The Hierarchical Smart Home Cyberattack Detection Considering Power Overloading and Frequency Disturbance

Yang Liu, Shiyan Hu, Senior Member, IEEE, Albert Y. Zomaya, Fellow, IEEE

Abstract—The concept of smart home has recently gained significant popularity. Despite that it offers improved convenience and cost reduction, the prevailing smart home infrastructure suffers from vulnerability due to cyberattacks. It is possible for hackers to launch cyberattacks at the community level while causing a large area power system blackout through cascading effects. In this paper, the cascading impacts of two cyberattacks on the predicted dynamic electricity pricing are analyzed. In the first cyberattack, the hacker manipulates the electricity price to form peak energy loads such that some transmission lines are overloaded. Those transmission lines are then tripped and the power system is separated into isolated islands due to the cascading effect. In the second cyberattack, the hacker manipulates the electricity price to increase the fluctuation of the energy load to interfere the frequency of the generators. The generators are then tripped by the protective procedures and cascading outages are induced in the transmission network. The existing technique only tackles overloading cyberattack while still suffering from the severe limitation in scalability. Therefore, based on partially observable Markov decision processes, a hierarchical detection framework exploring community decomposition and global policy optimization is proposed in this work. The simulation results demonstrate that our proposed hierarchical computing technique can effectively and efficiently detect those cyberattacks, achieving the detection accuracy of above 98%, while improving the scalability.

Index Terms—Smart Home, Cascading, Power Overloading, Frequency Disturbance, Hierarchical Optimization

I. INTRODUCTION

S

MART home, as a key part of the smart grid, automatically controls the household activities and energy usage of the customers with smart controllers. It can shift the heavy energy load away from the peak pricing hours to non-peak ones, thus providing convenience, energy saving and electricity bill reduction to the customers [2], [3]. Under a sophisticated pricing scheme, smart home technique can also benefit the power grid through balancing the energy load [1]. In the prevailing U.S. electricity market, real time pricing and guideline pricing, also known as predictive pricing and day ahead pricing are widely deployed pricing schemes which are usually used together. While the customers are billed based on the real time energy usage in real time pricing, the utilities predicts the future electricity price to facilitate smart scheduling in guideline pricing. Refer to [4] for guideline and real time prices. The smart controller in each home can launch the home appliances when the guideline price is relatively low, which is known as smart home scheduling.

The smart home scheduling technique is facilitated by advanced metering infrastructure (AMI), which connects the smart meters installed in the homes of customers to the communication networks of smart grid. Taking advantage of the AMI, the utility transmits the guideline price to the data center of each community. Subsequently, the guideline price is broadcast to all the smart meters in the target community through the wireless communication protocols such as WiFi and WLAN [5]. Such an infrastructure is vulnerable to different threats [6]. For example, the work [7] hacks an Itron CL200 smart meter by analyzing EEPROM dump to modify the ID. Subsequently, the hacked smart meter is used to send out manipulated metering data containing the ID of target smart meters. Furthermore, the work [8] studies the vulnerability of smart meters to malware propagation through the advanced metering infrastructure. In the recent Ukrainian blackout in December 2015, the attackers gained a foothold on the computer system of a power company, open the breakers and delayed restoration efforts using malware [9]. This is the first known blackout induced from malware, which further demonstrates the vulnerability of AMI.

This paper considers electricity pricing manipulation cyberattack as in [1]. In the electricity pricing manipulation cyberattack, a malicious hacker can tamper the smart meters, jam the access points or even attack the data center. Subsequently, the hacker can manipulate the guideline price, thus misleading the smart controllers to increase the peak energy load. However, the works [1] do not consider the system level impact of pricing cyberattacks. The increase of peak energy load in a community can increase the power flow on the transmission lines, which weakens the power grid by reducing the operation margin. In this scenario, the power flow of a transmission line can be further increased easily by an additional fault such that the capacity is violated. The violation of transmission line capacity can also be directly caused by a severe peak energy load. Thus, that transmission line will be tripped to protect the power system and the power flow has to be reallocated, which may trip more transmission lines due to overloading [10]. Such a sequential procedure can cut off the power supply of each local community, which eventually results in the blackout. In fact, a great portion of the well known blackouts are caused by cascading failure including the Northeast blackout in 2003 [11].

The cascading outages in power systems have been studied in the existing literature. In [14], the impact of hidden failure on cascading outages is studied. In [15], the relationship between power system topology and cascading failure is investigated. Preventing the cascading outages is also a widely studied topic. In [16], the potential cascading modes are identified by contingency analysis and fast sequential outage simulation, respectively. In [10], the benefit of distributed generation is studied in mitigating...
cascading impact of transmission line outages. However, all of the above works only analyze the theoretical setup which could potentially induce cascading impacts. For example, some existing works simulate the cascading outages starting from the fault on a random transmission line, which is not practical.

This work analyzes the cascading impact of electricity pricing manipulation cyberattack which is relatively more practical to be deployed. Besides the cascading impact of power overloading, a new type of cyberattack is studied, which impacts the dynamics of the power system. The hacker can manipulate the guideline price such that the energy load changes dramatically at a time slot to impact generation frequency [12]. A significant frequency change can damage the equipments such that the grid operator has to trip the generators if the frequency cannot be recovered to standard level by the load frequency control techniques [13], which can induce a larger area blackout through cascading outages.

The significant impact of smart home cyberattacks necessitates the development of detection techniques. There can be various solutions to protect the smart meters from being hacked. For example, a community can utilize smart meters from different manufacturers such that a hacker cannot attack a large number of smart meters using the same strategy due to the uniqueness. The manufacturer can also improve the security level of smart meters while fabrication using jointly verification of software and hardware. Despite the increased difficulty for hacking the smart meters, a system level cyberattack detection technique is still necessary since there still exit various backdoors in smart meters and advanced metering infrastructure. Although partially observable Markov decision process (POMDP) based detection technique has been proposed in [1], it suffers from limited scalability [17]. Given a system with large number of customers, the conventional POMDP based detection technique cannot compute a solution efficiently or even runs out of memory. To tackle this difficulty, a hierarchical framework is developed such that the attacking states of the smart meters are modeled in a distributed fashion while a centralized decision is made for checking and repairing the hacked smart meters. The contributions of this work are summarized as follows.

• The electricity pricing manipulation cyberattack that creates a sharp change in the energy load is proposed, which can potentially change the generation frequency dramatically.
• The cascading impact of the pricing cyberattacks are analyzed. The cyberattack targeting increasing the peak energy load can sequentially trip the transmission lines through overloading while the cyberattack targeting increasing the energy load fluctuation can trip the generators through frequency disturbance. Both of them can induce a large area blackout.
• A hierarchical detection framework is developed based on partially observable Markov decision process. It models the state of each smart meter in a distributed fashion and uses global policy optimization algorithm to make a centralized decision on checking and repairing the hacked smart meters.
• The simulation results demonstrate that the cyberattacks can effectively manipulate the energy load in the local community and cause blackout to the large area through cascading impact.
• The proposed detection framework is validated through simulations. It is demonstrated that the proposed detection framework can detect the cyberattacks with an accuracy above 98% and effectively reduce the peak and fluctuation of the energy load due to cyberattacks.

The rest of this paper is organized as follows. In Section II, two different types of pricing cyberattacks are introduced. In Section III, the cascading impacts of the proposed cyberattacks are analyzed. In Section IV, the hierarchical detection framework is developed based on partially observable Markov decision process. In Section V, simulations are conducted to evaluate the impact of the cyberattacks and the performance of the detection technique. The paper is summarized in Section VI.

II. PRICING CYBERATTACKS ON SMART HOME SYSTEMS

The smart home system features the automatic control of household activities. In particular, based on the guideline price published by the utility, it optimizes the energy usage scheduling such that the customers schedule more energy consumption at non-peak pricing hours, which is known as smart home scheduling technique. This helps balance the energy load in the power grid and save the economical cost of the customers on energy usage [1]. The smart home scheduling problem has been studied in the work [3], [18]. Generally speaking, it relies on the massive deployment of smart meters, which is supported by the advanced metering infrastructure (AMI) [6]. The utility uses fiber cable to transmit the pricing information to the community level data center, which then forwards it to the targeting customers through the wireless communication protocols such as WiMAX, WLAN and WiFi [5]. As is studied in [1], such an infrastructure is vulnerable to cyberattacks.

In the smart home context, the hacker can attack the smart meters and modify the received pricing information, which is defined as electricity pricing manipulation cyberattack [1]. In the advanced metering infrastructure (AMI), each smart meter can be easily identified. Thus, a malicious hacker can launch a cyberattack on the smart meter using malware and propagate it in the AMI to infect more even smart meters. The work [8] has analyzed malware propagation and demonstrated that it can lead to the delay of communications and denial of service. In the smart home context, the malicious hacker can manipulate the received guideline price through the cyberattacks, which can increase the peak energy usage or create a sharp energy load change.

A. Pricing Cyberattack Targeting Increasing Peak Energy Usage

The cyberattack targeting increasing peak energy usage has been studied in the previous works [1]. An overview is included in this paper for completeness. In the smart home context, the customer usually avoid using electricity energy during peak hours to save the bill. However, the energy usage in the evening may still be high due to the activities such as watching TV. Suppose that the hacker launches a cyberattack and manipulate the guideline price to make it very low during these time slots, heavy energy load will accumulate there due to the smart home scheduling as well as the existing human activities. This will increase peak energy usage, which could lead to cascading outages in the power system as discussed in Section III. The procedure for the cyberattack targeting increasing the peak energy usage is as follows [1].

• Determine the starting time \( t_s \) and ending time \( t_e \) for creating peak energy usage.
• Manipulate the guideline electricity price received by the target smart meters to make it very low from \( t_s \) to \( t_e \).
• Energy load will be increased significantly from \( t_s \) to \( t_e \).
A hacker can increase the peak energy load of some communities such that the capacity of a transmission line is exceeded due to power flow increase. Subsequently, the protective mechanism will be triggered to trip the transmission lines, which changes the topology of the transmission network such that the power flow need to be re-calculated. This can cause more transmission lines being tripped and break the transmission network into disconnected islands, which results in a large area blackout.

- A sharp fluctuation of energy load can disturb the power system dynamics. Thus, a hacker can increase the energy load rapidly such that the rotor of the generator needs to slow down to release the kinetic energy in order to compensate the increased electricity energy demand. This leads to the drop of generation frequency. The operation frequency is usually maintained within a normal range by load frequency control (LFC) technique. However, if the change of system frequency is beyond a certain threshold (e.g., 1% of the nominal operation frequency), the LFC is no longer able to recover it. The impact of the frequency change will propagate in the power grid and damage the equipments. In this situation, the generators have to be tripped and the energy supply is interrupted.

A. Cascading Outages on Transmission Line

Consider a set of communities where each community is connected to a bus, which is inter-connected with other buses by transmission lines. Some of the buses are directly connected to the generators, which are defined as generation buses. The buses without generators are defined as load buses. The energy demand of the load buses is supplied by the generators via the transmission lines. Thus, the energy load increase of a load bus will increase the power flow of some transmission lines. If the power flow on a transmission line exceeds the capacity, protective mechanism will be triggered and trip the transmission line to prevent further damage. However, the topology change may cause cascading impact. Take the 5-bus system depicted in Figure 6 as an example. Suppose that the transmission line 7 is tripped due to over loading. The original load of transmission line 7 is distributed to other transmission lines. This could cause other transmission lines overloaded and tripped. If all transmission lines connected to a bus are tripped, the bus becomes an isolated island and the corresponding community is out of power. The outages on multiple buses lead to the blackout in a large area.

There exists some classical techniques to estimate the transmission line power flows and analyze cascading impact. Without loss of generality, DC power flow equations are deployed in this work [10]. Consider a system with φ buses and ξ transmission lines. At the time slot h, denote by \(G_{i,h}\) and \(P_{i,h}\) the energy generation and load of bus \(i \in \{1, 2, \ldots, \phi\}\). \(G_{i,h}\) is bounded by \(0 \leq G_i \leq G^0_i\) and \(G^0_i = 0\) if the bus \(i\) is not a generation bus. Denote by \(Q\) the power injection from buses, where \(Q = \{Q_{1,h}, Q_{2,h}, \ldots, Q_{\phi,h}\}\). Denote by \(A_0\) the edge-node incidence matrix. \(A_{0,ij} = 1\) if the transmission line \(i\) exits bus \(j\), \(A_{0,ij} = -1\) if the transmission line \(i\) enters bus \(j\) and \(A_{0,ij} = 0\) if the transmission line \(i\) is not connected to bus \(j\). Denote by matrix \(A\) the reduction of \(A_0\) where the column associated with slack bus is removed. For example, the edge-node incidence matrix corresponding to the transmission network depicted in Figure 6 is presented as

\[
A_0 = \begin{bmatrix}
1 & -1 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 \\
0 & 1 & 0 & -1 & 0 \\
0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 1 & -1 \\
0 & 0 & 1 & 0 & -1
\end{bmatrix},
\]
if bus 1 is chosen as the slack bus, it is reduced to

\[
A = \begin{bmatrix}
-1 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 \\
1 & 0 & -1 & 0 \\
0 & 1 & -1 & 0 \\
0 & 0 & 1 & -1 \\
0 & 0 & 0 & -1 \\
\end{bmatrix}. \tag{2}
\]

Denote by \( \Theta = \text{diag}(1/\theta_1, 1/\theta_2, \ldots, 1/\theta_i) \) the line property matrix, where \(1/\theta_i\) is the line susceptance of line \(i\). Denote by \( B = A^T \Theta A \) the bus susceptance matrix. Thus, the DC power flow on each transmission line is calculated as

\[
f = CAB^{-1}Q. \tag{3}
\]

Denote by \( f = \{f_1, f_2, \ldots, f_i\}^T \) the capacity of each transmission line. In order to restrict the power flow, the \( l_1 \) norm of the line loading \( \|f^f\|_1 \) is minimized. Thus, the DC power flow optimization problem is formulated as follows [10]

\[
P1 \text{ minimize } \|f^f\|_1 \\
\text{ subject to } f = CAB^{-1}Q \\
Q = G - P \\
0 \leq G \leq G^0.
\]

At each time slot, the grid operator plans the power flow through solving Problem P1. A hacker can launch a cyberattack targeting increasing the peak energy usage in the community attached to bus \( j \) such that the peak energy load \( P_{j,h} \) is significantly increased during the corresponding time slots. Subsequently, Problem P1 is solved to compute the power flow. For each transmission line \( i \), if the power flow \( f_i > f_i^\ast \), the line \( i \) is tripped such that the corresponding component in matrix \( \Theta \) is updated as zero. As the topology is changed, Problem P1 is solved again to compute the new DC power flow and check violation. If the matrix \( A \) is not full ranked, the grid is broken up [10] and some buses become isolated. Thus, the matrix \( A \) is formulated with the remaining connected buses to compute new power flow. This is repeated until no more transmission line can be tripped.

B. Cascading Outages on System Frequency

There are some existing works on system frequency analysis such as [12], [13]. The frequency analysis in this work is in the same spirit of them. As is discussed in Section II, the cyberattack targeting increasing the energy load fluctuation can change the energy load dramatically. As the generators convert mechanical energy into electrical energy, they adjust the rotation speed of the generation units responding to the change of energy load. If the energy load increases rapidly, the rotor of the generation units decelerate to release the stored kinetic energy to compensate the increasing demand [12]. For each generation unit, the steady state power frequency relation is given as

\[
-R = \frac{\Delta f}{\Delta G}, \tag{4}
\]

where \( R \) is the control constant of the generator, \( \Delta f \) is the normalized change of frequency and \( \Delta G \) is the normalized change of generation load. \( \Delta G \) is calculated as \( \Delta G = \frac{\delta G}{G^0} \) where \( \delta G \) is the change of generation load in MW and \( G^0 \) is the capacity of the generator. The system frequency can be finally recovered to the standard value through the control mechanisms such as LFC. However, a significant change of energy load may impact the system frequency dramatically, which can damage the frequency, degrade the load performance and cause the transmission lines to be overloaded [20]. Thus, the LFC is not able to control the frequency and a sequence of protective procedures will be triggered, such as tripping the generator and separate it from the system [13].

Refer to Figure 6. Suppose that the generator connected to bus 3 is tripped due to the dramatic frequency change. The total demand of the power grid is only supplied by the generator connected to bus 1 and the power flow need to be re-calculated. This can cause cascading impact in two aspects as follows.

- The redistribution of power flow causes some transmission lines overloaded and tripped, which causes cascading outages and separate the bused into isolated islands. This induces blackout to the large area.
- The remaining generator need to increase the energy generation to meet the increasing demand, which leads to the dramatic change of frequency. If the frequency change is significant, the remaining generator is also tripped, which induces blackout to the whole area.

Similar to computing power flow, the grid operator need to solve Problem P1 to determine the generation of each generator. The hacker can launch a cyberattack targeting increasing energy load fluctuation in the community attached to a generation bus. Thus, the corresponding generator is tripped due to the dramatic frequency change. Subsequently, Problem P1 is solved again to determine the new generation and power flow. Denote by \( \Delta f_j \) the frequency change of generator connected to bus \( j \). The generator \( j \) is tripped if \( \Delta f_j > \delta f \), where \( \delta f \) is the threshold to trigger the protective mechanism. If \( j \) is a load bus, \( \Delta f_j = 0 \). If the capacity of a transmission line is exceeded, it is tripped as well. This is repeated until no further change can be made in the power grid.

IV. Hierarchical Framework for Pricing Cyberattack Detection

The detection techniques for pricing cyberattacks has been studied in the previous work [1]. However, the conventional partially observable Markov decision process (POMDP) based detection technique in [1] is computational expensive due to the limitation of scalability [17] despite the effectiveness. In contrast, this paper tackles this difficulty through formulating the POMDP models in a hierarchical fashion. As depicted in Figure 3, the community is divided into sub-communities. In each sub-community, a POMDP model is used to compute the expected costs for ignoring or checking the cyberattack. Based on that, the data center of the community makes a centralized decision on whether to check and repair the smart meters in each sub-community. This can significantly reduce the complexity.

A. POMDP model for cyberattack detection

POMDP is an advanced control theoretical technique, which takes the real world states as the input and generate the optimal actions as the output. Since the system state is usually not able to be obtained directly, the decision maker (e.g., the local data
global policy optimization

A POMDP problem is presented in the form $(S, A, T, R, \Omega, O)$, in which system state $S$, observation $O$ and action $A$ are the three key components [21]. In our problem, a state can represent which smart meters are hacked in a sub-community. Suppose that the community is divided into $K$ sub-communities where there are $V_k$ customers in sub-community $1 \leq k \leq K$. For each customer $i$ in sub-community $k$, a sub-state $\omega_i$ is defined such that $\omega_i = 1$ means the smart meter of customer $i$ is hacked. Otherwise, $\omega_i = 0$. The state of sub-community is $s = [\omega_1, \omega_2, \ldots, \omega_{V_k}]$. $s = s_j$ if $j$ is the value of the binary number $\omega_1 \omega_2 \ldots \omega_{V_k}$. The number of hacked smart meters in sub-community $k$ is denoted by $s(k)$, which is calculated by $s(k) = |s_j| = \sum_{i=1}^{V_k} \omega_i$. The observation $o$ is defined as $o = [\mu_1, \mu_2, \ldots, \mu_{V_k}]$, where $\mu_i = 1$ if the smart meter of customer $i$ is hacked according to the observation. Otherwise, $\mu_i = 0$. $o = o_j$ if $j$ is the value of the binary number $\mu_1 \mu_2 \ldots \mu_{V_k}$. Similar to $s(k)$, the observed number of hacked smart meters is denoted by $o(k) = \sum_{i=1}^{V_k} \mu_i$. There are two available actions $A = \{a_0, a_1\}$, in which $a_0$ means ignoring the cyberattacks and taking no action while action $a_1$ means checking with human interaction for cyberattacks and fix the smart meters in the sub-community.

Since the electricity price tends to be similar in short term, the observation in the POMDP model is obtained as follows. Support vector regression (SVR) [22] is employed to predict the guideline price from historical data. Subsequently, the predicted guideline price is compared with the received guideline price based on their impacts on the energy load [1]. The cyberattack is reported if the difference is above the predefined threshold. As mentioned before, an electricity pricing manipulation cyberattack can increase the peak and fluctuation of the energy load. Thus, once receiving the guideline price, the smart meter conducts smart home scheduling simulation with it. It computes the increase of peak energy load $I_p$ and increase of energy load fluctuation $I_f$ comparing with that corresponding to the predicted guideline price. We define the thresholds $\delta_p$ and $\delta_f$ such that the smart meter $i$ identifies itself to be hacked i.e., $\mu_i = 1$ if $I_p > \delta_p$ or $I_f > \delta_f$. Otherwise, $\mu_i = 0$.

In POMDP, each action taken by the decision maker causes the change of the state subject to the probabilistic transition function denoted by $T$. Given action $a$, the state transits from $s$ to $s'$ with probability $T(s', a, s)$. In our model, the state transition given action $a_0$ only depends on the hacker. For example, $T(s_1, a_0, s_0)$ is the probability that the hacker attacks a previously un_hacked smart meter. The model training technique developed in the previous work [1] is used to derive $T(s_i, a_0, s_j)$. If the action is $a_1$, the state is reset to $s_0$ and the state transition function corresponding to $a_1$ is defined as

$$T(s_j, a_1, s_i) = \begin{cases} 1, & \text{if } s_j = s_0 \\ 0, & \text{otherwise} \end{cases}.$$  \hspace{1cm} (5)

Since an action taken by the decision maker leads to the transitions of state, it also returns a new observation. The observation function $\Omega$ denotes the mapping between the state and observation. Given an action $a$, the observation function $\Omega(o, a, s)$ is the probability that the real world state is $s$ while the observation is $o$. In our model, the observation function corresponding to action $a_0$ depends on the accuracy of the detection technique. While action $a_1$ is taken, the smart meters are checked and observed cyberattacks are eliminated. Thus, $\Omega_0$ is the only possible observation. Therefore, the observation function corresponding to the action $a_1$ is defined as

$$\Omega(o_j, a_1, s_i) = \begin{cases} 1, & \text{if } o_j = o_0 \\ 0, & \text{otherwise} \end{cases}.$$  \hspace{1cm} (6)

The cyberattacks on the smart meters can induce a loss to the system. On the other hand, repairing a hacked smart meter is also associated with labor cost. They are modeled by the reward function $R$ in the POMDP model formulation. Denote by $C^a$ and $C^b$ the loss of the system due to the cyberattack on a smart meter and the labor cost to fix a hacked smart meter. Suppose that the state transits from $s$ to $s'$ while taking action $a$. The decision maker can receive a reward denoted by $R(s', a, s)$. The reward functions corresponding to action $a_0$ and $a_1$ are defined as follows.
Due to the uncertainty of observation, the POMDP estimates the state using belief state \( b = b(s_0), b(s_1), \ldots \) where \( b(s) \) is the probability that the current state is \( s \). Given the last action \( a \) and current observation \( o \), the belief state is computed by [21]

\[
b'(s') = \frac{\Omega(a, s', o) \sum_{s \in S} T(s, a, s') b(s)}{P(o|a, b)}.
\]  

(8)

In the typical POMDP problem, the decision maker computes the optimal action that maximizes the long term expected reward, which is defined as \( E[\sum_{t=0}^{\infty} r_t] \). \( r_t \) is the reward achieved by the decision maker at step \( t \) and a discount factor \( \gamma \) is introduced to reduce the importance of future events in the optimization target. The optimization of expected reward can be written as the Bellman equation \( V^*(b) = \max_{a \in A} \{ \sum_{s \in S} b(s) \sum_{s' \in S} R(s', a, s) + \gamma \sum_{b' \in B} \tau(b', a, b) V^*(b') \} \) [21], where \( \tau(b', a, b) \) is the transition probability of belief state, which is computed by \( \tau(b, a, b') = P(b'|a, b) = \sum_{o \in O} P(b'|a, b, o) P(o|a, b) \).

In the distributed formulation of the hierarchical detection framework, denoted by \( b_k \) the belief state of sub-community \( k \). Thus, the POMDP model of each sub-community \( k \) computes the expected reward corresponding to each action \( C_{b_k, a_0} \) and \( C_{b_k, a_1} \), respectively, such that

\[
C_{b_k, a_i} = \max_{a=0, 1} \sum_{s \in S} b(s) \sum_{s' \in S} R(s', a, s) + \gamma \sum_{b' \in B} \tau(b', a, b) V^*(b')
\]  

(9)

Based on these expected rewards, the community data center makes a global decision using the global policy optimization algorithm.

B. Global Policy Optimization

Based on the optimal reward corresponding to each action of the sub-communities, \( C_{b_k, a_0} \) and \( C_{b_k, a_1} \), the utility computes the optimal action taking on each smart meter based on the rules as follows.

- Since the cyberattack can cause the cascading impact to the power system when the scale is sufficiently large, the utility needs to fix the hacked smart meters only if the expected system loss due to cyberattack is significant enough.
- Note that checking the smart meters is associated with human interaction. The utility needs to pay for the labor cost for checking whether smart meters are hacked or not. Thus, the utility needs to take into account the checking cost while computing the optimal actions.

Based on these rules, the global policy optimization method is proposed to compute the action. If action \( a_1 \) is taken in a sub-community \( k \), only the smart meters with \( \mu_1 = 1 \) are checked and repaired. Denote by \( F \) the set of sub-communities to be checked and \( C^L \) the labor cost to check a smart meter. Thus, it costs the utility \( \sum_{k \in F} o(k) \cdot C^L \) to check the smart meters. For each sub-community \( i \in F \), the benefit for taking action \( a_1 \) is \( C_{b_i, a_1} - C_{b_i, a_0} \). The decision maker aims to choose the set \( F \) such that the difference between total benefit and checking cost is maximized, which is presented by the optimization problem

\[
P_2 \max \sum_{k \in F} \left[ C_{b_k, a_1} - C_{b_k, a_0} \right] - \sum_{k \in F} o(k) \cdot C^L.
\]

A threshold \( \eta \) is defined such that the utility checks and fixes the smart meters of the sub-communities in set \( F \) when

\[
\sum_{k \in F} \left[ C_{b_k, a_1} - C_{b_k, a_0} \right] - \sum_{k \in F} o(k) \cdot C^L > \eta.
\]

The threshold is set based on the need of accuracy. Considering both the decentralized POMDP modeling and the global policy optimization, the complete algorithmic flow for the hierarchical detection framework is presented in Algorithm 1.

Algorithm 1 Hierarchical Framework for Cyberattack Detection.

Input: Observation \( o_k \) and last action \( a \).
\( F = \emptyset \).

for Each sub-community \( k \) do

Update belief state \( b_k \) according to Eqn. (8).

Compute \( C_{b_k, a_0} \) and \( C_{b_k, a_1} \) according to Eqn. (9).

if \( C_{b_k, a_1} - C_{b_k, a_0} > C^L \cdot o(k) \) then

\( F = F \cup \{k\} \).

end if

end for

if \( \sum_{k \in F} \left[ C_{b_k, a_1} - C_{b_k, a_0} \right] - \sum_{k \in F} o(k) \cdot C^L > \eta \) then

Apply \( a_1 \) to the sub-communities in \( F \) and \( a_0 \) to other sub-communities.

else

Apply \( a_0 \) to all the sub-communities.

end if

Suppose that we consider \( t \) steps forward. Thus, in each step, the computational cost is \( 2N^2 \) since all the transition probabilities need to be visited to compute the instant reward \( \sum_{s \in S} b(s) \sum_{s' \in S} R(s', a, s) \) and next belief state \( b' \). We need to compute these two parameters \( A + A^2 + \ldots + A^t \) times. Thus, the computational complexity of the standard POMDP formulation is \( O(A^t N^2) \). In the hierarchical formulation of POMDP, suppose the community is divided into \( \frac{M}{N} \) sub-communities while there are \( M \) customers in each sub-community. Thus, in each sub-community, there are \( L \) states. The complexity is \( O(\frac{M}{N} A^L L^2) \). In the hierarchical formulation, the number of states is significantly reduced such that \( L \ll N \). For a POMDP problem with 1000 states, if we choose \( M = 5 \), the computational complexity can be reduced by 99.36%.

V. Simulations

Simulations are conducted using MATLAB to analyze the impact of cyberattacks to the power grid and the performance of the proposed detection framework. In the simulation setup, the 5-bus test case shown in Figure 6 [23] and IEEE 30-bus test case [24] are considered where each bus is connected to a community consisting of 1000 customers. Without loss of generality, for each generator in the test cases, \( R = 0.05 \) [12]. For the 5-bus test case, the generation capacity of each generator is 6 MW. For the 30-bus test cases, the generation capacity of each generator is 30 MW. For each customer, the average daily energy consumption created by manually controlled home appliances is created similar to the previous works [1], [18]. The daily energy consumptions are shown in Table 1, which are similar to the previous works [1], [18]. In the smart home scheduling, the smart controller of each customer schedules the energy consumption next 24 hours. The quadratic pricing model in [18] is deployed while electricity price is updated each hour.
The guideline price and average energy load without cyberattack are shown in Figure 4(a) and Figure 4(d), respectively. Refer to Figure 4(d), the average energy load of each customer is balanced by the smart home scheduling technique such that the peak to average ratio (PAR) is 1.2240.

### A. Cascading Impact Analysis for Cyberattack Targeting Increasing Peak Energy Usage

In this simulation, the cyberattacks targeting increasing peak energy usage is studied. The manipulated guideline price and energy load are shown in Figure 4(b) and Figure 4(e). Comparing with Figure 4 (a) and (d), the following observations can be obtained. As shown in Figure 4(b), the guideline price is very low from 7:00 pm to 8:00 pm. The corresponding average energy load for each customer is shown in Figure 4(e). The energy load is increased significantly from 7:00 pm to 8:00 pm such that the PAR is 1.7880, which is increased by \( \frac{1.7880 - 1.2240}{1.2240} = 46.08\% \). The maximum energy load fluctuation is 0.99, which is increased by \( \frac{0.99 - 0.56}{0.56} = 76.79\% \).

In order to analyze the cascading impact of the cyberattack targeting increasing peak energy usage, such a cyberattack is launched on 5-bus and 30-bus testcases, respectively. Shown in Figure 5 are the simulation results for 5-bus testcase. The cyberattack cannot cause cascading impact to the large area if it is launched on bus 1 and bus 3 since they are directly supplied by the generators. In contrast, the cyberattack launched on the other buses can cause the transmission lines being tripped such that bus 2, 4 and 5 are out of power.

In order to illustrate the procedure of cascading impact, an example is given in Figure 6 (a) and (b). A cyberattack is launched on bus 4, which causes line 2, 3, 4, 5 and 7 being tripped due to overloading. Since the topology of the transmission system is being changed, power flow is reallocated and bus 2 is only supplied by line 1. Thus, line 1 is also tripped due to overloading. Such a cyberattack causes bus 2, 4 and 5 out of power.

Likewise, the cyberattack targeting increasing peak energy load is launched on each bus in the 30-bus system. The results are shown in Figure 5 (c) and (d). As shown in Figure 5(c), when the cyberattack is applied on bus 1 or 2, there is no bus out of power since they are the generation buses. If the cyberattack is applied on bus 3, only one bus will be out of power. However, if the cyberattack is launched on the buses from bus 4 to bus 30, all the buses will be out of power except the generation buses. As shown in Figure 5(d), when the cyberattack is applied on different buses, different number of lines are tripped while most of them can lead to cascading impact and induce blackout to the large area.

### B. Cascading Impact Analysis for Cyberattack Targeting Increasing Energy Load Fluctuation

In this simulation, the cyberattacks targeting increasing the energy load fluctuation is studied. Shown in Figure 4(c) and (f) are the manipulated guideline price and resulting energy load profile. As shown in Figure 4(c), the guideline price is manipulated such that it is very low from 7:00 am to 9:00 am. Correspondingly, the energy load increases suddenly at 7:00 am as shown in Figure 4(f). The increasing is 1.328kWh per customer on average.

The cascading impact of the cyberattack targeting increasing the energy load fluctuation is analyzed using the 5-bus testcase. The cyberattack is launched on bus 3. According to the result of the DC power flow analysis and Eqn. (4), from 6:00 am to 7:00 am, the frequency change of generator 3 is 1.25%. Thus, generator 3 is tripped according to [13] and the total demand of the system is supplied by generator 1. The power flow of is recalculated. According to the DC power flow results, line 1, 3, 4 and 5 are tripped due to overloading. Refer to Figure 7 for the cascading impact procedure.

### C. Detection Framework

The performance of POMDP based hierarchical detection framework is analyzed in this simulation. The parameters in our POMDP model are set as shown in Table II. In order to demonstrate the advantages of our proposed method, it is compared with three other set of simulation results. The first one is the POMDP based method proposed in the previous work [1]. Due to the scalability issue, that method runs out of memory in the 1000 customer testcase. To use it in our comparison, it is modify as follows. Each two adjacent smart meters are grouped as a “super smart meter”, which is defined to be hacked if at least one of them is hacked. The second one is the heuristic method, which is repeatedly applying the single event detection technique developed in the previous work [1]. In the third set of simulation, no detection is employed.

The simulation is executed in 48 time slots. The observation accuracies at each time slot are shown in Figure 8. Denote by \( N_a \) the total number of hacked smart meters, among which \( N^F_a \) are included in the set \( F \). The detection accuracy is defined as \( 1 - \frac{N_a - N^F_a}{N_a} \). As is observed from Figure 8, the detection accuracy of our proposed POMDP based hierarchical detection technique is 98.34% on average while those of the POMDP based method in [1] is 50.67% on average and heuristic method is 69.91% on average.

The PAR, largest energy load fluctuation and labor cost are shown in Table III. The largest energy load fluctuation and labor cost are normalized. The following observations can be obtained from the simulation results.

- Compared with the results without detection, the PAR is reduced by \( \frac{1.691 - 1.2330}{1.691} = 25.23\% \) and the largest energy

---

**TABLE I**

**DAILY ENERGY CONSUMPTION AND OF AUTOMATICALLY CONTROLLED HOME APPLIANCES [1], [18]**

<table>
<thead>
<tr>
<th>Home Appliance</th>
<th>Daily Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washing Machine</td>
<td>1.2kWh-2kWh</td>
</tr>
<tr>
<td>Dish Washer</td>
<td>1.2kWh-2kWh</td>
</tr>
<tr>
<td>Cloth Dryer</td>
<td>1.5kWh-3kWh</td>
</tr>
<tr>
<td>Electric Vehicle</td>
<td>9kWh-12kWh</td>
</tr>
<tr>
<td>Air Conditioner</td>
<td>2kWh-3kWh</td>
</tr>
<tr>
<td>Heater</td>
<td>2kWh-3kWh</td>
</tr>
</tbody>
</table>

**TABLE II**

**PARAMETERS USED IN SIMULATIONS. ** \( C^0 \) ** IS THE SYSTEM LOSS FOR THE CYBERATTACK ON EACH SMART METER. \( C^F_a \) ** IS THE LABOR COST FOR FIXING A HACKED SMART METER. \( \eta \) ** IS THE THRESHOLD FOR CHECKING AND REPAIRING THE SMART METER. \( C^C \) ** IS THE LABOR COSTS FOR CHECKING A SMART METER. \( \gamma \) ** IS THE DISCOUNT FACTOR IN THE POMDP MODEL.**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>( C^0 )</th>
<th>( C^F )</th>
<th>( \eta )</th>
<th>( C^C )</th>
<th>( \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Value</td>
<td>$30</td>
<td>$30</td>
<td>$8000</td>
<td>$27.5</td>
<td>0.9</td>
</tr>
</tbody>
</table>

---

1551-3203 (c) 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2016.2591911, IEEE Transactions on Industrial Informatics

Fig. 4. (a) Guideline Electricity Price without Cyberattack. (b) Guideline Electricity Price under Peak Energy Load Cyberattack. (c) Guideline Electricity Price under Frequency Attack. (d) Average Energy Load without Cyberattack, PAR=1.2240, Maximum Fluctuation 0.56. (e) Average Energy Load under Peak Energy Load Cyberattack, PAR=1.7880, Maximum Fluctuation 0.99. (f) Average Energy Load under Frequency Attack, PAR=1.3596, Maximum Fluctuation 1.328.

Fig. 5. Cascading impact due to transmission line overloading. (a) Number of buses out of power when different buses are hacked for 5-bus testcase. (b) Number of tripped lines when different buses are hacked for 5-bus testcase. (c) Number of buses out of power when different buses are hacked for 30-bus testcase. (d) Number of tripped lines when different buses are hacked for 30-bus testcase.

Load fluctuation is reduced by $\frac{1-0.3516}{1} = 64.84\%$ using the proposed POMDP based hierarchical detection framework.

- Compared with the heuristic method, our proposed POMDP based hierarchical detection framework can reduce the PAR by $\frac{1.3491-1.2330}{1.3491} = 8.61\%$ and reduce the largest energy load fluctuation by $\frac{0.5367-0.3516}{0.5367} = 34.49\%$. Since our proposed POMDP based hierarchical detection framework can detect and fix more hacked smart meters, the corresponding labor cost is increased by $\frac{1.0362-1}{1} = 3.62\%$ than the heuristic method.

- The conventional POMDP based method in [1] runs out of memory for our testcase. Comparing with the POMDP based method by grouping the smart meters, our proposed POMDP based hierarchical detection framework can reduce the PAR by $\frac{1.2674-1.2330}{1.2674} = 2.71\%$ and reduce the largest energy load fluctuation by $\frac{0.4038-0.3516}{0.4038} = 13.14\%$. The labor cost is reduced by $\frac{2.1262-1.0362}{2.1262} = 51.27\%$.

Note that the hacked smart meters need to be checked manually, which may involve delay such that the hacked smart meters cannot be fixed in all. The impact of manually delay is evaluated by considering maximum number of smart meter that can be fixed per time slot. We set the upper bound of smart meters can be fixed per time slot from 400 to 900. The peak to average ratio and maximum fluctuation of energy load are shown in Table IV. It can be observed from this table that when the maximum number of smart meter can be fixed per time slot increases from 400 to 900, the peak to average ratio of energy load are 1.4941, 1.4485, 1.4049, 1.3582, 1.3143 and 1.2331, respectively. Similarly, the normalized largest fluctuation are 0.7732, 0.7193, 0.6690, 0.6156, 0.5672 and 0.4718, respectively.

VI. CONCLUSION

In this paper, two types of cyberattacks are studied, which can increase the peak energy usage and energy load fluctuation, respectively, in the smart home context. It is demonstrated that the cyberattacks in a local community are able to impact a larger area power grid. These cyberattacks can induce cascading outages through increasing the peak energy load and disturbing
the frequency, respectively, which are analyzed in this work. Furthermore, the hierarchical detection framework is proposed based on partially observable Markov decision process to detect and eliminate the cyberattacks. The simulation results demonstrate that our proposed method can detect over 98% of the cyberattacks and prevent the cascading outages induced from the cyberattacks.

VII. ACKNOWLEDGEMENT

Professor Albert Y. Zomaya’s work was supported by funding from the Faculty of Engineering & Information Technologies, The University of Sydney, under the Faculty Research Cluster Program.

Fig. 6. Cascading impact of cyberattack targeting at increasing peak energy usage on 5-bus testcase, (a) A cyberattack targeting at increasing peak energy usage is launched on bus 4. (b) Lines 2, 3, 4, 5 and 7 are tripped simultaneously due to overloading. (c) Line 1 is tripped due to overloading. Buses 2, 4 and 5 are out of power.

Fig. 7. Cascading impact of cyberattack targeting at increasing energy load fluctuation on 5-bus testcase, (a) A cyberattack targeting at increasing energy load fluctuation is launched on bus 3. (b) Generator 3 is tripped due to frequency change. (c) Lines 1, 3, 4 and 5 are tripped due to overloading. Buses 2, 3, 4 and 5 out of power.

| TABLE III |
| Peak to average ratio of energy load, normalized largest fluctuation and normalized labor cost for different detection techniques. |
| No Detection | The Heuristic Method | POMDP Based Method in [1] | Hierarchical POMDP Based Method |
| PAR           | 1.6491               | 1.3491                       | 1.2674                          | 1.2330                          |
| Normalized Largest Fluctuation | 1 | 0.5367 | 0.4048 | 0.3516 |
| Normalized Labor Cost | - | 1 | 2.1262 | 1.0362 |

| TABLE IV |
| Peak to average ratio and of energy load normalized largest fluctuation for different upper bounds of smart meters can be fixed per time slot. |
| Maximum Number of Fixed Smart Meters Per Time Slot | 400 | 500 | 600 | 700 | 800 | 900 |
| PAR                       | 1.4941 | 1.4485 | 1.4049 | 1.3582 | 1.3143 | 1.2331 |
| Normalized Largest Fluctuation | 0.7732 | 0.7193 | 0.6690 | 0.6156 | 0.5672 | 0.4718 |

REFERENCES


Fig. 8. Detection accuracy.

analysis-confirms-coordinated-hack-attack-caused-ukrainian-power-outage/