Distributed Internet-based Load Altering Attacks against Smart Power Grids

Amir-Hamed Mohsenian-Rad, *Member, IEEE* and Alberto Leon-Garcia, *Fellow, IEEE*

***Abstract*—With the increase in use of information technology in advanced demand side management and given the growth in power consumption in the computation and communications sectors, a new class of cyber-intrusion plans is emerging that aims to alter the *load* through the Internet and by means of automatic and distributed software intruding agents. These attacks work by compromising direct load control command signals, demand side management price signals, or cloud computation load distribution algorithms to affect the load at the most crucial locations in the grid in order to cause circuite overflow or other malfunctions and damage the power system equipments. To gain insights into these less-examined yet important intrusion strategies, in this paper, we identify a variety of practical loads that can be volnurable to Internet-based load altering attacks. In addition, we overview a collection of defence mechanisms that can help in blocking these attacks or minimizing the damage caused by them. Our simulation results based on the standard setting in the IEEE 24-bus Reliability Test System show that our proposed *cost-efficent load protection* strategy can significantly reduce the cost of load protection while it guarantees that no Internet-based load altering attack may overload the power distribution system.**

***Keywords*: Smart grid security, Internet-based load altering attacks, demand side management, cost-efficient load protection.**

I. Introduction

The recent advancements in smart grid systems and smart metering, such as two-way communication capabilities and distributed intelligence, can significantly enhance efficiency and reliability [1]. However, they may also create new vulnerabilities in power infrastructures if they are not accompanied with appropriate security enforcements. Providing security for such a large-scale system may seem an unfathomable task, and if done incorrectly, can potentially leave utilities and the grid open to a wide range of damaging cyber-attacks [2], [3].

An cyber-intrusion attempt may target any sector in a power system: *generation*, *distribution and control*, and *consumption*. Therefore, depending on the target of attacks, we can identify three different cyber-attack scenarios as shown in Fig. 1. A Type I cyber-attack targets power plants and aims in disrupting or taking over the operation of generators. Although such attacks are sophisticated and require significant resources to be successful; there are multiple reports indicating that such attacks have taken place in the past. For example, in January 2008, the Central Intelligence Agency reported knowledge of four disruptions by hackers of the power suppliers for four cities [3]. Detailed discussions on possible defence mechanisms against Type I cyber-attacks can be found in [4], [5].

Manuscript received October 13, 2010; revised May 06, 2011; accepted June 05, 2011. Date of current version June 16, 2011.

A. H. Mohsenian-Rad is with the Department of Electrical and Computer Engineering, Texas Tech University, Lubbock, TX, 79414, USA, e-mail: hamed.mohsenian-rad@ttu.edu. A. Leon-Garcia is with the the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, M5S 2E4, Canada, e-mail: alberto.leongarcia@utoronto.ca.

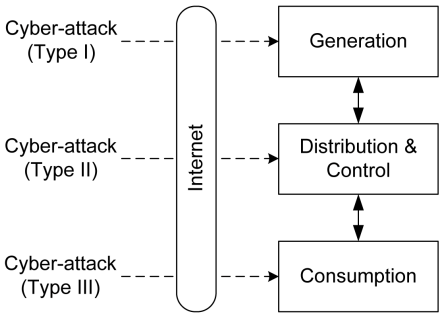

Fig. 1. Three types of cyber-attacks on the electric grid through the Internet. Our focus here is on Type III cyber-attacks against *consumption* sector.

Another class of cyber-attacks, i.e., Type II attacks in Fig. 1, targets power distribution and control. This includes intrusion attempts for altering phase and other grid state information. For example, in *false data injection attacks* against *state estimation*, the hackers attempt to compromise measurement sensors or break into the routers that relay the measured data towards the supervisory control and data acquisition (SCADA) systems in order to insert errors into certain state variable estimations [6]. A successful attack can potentially cause grid instability [7]. Some recent algorithms on detecting and preventing cyber-attacks against state estimation are presented in [8], [9]. Other Type II cyber-attacks may include intrusion attampts to the *control* and *dispatching centers* which can cause blackout or damage to the grid equipments [5].

With the increase in use of information technology (IT) in *demand side management* (DSM) and given the growth in power consumption at the IT, computation, and communications sectors, a new class of cyber intrusion plans is emerging that alter the *load* at certain grid locations through the Internet and by means of automatic and distributed software intruding agents. We refer to this class of cyber-attacks as Type III attacks. The target in Type III cyber-attacks is the consumption sector. An attack may involve *abruptly increasing* the load at the most crucial locations in the grid in order to cause *circuite overflow* or other malfunctioning that can immediately bring down the grid or cause significant damage to the power transmission and user equipments. In this paper, we focus on this less-examined yet important class of intrusion plans. The contributions in our paper can be summarized as follows:

- We identify a variety of practical loads that can be vulnerable targets for Internet-based load altering attacks and the scenarios where the attacks can be successful and cause major damage to the grid. These loads may include

certain types of computation load as well as the loads in direct and indirect demand side management programs.
- We overview multiple defence mechanisms that can be used against Internet-based load altering attacks. They range from protecting the command and price signals in direct and indirect load control to load shedding, attack detection, protecting smart meters, and load relocating.
- Given the high cost of protecting all vulnerable loads in a large power system, we propose a more practical yet cost-efficient load protection strategy which minimizes the cost of load protection while it guarantees that no load altering attack can cause circuite overflow on any transmission line. Our design is within an optimization framework and works by identifying the key locations in the grid where load protection should be focused on.

The rest of this paper is organized as follows. In Section II, we explain three representative target loads for Internet-based load altering attacks and discuss how an attack can take place against each load. A number of defence mechanisms are discussed in section III. Cost-efficient load protection is formulated within an optimization framework in Section IV. Simulations results are presented in Section V. Conclusions and future work are discussed in Section VI.

II. Load Altering Through the Internet

The key idea in Internet-based load altering attacks is to use the Internet to abruptly increase the load at some carefully selected grid locations to cause circuite overflow at the most vulnerable areas of the electric grid. Clearly, not every type of load can be a target for Internet-based load altering attacks as not every type of load is *accessible* through the Internet.

Definition: An Internet-based load altering attack is an attempt to control and change (usually increase) certain load types that are accessible through the Internet in order to damage the grid through circuite overflow or disturbing the balance between power supply and demand. Internet-based load altering attacks are expected to be distributed and target a large number of load and consumption units to be effective.

Next, we discuss three type of loads that are accessible through the Internet and can be target for load altering attacks.

A. Data Centers and Computation Load

Current estimates suggest that the electricity consumption at the IT sector is about 2% of the total consumption in the United States. This share is expected to further increase to about 5% over the next decade [10]. The electricity consumption at the IT sector is particularly boosting as *cloud computing* and the idea of selling *computation power as utility* is becomeing popular and the major cloud providers such as Google and Microsoft are building the world's largest *data centers* across the United States and elsewhere [11]. In most cases, a data center includes hundreds of thousands of computer servers, cooling equipment, and substation transformers. For example, Microsoft's data center in Quincy, Washington has 43,600 square meters of space and uses 4.8 kilometers of chiller piping, 965 kilometers of electric wire, and 1.5 metric tons of backup batteries. In total, this data center consumes 48 MW which is enough to power 40,000 homes [12]. As another example, the National Security Agency is planning to build a massive data center at Fort Williams in Utah which is expected to consume over 70 MW electricity [13].

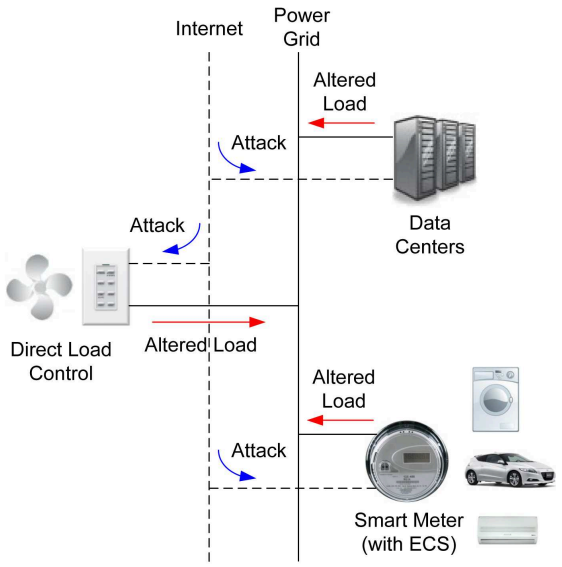

Fig. 2. Internet-based load altering attacks can target data centers, direct load control, and automated energy consumption scheduling units at smart meters.

The power load of a data center is highly *elastic* and depends on the data center's *computation load* [14], [15]. In fact, a data center's energy consumption can almost double when all computer servers are *busy* with computation tasks compared to when the servers are *idle*. Therefore, data centers can be appropriate targets for Internet-based load altering attacks as shown in Fig. 2. While the attacks can be initiated through the Internet and by overwhelming the data center's computer servers via *bogus computation tasks*, the resulting extra power consumption at a data center can cause major impact to the electric grid due to abrupt load fluctuations.

B. Direct Load Control

Demand side management and load shaping programs have been widely deployed over the last two decades. The key idea in these programs is to modify the load curve shape of customers by *deliberate utility intervention*, in order to achieve several objectives, such as minimising peak demand, improving system operation or maximising quality-of-service [16], [17]. One of the most common demand side management programs is known as direct load control (DLC) in which a portion of the load such as air conditioning, water heating, refrigeration, and pool pumps are under the direct control of the utility. One of the largest residential direct load control systems in the world is currently operated by the the Florida Power & Light Co. (FPL) in the United States. It utilizes 800,000 load control transponders and controls 1,000 MW of electrical power (2,000 MW in an emergency). FPL has been able to avoid the construction of some new power plants due to their demand side management programs [18].

Various studies have shown that for a residential direct load control program to be successful, the system should be made as invisible as possible to the customers. A storage water-heating program, for example, can be controlled unnoticed by the customer most of the time. In addition, it is highly beneficial to use *automated* load control systems which are equipped with two-way communications for sending *command signals* to the appliances being controlled. In most cases, command signals include *switch on* or *switch off* commands. Other command signals may also indicate the *length* of each on-off cycle or the *operational power level* to be used by the appliances. Although it may vary depending on the implementation approach, DLC command signals are usually sent via power line carrier [19] or through the Internet [20], [21].

In a Type III cyber-attack scenario, the attacker may aim to compromise the command signals to take over the operation of the residential and industrial load which are supposed to be controlled by DLC programs. For example, by simultaneously sending fabricated *switch on* signals to a group of thousands water heating devices, the attacker can cause a major spike in the aggregate load demand. This can lead to degradation of the power quality, voltage problems, and potential damage to utility and consumer equipment if the system is not properly reinforced. Interestingly, although direct load control has been studied for decades, there have been limited efforts on understanding the impact of possible cyber attacks against these programs. With the recent advancements in smart grid systems and the increasing use of information technology in power infrastructures, such attacks are likely to take place, specially in large scales using sophisticated intrusion techniques.

C. Indirect Load Control

An alternative to DLC is indirect load control which allows customers to control their loads *independently* according to the *price signals* that are sent by the utilities, e.g, through the Internet. In this regard, home automation and the use of *energy consumption scheduling* (ECS) functionality in smart meters have recieved increasing attention over the past few years [22]–[25]. Given the price information and based on the energy consumption needs indicated by the users, the ECS units accordingly schedule the timing and the amont of energy consumption for each household appliance (see Fig. 2). The appliances that are controlled may include thermal comfort equipment (i.e., heating, ventilating, and air conditioning), washing machines, plug-in hybrid electric vehicles, and lighting. The decisions can be made with respect to minimizing the cost of energy, minimizing the finishing time for the operation of certain appliances, or achieving a desired trade-off between cost and timing [22]. The price information can be updated either in real-time or according to a time-ahead pricing model.

Since the price information is obtained through the Internet, automated residential load control is exposed to potential load altering attacks which can be triggered by *false price injection*. By compromising the price signals, an attacker can plan to simultaneously change the energy consumption program in hundreds or thousands of residences and cause major changes in the load profile. The amount of changes highly depends on load elasticity. In general, a decrease in price values results in an increase in the load demand as illustrated in Fig. 3. Therefore, by fabricating signals which indicate lower than actual price values the attacker can cause a major spike in the aggregate load demand. In this case, the damaging impact to the grid will be major if there is no mechanism deployed at smart meters to identify fabricated price information.

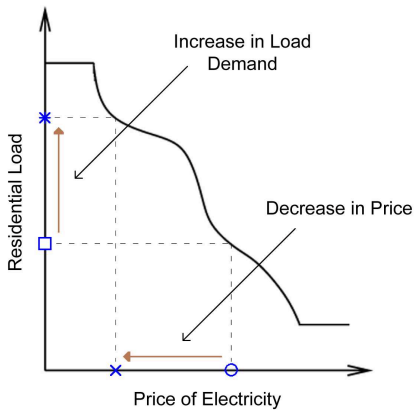

Fig. 3. An example curve showing the relationship between price and the load demand. A decrease in the price value can cause a major increase on load demand depending on how elastic the load is with respect to price changes.

III. Defense Mechanisms and Challenges

From the discussions in Section II, Internet-based load altering attacks against smart power grids can take place in a variety of scenarios. Depending on the scale of the attack, the damage to the grid can be significant and crucial. In this section, we overview a collection of defence mechanisms that can help in blocking this type of cyber-attacks or minimizing the damage caused by them. Here, our focus is to highlight different directions and possible challenges along the line of each defence approach. Details on how each defence mechanism can be implemented and how the listed challenges can be addressed in practice remain open to future studies.

A. Protecting Command and Price Signals

From Sections II-B and II-C, we can see that a large portion of Internet-based load-altering-attack work is based on compromising or fabricating command and price signals in demand side management programs. On one hand, fabricating the command messages can affect direct load control. On the other hand, altering price messages can affect indirect load control and automated energy consumption scheduling. Therefore, protecting the command and price messages can reduce the chance of a Type III cyber-attack to be successful. Such protection can be achieved in different ways. While some approaches are applicable to both command and price messages, there are also certain schemes that better fit the special protection needs for each of the two types of signals.

In direct load control, command messages are usually transmitted as *unicast*. That is, each command is exclusive to a particular user. For example, when a command message indicates the operational power level for a particular appliance,

such command may not be applicable to all users. Instead, it may aim for one user or one chosen group of users. Moreover, the *switch on* and *switch off* cycles are not usually synchronized among all users in order to avoid unwanted spikes in load demand. Therefore, we can assume that command message transmission is essentially a *one-to-one* communication. Then we can apply appropriate message authentication schemes accordingly. One approach is to use *private key encryption* and *message authentication code* (MAC) generation as shown in Fig. 4. Various standard encryption algorithms such as RSA [26] can be used. Some details on private key encryption and related implementation issues can be found in [27].

On the other hand, in indirect load control, price signal transmissions are usually *multicast* as the price is announced to all users. Nevertheless, there is still a critical need for protecting the price signal. In fact, while we want all users to be able to receive and understand the price signals, we want to block any of the users from regenerating the price signals. From this and knowing that some demand side management programs encourage message exchanges not only between the utility and the users but also among the users themesevles [23], [25], there is a need to implement an efficient *group key management* between the utility and its corresponding users. This can be done, for example, by simple pairwise key management which is similar to the structure we already saw in Fig. 4. However, depending on the grid topology and the pricing model, there can be a need for more scalable and computationally efficient schemes such as distributed or hierarchical group key management methods [28], [29].

B. Protecting Smart Meters and Data Centers

Besides direct protection of the price and command signals from being fabricated by unauthorized sources, we also require to protect the smart meters themselves from intrusion. In a recent study on advanced metering infrasttructure, the cyber security issues of smart meters are identified within four categories of *confidentiality*, *integrity*, *availability*, and *accountability* [30]. Both integrity and availability concern unauthorized modification or access to the normal operation of the smart meters by means of setting up passwords, firewalls, and identity authentication. Clearly, the chance for a cyber attack to be successful can be significantly reduced in a reinforced metering infrastructure where *both* the meter and the incoming price and command signals are being highly protected. In a similar way, data centers need to be protected against *bogus computation tasks*, *flooding*, and *denial-of-service* attacks.

C. Attack Detection and Learning Demand Patterns

While the defence mechanisms that we explained in Sections III-A and III-B intend to prevent load altering attacks, we also need strategies to block a successful intrusion from causing a major damage to the grid. In this regard, a regional grid operator or a utility company may attempt to curtail an affected load at certain buses through the use of aggregators, substations, and circuit breakers. However, any action of this kind requires to first carefully *identify which load has been compromised*. This can be done, for example, by learning

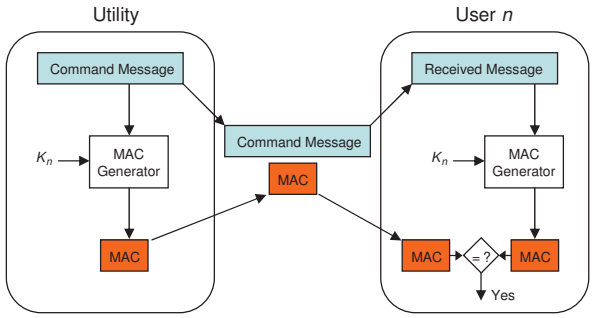

Fig. 4. The command messages sent by utility can be authenticated by using a private key encryption and message authentication code generation.

the normal demand pattern for each type of residential or commercial load at each region. That is, by keeping track of the daily and hourly load at each power consumption sector and looking for any behavior which demonstrates significant mismatch with the normal trend for that particular load. As an example, most measurements suggest that the residential peak load is usually around 5:00 PM to 11:00 PM while the industrial peak load is around 7:00 AM to 5:00 PM [29]. Therefore, if an aggregator observes a sudden increase for a group of houses on a weekday at 10:00 AM, then it can become suspicious about a potential cyber-attack to the automated energy consumption scheduling units in that neighborhood. Of course, this simple example can be extended to more sophisticated and multi-layer detection scenarios. Given a load altering attack detection alarm, the aggregator can set up a quick authentication process with the suspected smart meter and possibly consider load shedding as the final step, when the grid is indeed at risk, as we will discuss next.

D. Load Shedding and Load Relocating

If the grid and power transmission equipments are at risk due to excessive load demand, *load shedding* is an inevitable option. As the first step, the immediate action could be shutting down automated load scheduling or curtailing the load at locations where an load altering attack is detected with a high probability. This will not affect the operation of the rest of the grid, but there is still a need for a chain of actions to bring the affected load into normal operation. The next step, could be shedding other load at the most crucial grid locations while taking into account different classes of load contracts and other considerations which are common in load curtailing processes such as the cost of load shedding [31], [32].

In certain scenarios, *load relocating* can replace load shedding, where instead of curtailing a load, we move it from one location to a different grid location in order to make the load distribution more balanced and to reduce the load at buses that are overloaded. One example for the load that can be relocated is the load at the computation sector which can be moved through the Internet from one data center to another data center somewhere else in the grid. Therefore, while the IT loads can be potential targets for Internet-based load altering attacks, if they are well-protected, they can instead help the grid in load relocating. Recent results on the coordination of computation sector and the smart grid can be found in [33].

IV. Cost-Efficient Load Protection

Applying the defence mechanisms from Section III can prevent load altering attacks, but they also impose new costs to the grid operators. In fact, depending on the type of load and the choice of defence mechanisms being implemented, the cost of a *full load protection*, i.e., protecting *all* vulnerable loads, can be significant. Therefore, in practice, the grid operators may choose to implement *partial load protection*. In that case, they need to carefully identify the most critical locations in the electric grid and protect the load only at those locations. This leads to the following design problem. Given the prior knowledge about the grid topology, the locations of loads, the type of load at each location, locations and capacities of generators, and nodal admittance and the capacity of all power transmission lines, we need to identify the portion of the load to protect against Internet-based load altering attacks such that the cost of load protection is minimized while ensuring that the remaining unprotected load cannot cause circuite overflow or any other major harm to the electric grid. In this section, we solve this problem within an optimization framework.

A. System Model

Let N denote the set of all buses in the grid. For each bus $i \in \mathcal{N}$, let G_i denote the amount of active generation power at bus i. Also let L_i denote the amount of normal active load power at bus i, that is, the load when no load altering attack is taking place. Similarly, we assume that Δ_i denotes the *maximum* amount of *extra* active load power that can be added to bus i in the absence of any load protection. Moreover, we assume that the portion of the extra load at bus i which is being protected is denoted by α_i. Note that $0 \leq \alpha_i \leq 1$. If no protection is used at bus i, then the total altered load can be as high as Δ_i, i.e., the whole vulnerable load. However, if α_i portion of the vulnerable load at this bus is protected, then the total altered load will be limited to $(1-\alpha_i)\,\Delta_i$. Therefore, the total active load power at bus i is obtained as

$$P_i = L_i + (1-\alpha_i)\,\Delta_i - G_i. \tag{1}$$

Clearly, if the active power generation is greater than the active power load, then P_i will be a negative number. Next, assume that θ_i denotes the voltage phase angle at bus i and B_{ij} denotes the imaginary term in the complex value at row i and column j of the *Y-bus* matrix of the grid. We also denote P_{ij} as the power flow over each branch (i,j) in the electric grid where $i,j \in \mathcal{N}$. Focusing on the *per-unit* setting of power systems, we can derive *DC power flow equations* as follows [34]:

$$G_i - L_i - (1-\alpha_i)\Delta_i = \sum_{j=1, j\neq i} B_{ij}\,(\theta_i - \theta_j)\,, \qquad \forall\, i \in \mathcal{N}, \tag{2}$$

and

$$P_{ij} = B_{ij}\,(\theta_i - \theta_j)\,, \qquad \forall\, i,j \in \mathcal{N}. \tag{3}$$

In order to solve the system of linear equations in (2) and (3), it is required to take one voltage phase angle as reference. For example, we may assume that $\theta_1 = 0$. In that case, and given the values of L_i, Δ_i, G_i, α_i, and B_{ij} for all buses and all branches in the grid, solving (2) and (3) will uniquely identify all voltage phase angles and all branch power flows.

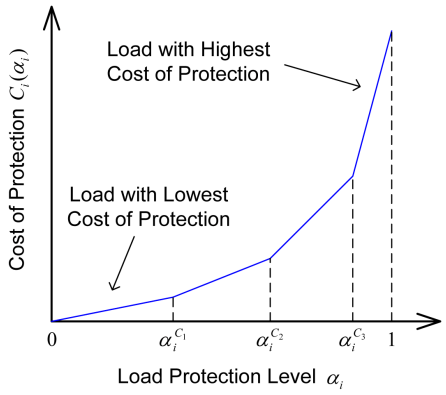

Fig. 5. A piecewise linear load protection cost funcion with four load classes.

B. Problem Formulation

Let $P_{ij}^{\max}$ denote the power transmission capacity of branch (i,j). In order to avoid circuite overflow, it is required that

$$P_{ij} \leq P_{ij}^{\max}, \qquad \forall\, i,j \in \mathcal{N}. \tag{4}$$

From (2) and (3), whether circuite overflow occurs depends on the amount and the distribution of load across different buses in the electric grid. Without loss of generality, we assume that no circuite overflow occurs if $\Delta_i = 0$ for all $i \in \mathcal{N}$. That is, the power transmission capacity of the branches are enough as long as no load altering attack is taking place. Next, we find the *best* choice of *load protection level* α_i for all buses $i \in \mathcal{N}$ such that we can minimize the cost of load protection.

Let $C_i(\alpha_i)$ denote the cost of load protection at bus $i \in \mathcal{N}$. We assume that the cost is an increasing function of the protection level α_i. If $\alpha_i = 0$ then $C_i(\alpha_i) = 0$. That is, if no load is being protected at bus i, then no cost would be associated to the load protection at this bus of the electric grid. The cost of load protection grows as α_i increases. If $\alpha_i = 1$, then full load protection is being implemented at bus i. We are now ready to formulate *cost-efficient load protection* as the optimal solution of the following optimization problem:

$$\begin{aligned} \textbf{minimize}_{\boldsymbol{\alpha}} \quad & \sum_{i\in\mathcal{N}} C_i(\alpha_i) \\ \textbf{subject to} \quad & \text{Eqs. } (2)-(4). \end{aligned} \tag{5}$$

Here, the optimization variables are the load protection levels at all buses, i.e., the entries in vector $\boldsymbol{\alpha} = (\alpha_i,\ \forall\, i \in \mathcal{N})$. By solving (5), we determine the amount of load protection at each bus to minimize the total cost of load protection.

C. Solution Approach

The complexity of optimization problem (5) mostly depends on the type of the cost functions $C_i(\cdot)$ for all buses $i \in \mathcal{N}$. A class of cost functions which is practical and can also lead to tractable formulation of problem (5) is the family of *piecewise linear* functions as shown in Fig. 5. In this setting, we divide the load to be protected at each bus into several classes

depending on their cost to be protected. Let K_i denote the number of such load classes at bus i. After sorting these classes in an ascending order with respect to the cost of protection, we define K_i class indicators $\alpha_i^{C_1}, \alpha_i^{C_2}, \ldots, \alpha_i^{C_{K_i-1}}$, where

$$0 < \alpha_i^{C_1} < \alpha_i^{C_2} < \ldots < \alpha_i^{C_{K_i-1}} < 1. \quad (6)$$

Starting with the case when no load is protected, the cost of protection increases linearly as we protect more load and we increase α_i from zero to $\alpha_i^{C_1}$. When all the load in the class with the lowest cost of protection is secured then we move on to the next load class which has a higher cost of protection. This procedure can continue by further increasing α_i until we finish protecting the class with highest cost of protection and reach the full load protection level, if necessary. Given piecewise linear cost functions, optimization problem (5) can be formulated as a linear program and be solved efficiently by using techniques such as the interior point method [35].

V. Numerical Example

A. Setting

Consider the power grid in Fig. 6. This is a modified version of the IEEE 24-bus reliability test system in [36]. It includes 24 buses and 38 branches. There are 10 buses with generation capacities. The generation capacity is fixed at nine buses. The generator at bus 22 works as a *spinning reserve* [34]. That is, at each time, it provides the extra generation capacity that needs to be injected into the grid in order to balance supply and demand. There are 18 buses with different amounts of load demand. Among them, in 10 buses the load is *not* accessible through the Internet and there is no risk of Internet-based load altering attack. However, there exist various loads that are vulnerable to load altering attacks at the other eight buses. The location of these buses are highlighted by a separate numbering in Fig. 6. The generation capacities and the load demand parameters at all buses are shown in Table I.

There are four data centers connected to the electric grid at buses 1, 13, 15, and 18. The energy consumption parameters for all data centers are assumed to be the same as those reported in [14], [33]. Therefore, for each data center, the normal load and the peak load are assumed to be 50 MW and 100 MW, respectively. There are also four demand side management units connected to the grid at buses 3, 7, 20, and 23. Automated load control is assumed to be direct at buses 7 and 20 and indirect at buses 3 and 23. For the purpose of our study, we assume that for all buses that serve the demand side management units, the normal load is 50 MW while the peak load is 100 MW. For all loads that are vulnerable to the Internet-based load altering attacks, we assume that the load protection cost function is piecewise-linear. Without loss of generality, we assume that $K_i = 2$ and $\alpha_i^1 = \frac{1}{2}$ for all $i \in \{1, 3, 7, 13, 15, 18, 20, 23\}$. The slope of the piecewise-linear cost function increases by 50% for the portion of the load which has a higher cost of protection. Finally, we assume the use of underground monopole high voltage direct current transmission lines in the considered grid, where for each branch (i, j) of the grid we set $P_{ij}^{\max}$ = 400 MW.

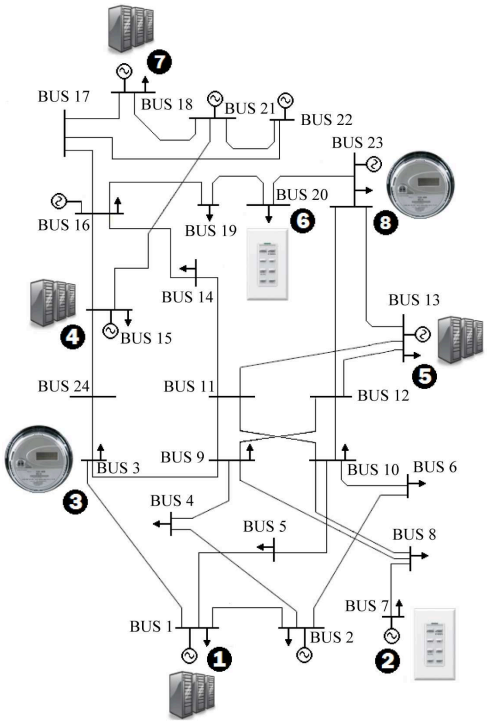

Fig. 6. The IEEE 24-bus reliability test system. Various types of load which are accessible through the Internet are connected to the grid at eight buses.

TABLE I
Generation Capacity and Load Demand at Each Bus‡

	Generation Capacty G_i	Fixed Load L_i	Added Load Δ_i
BUS 1	172	50	50
BUS 2	172	116	-
BUS 3	-	50	50
BUS 4	-	74	-
BUS 5	-	71	-
BUS 6	-	136	-
BUS 7	115	50	50
BUS 8	-	171	-
BUS 9	-	175	-
BUS 10	-	195	-
BUS 11	-	-	-
BUS 12	-	-	-
BUS 13	186	50	50
BUS 14	-	294	-
BUS 15	215	50	50
BUS 16	155	233	-
BUS 17	-	-	-
BUS 18	200	50	50
BUS 19	-	181	-
BUS 20	-	50	50
BUS 21	231	-	-
BUS 22	400†	-	-
BUS 23	600	50	50
BUS 24	-	-	-

‡ All amounts are in megawatts.
† Spinning reserve generation capacity.

B. Cost-efficient Load Protection

Based on the simulation setting described in Section V-A, we first compare the three cases of *full load protectioin*, *optimal cost-efficient load protection*, and *no load protection*. The results are shown in Fig. 7, where we plot the power flow amounts on the three highly congested transmission lines

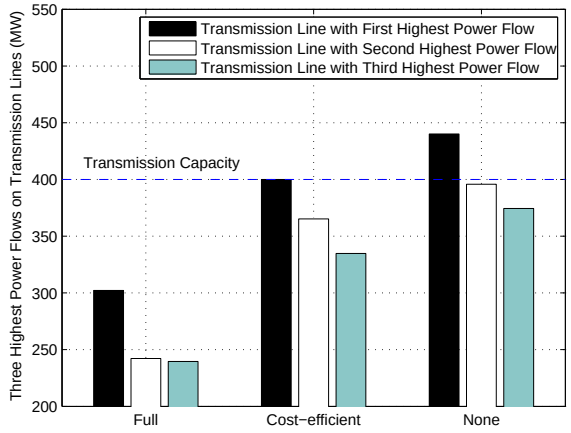

Fig. 7. Comparing power flows at three load protection scenarios.

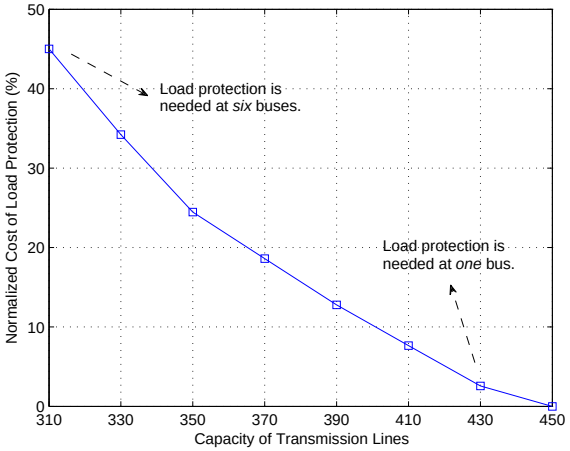

Fig. 8. The cost of optimal load protection for different line capacities.

for each load protection scenario. We can see that if no load protection is being implemented there will be one transmission line with a power flow over 440 MW which is significantly higher than the assumed capacity of the transmission lines. It corresponds to the branch (17, 16) in the grid in Fig. 6. On the other hand, a full load protection can assure no extra load on any of the eight buses with accessible load through the Internet. However, we can see that even a partial yet efficient load protection approach can be sufficient to limit the power flow across all grid branches below their transmission capacities. In a cost-efficient load protection scenario, we have $\alpha_{13} = 0.50$, $\alpha_{20} = 0.50$, and $\alpha_{23} = 0.22$. In addition, $\alpha_i = 0$ for all $i \in \mathcal{N}\backslash\{13, 20, 23\}$. That is, in order to assure that no Internet-based load altering attack can cause a circuite overflow, it is *enough* to only protect half of the computation load at bus 13, half of the directly controled load at bus 20, and a quarter of the indirectly controlled load at bus 23. The cost in this case is only 10.2% of the cost in full load protection.

C. Impact of Changes in Grid Parameters

In general, the cost of efficient load protection against Internet-based load altering attacks depends on various grid parameters such as the capacity of transmission lines, as shown in Fig. 8. In this figure, the costs are normalized with respect to the cost of full load protection. We can see that the cost drops as the capacity of transmission lines increases. As an example, for the case when the line capacity is 310 MW, the optimal load protection variables are obtained as $\alpha_1 = 0.50$, $\alpha_3 = 0.50$, $\alpha_7 = 0.79$, $\alpha_{13} = 0.81$, $\alpha_{20} = 0.84$, and $\alpha_{23} = 0.76$ while we have $\alpha_i = 0$ for all $i \in \mathcal{N}\backslash\{1, 3, 7, 13, 20, 23\}$. As another example, for the case when the line capacity is 430 MW, the optimal load protection variables are $\alpha_7 = 0.31$ and $\alpha_i = 0$ for all $i \in \mathcal{N}\backslash\{7\}$. In fact, the direct load control system connected to bus 7 is the most critical load to be protected against Internet-based load altering attacks for the electric grid scenario in Fig. 6.

Next, we investigate the cost of load protection when the location of spinning reserve generator changes. Recall that in our simulation setting, the spinning reserve generator is considered to balance the supply and demand and incorporate

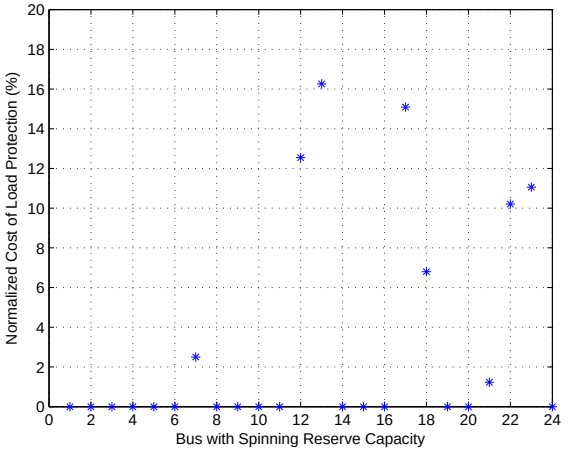

Fig. 9. The cost of optimal load protection when we change the location of the generator with spinning reserve capacity across the electric grid.

the changes in the load due to potential Internet-based load altering attacks. The results are shown in Fig. 9. Here, we assume that the line capacities are all 400 MW. We can see that depending on where we place the spinning reserve generator, the normalized cost of required optimal load protection can be as low as zero (as in the case when we place the spinning reserve generator at buses $1, 2, \ldots, 6$) or as high as 16% of the full load protection cost. This is yet another example showing that an efficient load protection mechanism against Internet-based load altering attacks shall necessarily take into account the grid topology and various other grid parameters.

VI. Conclusions and Future Work

In this paper, we took a first step towards understanding the Internet-based load altering attacks against smart power grids. In this regard, we studied different scenarios where a load can be accessed through the Internet and can become a target for load altering attacks. We identified three important classes of vulnerable load scenarios: data centers and computation load, direct load control, and indirect load control. We showed that

an attack may take place by compromising the direct load control command signals, indirect load control price signals, or cloud computation load distribution algorithms. Therefore, useful defence mechanisms can range from protecting the command and price signals to load shedding, attack detection, and load relocating. Given the high cost of protecting all vulnerable loads in a large power system, we proposed a cost-efficient load protection strategy which minimizes the cost of load protection while it prevents overloading the grid.

REFERENCES

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, pp. 52–62, Mar. 2009.

[2] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[3] S. M. Amin, "Securing the electricity grid," *The Bridge, quarterly publication of the U.S. National Academy of Engineering*, vol. 40, no. 1, pp. 13–20, Mar. 2010.

[4] N. Ye, J. Giordano, and J. Feldman, "Securing the electricity grid," *Communications of the ACM*, vol. 44, no. 8, pp. 76–82, Aug. 2001.

[5] W. F. Boyer and S. A. McBride, "Study of Security Attributes of Smart Grid Systems Current Cyber Security Issues," Idaho National Laboratory Technical Report, Apr. 2009.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM CCS'09*, Chicago, IL, Nov. 2009.

[7] H. M. Kim, J. H. Jeon, M. C. Shin, and T. K. Oh, "New design of PMU for real-time security monitoring and control of wide area intelligent system," *Lec. Notes in Comp. Sci.*, vol. 4252, pp. 812–818, Oct. 2006.

[8] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. of IEEE Int. Conference on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010.

[9] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. of First Workshop on Secure Control Systems*, Stockholm, Sweden, Apr. 2010.

[10] W. S. Baer, S. Hassell, and B. A. Vollaard, *Electricity Requirements for a Digital Society*. RAND Publisher, 2002.

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California at Berkeley, Research Report, Feb. 2009.

[12] R. H. Katz, "Tech Titans Building Boom," *IEEE Spectrum*, pp. 40–54, Feb. 2009.

[13] R. Miller, "NSA Plans 1.6 Billion Dollars Utah Data Center," Data Center Knowledge Website, Jun. 2009.

[14] X. Fan, W. D. Weber, and L. A. Barroso, "Power provisioning for a warehouse-sized computer," in *ACM International Symposium on Computer Architecture*, San Diego, CA, Jun. 2007.

[15] A. H. Mohsenian-Rad and A. Leon-Garcia, "Energy-information transmission tradeoff in green cloud computing," in *Proc. of IEEE Globecom'10*, Miami, FL, Dec. 2010.

[16] C. M. Chu, T. L. Jong, and Y. W. Huang, "A direct load control of air-conditioning loads with thermal comfort control," in *Proc. of IEEE PES General Meeting*, San Francisco, CA, Jun. 2005.

[17] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A direct load control model for virtual power plant management," *IEEE Trans. on Power Systems*, vol. 24, no. 2, pp. 959–966, May 2009.

[18] V. Silva, "Value of smart appliances in system balancing," Imperial College, London, Technical Report - Value of Smart Domestic Appliances in Stressed Electricity Networks, 2009.

[19] D. D. Weers and M. A. Shamsedin, "Testing a new direct load control power line communication system," *IEEE Trans. on Power Delivery*, vol. 2, no. 3, pp. 657–660, Jul. 1987.

[20] J. T. K. Ma, T. M. Liu, and L. F. Wu, "New energy management system architectural design and intranet/internet applications to power systems," in *Proc. of IEEE Int. Conference on Energy Management and Power Delivery*, Singapore, Mar. 1998.

[21] S. Medida, N. Sreekumar, and K. V. Prasad, "SCADA-EMS on the Internet," in *Proc. of IEEE Int. Conference on Energy Management and Power Delivery*, Singapore, Mar. 1998.

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

[23] A. H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, and R. Schober, "Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid," in *Proc. of IEEE PES Conference on Innovative Smart Grid Technologies*, Gaithersburg, MD, Jan. 2010.

[24] S. Caron and G. Kesidis, "Incentive-based energy consumption scheduling algorithms for the smart grid," in *Proc. of IEEE Int. Conference on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010.

[25] A. H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. on Smart Grid*, vol. 1, no. 3, pp. 320–331, 2010.

[26] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Jul. 1978.

[27] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC Press, 2007.

[28] P. Kruus and J. Macker, "Techniques and issues in multicast security," in *Proc. of IEEE Milcom*, Boston, MA, Oct. 1998.

[29] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, 2003.

[30] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure," in *Proc. of IEEE Power and Energy Society General Meeting*, Pittsburgh, PA, Jul. 2008.

[31] G. S. Grewal, J. W. Konowalec, and M. Hakim, "Optimization of a load shedding scheme," *IEEE Industry Applications Magazine*, vol. 4, no. 4, pp. 1077–2618, Aug. 1998.

[32] P. Wang and R. Billinton, "Optimum load-shedding technique to reduce the total customer interruption cost in a distribution system," *IEE Proceedings Generation, Transmission and Distribution*, vol. 147, no. 1, pp. 51–56, Jan. 2000.

[33] A. H. Mohsenian-Rad and A. Leon-Garcia, "Coordination of cloud computing and smart power grids," in *Proc. of IEEE Int. Conference on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010.

[34] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. Wiley-Interscience, 1996.

[35] D. Bertsimas and J. N. Tsitsiklis, *Introduction to Linear Optimization*. Belmont, MA: Athena Science, 1997.

[36] "Reliability Test System Task Force of the Application of Probability Methods subcommittee - The IEEE Reliability Test System - 1996," pp. 1010–1020, Aug. 1999.

Amir-Hamed Mohsenian-Rad (S04-M09) received masters degree in Electrical Engineering from Sharif University of Technology in 2004 and Ph.D. degree in Electrical and Computer Engineering from The University of British Columbia in 2008. Currently, he is an Assistant Professor at the Department of Electrical and Computer Engineering at Texas Tech University. He is an Associate Editor of the *International Journal of Electronics and Communication* and the TPC Co-chair of the first *IEEE International Workshop on Smart Grid Communications and Networking*. His research interests include design, optimization, and game-theoretic analysis of communication networks and smart power systems.

Alberto Leon-Garcia (F99) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of Southern California, in 1973, 1974, and 1976, respectively. Currently, he is a Professor in Electrical and Computer Engineering at the University of Toronto. He is a Fellow of the IEEE "For contributions to multiplexing and switching of integrated services traffic". He is also a Fellow of the Engineering Institute of Canada. He has received the 2006 Thomas Eadie Medal from the Royal Society of Canada and the 2010 IEEE Canada A. G. L. McNaughton Gold Medal for his contributions to the area of communications. He holds a Canada Research Chair in Autonomic Service Architecture.