total of 20 samples. The optimized load profile in Fig.9a shows a greater deviation from the forecast load profile, unlike in Fig.9b and Fig.9c which shows lesser deviations. There is zero false data content in the pricing data according to Fig.9a whereas in Fig.9b and Fig.9c, the false data content is at 10% and 20% of the maximum price value respectively. This information is very important here because it shows that there is a significant difference between the optimized load profiles in Fig.9a and Fig.9b, but little or no difference between Fig.9b and Fig.9c. Hence, introducing false data can quickly degenerate the output almost instantaneously.

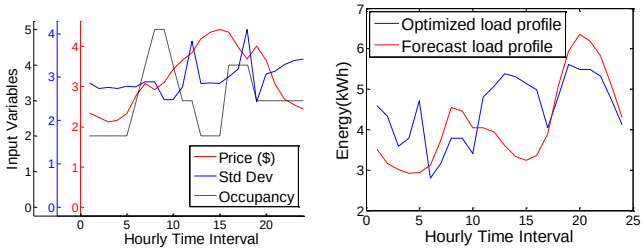

Fig 9a: Load Schedule for High 0 % false data content

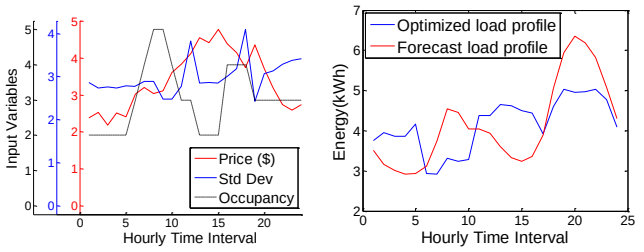

Fig 9b: Load Schedule for Medium 10 % false data content

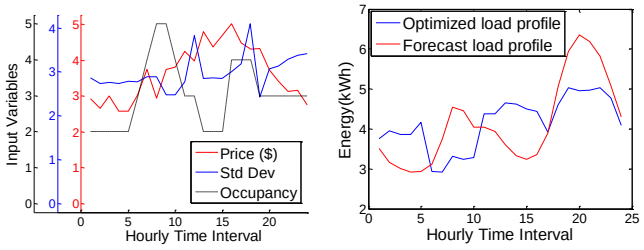

Fig 9c: Load Schedule for Low 20 % false data content

However, it is observable that there is always positive savings obtainable for any given false data injection on the price. This is due to the optimization program that tends to follow the cheapest possible cost for any given input hence, it will be difficult for the optimizer to detect them early enough.

V. DISCUSSION AND CONCLUSION

The optimization constraints are observed to play key roles in ensuring that the optimized load stayed within certain boundaries of the forecast load profile irrespective of the type of attack on the scheduler. This offers a great relief since the impact of such attacks on the household and the grid can be localized and the possibility of causing all the appliances in a household to turn ON at the same time can be suppressed.

The metering system is a possible means to detecting anomalies in view of the availability of the historical load consumption stored in the HEMS. So if strange scheduling pattern is generated, the system could call for a reassessment of all the input data. This is a good step towards effective error detection which will in turn create the avenue to seek the best solution depending on the type of attack involved.

In conclusion, every attack will produce results but with reduced savings and customer satisfaction. This may lead to reduced user engagement in demand response programs but with improved security, advancement of the grid is assured.

VI. REFERENCES

[1] C. Claire, "Survey: Only 14% of Utility Customers Participate in Demand Response Programs," 20 June 2014 ed: UtilityDrive, 2014.

[2] K. Beaver, Hacking for Dummies 5th ed.John Wiley and Sons, 2015.

[3] A. Kharpal, "Hackers are selling your data on the 'dark web' for only $1", CNBC, 2015. Online: Accessed 28th December, 2016. http://www.cnbc.com/2015/09/23/hackers-are-selling-your-data-on-the-dark-web-for-1.html

[4] R. M. Lee, M. J. Assante and T. Conway, Analysis of the Cyber Attack on the Ukranian Power Grid. E-ISAC, 2016. Online. Assessed 31st December 2016.

[5] A. Brauchli and D. Li. A solution based analysis of attack vectors on smart home systems. SSIC 2015. Online: Accessed 2nd January, 2017 http://www2.hawaii.edu/~depengli/Publication/SSIC_Andreas_2015.pdf

[6] B. Hn and H. Gharavi. Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkel Tree 4-Way Handshaking. IEEE Transations on Smart Grid, vol.5, no.2 pp. 550-558, 2013.

[7] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Detecting dynamic load altering attacks: A data-driven time-frequency analysis."

[8] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," IEEE Transactions on Smart Grid, no., 2016.

[9] P. Duhamel and M. Vetterli, "Fast Fourier transforms: a tutorial review and a state of the art," Signal processing, vol. 19, no. 4, pp. 259-299, 1990.

[10] F. Zhang, Z. Geng, and W. Yuan, "The algorithm of interpolating windowed FFT for harmonic analysis of electric power system," IEEE transactions on power delivery, vol. 16, no. 2, pp. 160-164, 2001.

[11] L. T. Berger and K. Iniewski, Smart grid: applications, communications, and security. Hoboken, N.J.: Wiley, 2012.

[12] A. H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," Smart Grid, IEEE Transactions on, vol. 1, no. 2, pp. 120-133, 2010.

[13] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service attacks," The Internet Protocol Journal, vol. 7, no. 4, pp. 13-35, 2004.

[14] A. Illinois, "Day Ahead Pricing used for billing RTP and HSS service," 1st May 2015.

[15] U.S. Department of Energy, "Commercial and residential hourly load profiles for all TMY3 Locations in the United States," 2nd July 2013.