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/TSG.2017.2705188, IEEE Transactions on Smart Grid

A Risk-based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks

Seyedamirabbas Mousavian, Melike Erol-Kantarci, Lei Wu, Thomas Ortmeyer

***Abstract*—Security of the smart grid is at risk when the vulnerabilities of the Electric Vehicle (EV) infrastructure is not addressed properly. As vehicles are becoming smarter and connected, their risk of being compromised is increasing. On various occasions and venues, hacking into smart or autonomous vehicles have been shown to be possible. For most of the time, a compromised vehicle poses a threat to the driver and other vehicles. On the other hand, when the vehicle is electric, the attack may spread to the power grid infrastructure starting from the electric vehicle supply equipment (EVSE) all the way up to the utility systems. Traditional isolation-based protection schemes do not work well in smart grid since electricity services have availability constraints and few of the components have physical backups. In this paper, we propose a Mixed Integer Linear Programming (MILP) model that jointly optimizes security risk and equipment availability in the interdependent power and electric vehicle infrastructure. We adopt an epidemic attack model to mimic malware propagation. We assume malware spreads during EV charging when an EV is charged from an infected EVSE and then travels and recharges at another EVSE. In addition, it spreads through the communication network of EVSEs. The proposed response model aims to isolate a subset of compromised and likely compromised EVSEs. The response model minimizes the risk of attack propagation while providing a satisfactory level of equipment availability to supply demand. Our analysis shows the theoretical and practical bounds for the proposed response model in smart grid in the face of attacks to the electric vehicle infrastructure.**

***Index Terms*—Electric vehicle, cyber attack, malware propagation, response model, smart grid.**

NOMENCLATURE

Θ: Set of detected compromised EVSEs.
M: Number of detected compromised EVSEs.
x_j: Binary decision variable which equals to 1 if $EVSE_j$ is kept connected to the network, and 0 otherwise.
$U_j(t)$: Random variable which equals to 1 if $EVSE_j$ is compromised at time t, and 0 otherwise.
$U_{ij}(t)$: Random variable which equals to 1 if $EVSE_j$ is compromised by $EVSE_i$ at time t, and 0 otherwise.
V_j: Random variable which equals to 1 if a cyberattack propagates to and compromises $EVSE_j$, and 0 otherwise.
V_{ijk}: Random variable which equals to 1 if a cyberattack propagated from $EVSE_i$ and targeting $EVSE_j$ compromises the kth communication relay between $EVSE_i$ and $EVSE_j$, and 0 otherwise.
$\theta_j(t)$: The probability of an EVSE being compromised.
L_i: Number of EVs charge at $EVSE_i$.
L_{ij}: Number of EVs charge at $EVSE_i$ and move to $EVSE_j$ for recharging.
β: The probability that an attack propagates without being detected.
η: The probability that an attack propagates through a communication relay.
γ: The probability that an attack compromises the EVSE at destination.
D_{ij}: Hop distance between $EVSE_i$ and $EVSE_j$ in the communication network.
Δt: Time duration that a propagation attempt takes.
C_j: Number of EVs that can be charged simultaneously at $EVSE_j$.
ρ: Unsatisfied demand threshold.
ψ: Maximum acceptable risk of demand exceeding the threshold.
W: Maximum threat level of the connected EVSEs.
y_j: Variable that is used to linearize the threat level, which equals to $-ln\big(1-\theta_j(K\Delta t)\big)$ if $EVSE_j$ is kept connected to the network, and 0 otherwise.

I. INTRODUCTION

Electric vehicles can pose significant threats to smart grid if their security vulnerabilities are not addressed properly. The integration of transportation and power systems may leave many open doors for hackers, especially in the interconnected environment, i.e. the electric vehicle infrastructure including electric vehicles (EVs), electric vehicle supply equipments (EVSEs), meters and other roadside infrastructure. In fact, a cyber attack can be launched from any component of the power or electric transportation systems. If the attack is programmed to be spread such as the case with a malware or a worm, then it can propagate further and infect other components, utility computers and servers of the operator [1]. There are more than 17,000 electric power substations in the U.S. and Canada. Each contains a number of electric power devices including electrical relays, power transformers, phase-shifting transformers and capacitor banks. Numerous automation and communication devices are used to measure, monitor, and control these power grid components [2]. Ensuring all are healthy and non-compromised is highly challenging. Adding electric vehicles to the interconnected environment of equipment calls for robust cyber attack response and readiness strategies.

S. Mousavian is with the School of Business, Clarkson University, Potsdam, NY, USA (email: amir@clarkson.edu).

M. Erol-Kantarci is with the School of Electrical Engineering and Computer Science, University of Ottawa, ON, Canada. She was with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA (emails: melike.erolkantarci@uottawa.ca, merolkan@clarkson.edu).

L. Wu and T. Ortmeyer are with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA (emails: lwu@clarkson.edu; tortmeye@clarkson.edu)

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

The recent Risk Management Process (RMP) guideline developed by the Department of Energy (DOE), the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) states that traditional boundary protection techniques are no longer effective in the energy sector [3]. With the integration of Information and Communication Technologies (ICT), attacks have become more permeable. Attackers can penetrate any part of the cyber-physical energy infrastructure and recruit agents which can steer the electrical grid to an unstable state. With the adoption of electric vehicles, transportation is also relying on the availability of the power grid. An outage in the power grid will also incapacitate electric transportation. This becomes a serious concern for electric public safety vehicles as they also rely on the power grid. This interdependency makes the smart grid more attractive for cyber attackers.

This paper proposes a Mixed Integer Linear Programming (MILP) based approach to minimize security risk and maximize availability of power and electric vehicle infrastructure. A preliminary version of this paper has appeared in [4]. However, it does not consider that malware can spread in the EVSE network. Malware spread in the EVSE network makes the power grid more vulnerable since they are connected to protection equipment of the power grid. The previous solution computes the minimal number of EVSEs to be isolated to keep the desired level of service, while protecting the grid from attack propagation. In this paper, we consider that the cyber attacks propagate through two different ways, i.e. through EV charging and the EVSE communication network. During charging, when an EV charges at a compromised EVSE and recharges at another EVSE, this may cause the malware to spread. Accordingly threat levels are computed. A cyber attack can also propagate in the EVSE network where EVSEs communicate with the service providers. The system architecture is illustrated in Fig. 1. We assume EVSEs have wireless connectivity to either small cell or macro cell base station. They access the charging service provider through wireless front end which is connected with the routers at the backhaul. Our objective in this paper is to model such attacks and propose a response model. Our response model jointly addresses the availability and risk. Risk is defined as the product of the magnitude of the potential loss (Consequences) and the probability that the loss will occur (Threat Levels). The consequence of an EVSE being compromised depends on the attacker's objective and malicious plan. A naive attacker may insert malicious software that runs at the background and slows down operation of utility computers whereas an aggressive attacker may aim for severe damages such as controlling generators and randomly shutting them off or controlling the EVSE network and interrupting the power supply to EVs. Since the consequences of the attack may not be identified at the time of detection, we consider the worst-case situation where the attacker aimed for severe damages. Hence, we minimize the threat levels to mitigate the risk of an attack. Experimental results show that implementing our proposed model versus taking no action against threats reduces the probability of attack propagation significantly. In addition, our findings directly translate to the management of the integrated power and EV infrastructure where the trade off between availability and risk is shown.

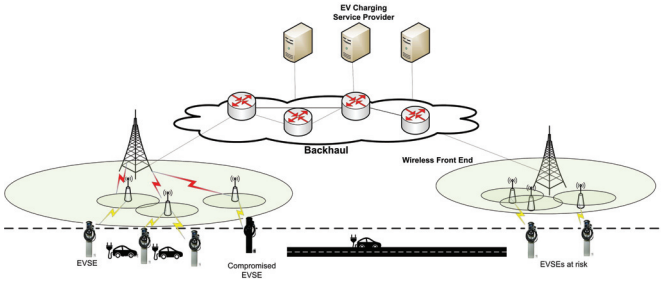


Fig. 1: Overview of system architecture.

There is a wide literature on smart grid security. For instance, in [5], a game theoretic approach has been utilized to protect the power grid from cyberattacks. Reliable strategies have been defined in terms of a budget allocation problem and solved for single and double attack scenarios. In [6], the authors have proposed a bilevel mixed integer linear formulation for optimal load shedding values under threats. Meanwhile, [7] has considered power grid vulnerability in cascaded attacks. However, the literature mostly focuses on one-time attacks implemented on the power grid. In this paper, we address infectious cyberattacks that initiate from EVs and spread into EVSE network as well as the power grid.

The paper is organized as follows. In Section II, we present the state-of-the-art risk mitigation approaches for infectious cyber attacks. In Section III, the cyber attack propagation model is described. Section IV presents the proposed optimization response model. The performance of the model is examined in Section V. Discussions and future research are discussed in Section VI and the conclusions are reported in Section VII.

II. Related Work

There is a large literature on smart grid security and EV infrastructure security. However, fewer works study the security vulnerabilities that rise from their interdependency. In [1], the authors have identified that malware infections can impact upstream equipment in the smart grid, which includes EVSEs, circuit breakers, transformers, PMUs, utility computers and so on. The authors have proposed security certificates as a possible solution. Security certificates are practical but they can be stolen via a trojan software. In turn, malicious users can sign malware as legitimate software and compromise the system. In [8], [9], the authors show how conventionally secure challenge-response schemes can be defeated by attackers. Similarly, authentication and jamming types of attacks have been explored in [10]. Besides Denial of Service (DoS), switching and unauthorized access attacks, load and supply alteration and false data alteration attacks have also been considered in the literature [11]–[17].

Besides modeling the cyberattack propagation, it is also important to develop a response model to mitigate or at least slow down attacks. Probabilistic response models have been

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

widely studied in the literature [4], [18]–[21]. Recently, multi-level optimization has been employed as a protection model where a tri-level defender-attacker-defender model has been proposed and solved by decomposing the original problem to bi-level problems [24]. The recent research in cyber security of power systems deals with attack resilience. [29] considers a proactive protection approach by linking contingency analysis to attack analysis. In our previous work [4], which forms the basis of this paper, we proposed an attack model that considers propagation only through charging. Based on that, the response model aims to minimize the number of EVSEs to be isolated. In the current paper, we extend the attack model to include malware spread due to communications within the EVSE network. We also extend the response model to jointly address risk and availability.

III. Attack Model

In this section, we estimate the threat levels of the EVSEs when one or more EVSEs are detected as compromised. We assume a cyber-attack propagates in the EVSE network in two ways, $i)$ through EVs charging at different EVSEs and spreading the attack from one EVSE to another before detection of the cyber-attack (Type-I), and $ii)$ through the EVSE's shared communication network after detection of the cyber-attack (Type-II). Type-I attacks initiate from an EV and spread to other EVs. Some examples are: malware downloaded as a software patch from an unreliable source, or a compromised mobile application that interacts with the EV and downloads a malware. Type-II attacks initiate either from EVs or EVSEs, and they spread from one EVSE to the other. An example scenario comes from a network of charging stations that share usage data with each other to improve operator's service. In a sophisticated attack, a compromised EVSEs can act like the operator side and send software updates that are actually malware. This type of attack obviously requires more sophistication but it is more effective in terms of compromising the infrastructure.

There are several scenarios to deal with compromised EVSEs. If an EVSE is detected as compromised, then it will be taken out of service temporarily until further inspection and recovery. Recovery is usually done by remotely uploading patches from a trusted source. Even if the compromised EVSEs are isolated, other EVSEs can still be compromised due to interactions with already infected EVs. Another reason for this post-discovery malware spread is that cyber-attacks such as viruses and worms sometimes do not activate until they become sufficiently widespread. Newly compromised, but not detected, EVSEs continue to further infect the other EVSEs through the communication network. If the attack propagates to more EVSEs, it could jeopardize the supply of power to EVs. The goal of our response model, described in the next section, is to avoid such situations. We first start with formulating the attack propagation model. The summary of notations used throughout this paper is given in the nomenclature in the beginning of the paper.

Let us assume that at time $t = 0$, M EVSEs are detected to be compromised while the remaining EVSEs are likely to be compromised but not detected. We represent the likelihood of an EVSE being compromised (also called threat level) at time t by the probability $\theta_j(t)$. We assume that the threat level of EVSE j at time $t = 0$, $\theta_j(0)$, is proportional to the number of EVs moved from detected compromised EVSEs to EVSE j. Accordingly, the initial threat levels of EVSEs are estimated as follows.

$$\begin{aligned}
\theta_j(0) &= 1 && \forall j \in \Theta \quad (1)\\
\theta_j(0) &= \Pr(U_j(0) = 1)\\
&= 1 - \Pr(U_j(0) = 0)\\
&= 1 - \prod_{i\in\Theta, i\neq j} \Pr(U_{ij}(0) = 0)\\
&= 1 - \prod_{i\in\Theta, i\neq j} \big(1 - \Pr(U_{ij}(0) = 1)\big)\\
&= 1 - \prod_{i\in\Theta, i\neq j} \big(1 - \beta\frac{L_{ij}}{L_i}\big) && \forall j \notin \Theta \quad (2)
\end{aligned}$$

At the end of the detection horizon, the detected compromised EVSEs will be taken out of service temporarily. However, the attack continues to spread through the communication network as explained before. Let Δt denote the time that a propagation attempt takes in the communication network and $K\Delta t$ denote the inspection period [21]. Equation (3) holds to estimate the threat levels of EVSEs at time $t = \Delta t$.

$$\begin{aligned}
\theta_j(\Delta t) &= \Pr(U_j(\Delta t) = 1)\\
&= \Pr\{U_j(\Delta t) = 1 | U_j(0) = 0)\}\\
&\times \Pr(U_j(0) = 0)\\
&+ \Pr\{U_j(\Delta t) = 1 | U_j(0) = 1)\}\\
&\times \Pr(U_j(0) = 1) && \forall j \notin \Theta \quad (3)
\end{aligned}$$

On the right hand side, the second term, $\Pr(U_j(0) = 0)$, equals to $1 - \theta_j(0)$, the third term, $\Pr\{U_j(\Delta t) = 1 | U_j(0) = 1)\}$, equals to 1 and the last term, $\Pr(U_j(0) = 1)$, equals to $\theta_j(0)$. The first term of the right hand side, $A = \Pr\{U_j(\Delta t) = 1 | U_j(0) = 0)\}$, is calculated as follows.

$$\begin{aligned}
A &= 1 - \Pr\{U_j(\Delta t) = 0 | U_j(0) = 0)\}\\
&= 1 - \prod_{\substack{i\notin\Theta\\ i\neq j}} \Big(\Pr\{U_j(\Delta t) = 0 | U_i(0) = 1)\}\Big)\\
&= 1 - \prod_{\substack{i\notin\Theta\\ i\neq j}} \Big(1 - \alpha_{ij}\theta_i(0)\Big) \quad (4)
\end{aligned}$$

where α_{ij} is the probability that the attack propagates from compromised $EVSE_i$ to an uncompromised $EVSE_j$ during the time period of Δt as given by equation (5). Notice that in equation (4), complementary probabilities are used. To calculate A, we need to calculate $\Pr\{U_j(\Delta t) = 1 | U_i(0) = 1)\}$ which represents the probability that EVSE j becomes compromised given that EVSE i is compromised. Due to the statistical dependency of these random variables ($\forall i \neq j$), we use complementary probabilities instead and calculate $\Pr\{U_j(\Delta t) = 0 | U_i(0) = 1)\}$. This term represents the probability that EVSE j does not become compromised given

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

that EVSE i is compromised. These terms are statistically independent for all $i \neq j$.

$$\begin{aligned} \alpha_{ij} &= \Pr(V_j = 1) \times \prod_{k=1}^{D_{ij}} \Pr\{V_{ijk} = 1\} \\ &= \gamma \times \prod_{k=1}^{D_{ij}} \eta \\ &= \gamma \eta^{D_{ij}} \qquad i, j \notin \Theta \end{aligned} \tag{5}$$

In equation (5), η is the probability that an attack propagates through a communication relay in the communication network and γ is the probability that a transmitted attack successfully compromises the EVSE at the destination. D_{ij} is called hop distance and it is the minimum number of relays that connect $EVSE_i$ and $EVSE_j$. Here, a relay could be a small cell base station or a macro cell base station in the radio access network, or a router in the backhaul, as shown in Fig. 1. By replacing equations (4)-(5) in equation (3), we obtain the threat level of $EVSE_j$ at time $t = \Delta t$, $\theta_j(\Delta t)$, given in equation (6).

$$\theta_j(\Delta t) = 1 - \Big(1 - \theta_j(0)\Big) \prod_{\substack{i \notin \Theta \\ i \neq j}} (1 - \alpha_{ij}\theta_i(0)) \quad \forall j \notin \Theta \tag{6}$$

The threat levels increase over time until full recovery of the network. Hence, the general threat level formula is obtained in a similar fashion as equation (6) and provided in equation (7).

$$\begin{aligned} \theta_j(0) = 1 \quad &- \quad \prod_{\substack{i \in \Theta \\ i \neq j}} \big(1 - \beta \frac{L_{ij}}{L_i}\big) \\ \theta_j(n\Delta t) = 1 \quad &- \quad \Big(1 - \theta_j((n-1)\Delta t)\Big) \\ &\times \quad \Big(\prod_{\substack{i \notin \Theta \\ i \neq j}} \big(1 - \theta_i((n-1)\Delta t) \times \alpha_{ij}\big)\Big) \end{aligned}$$
$$\forall j \notin \Theta; 1 \leq n \leq K \tag{7}$$

The formulated attack model and threat levels are used in the response model as described in the next section.

IV. Risk-based Response Optimization Model

When a cyber-attack takes place in the EVSEs network, the usual practice would be to take the detected compromised EVSEs out of service. In this paper, we propose that the compromised EVSEs as well as those under high risk of being compromised will be taken out of service as long as capacity demand of the EVs can be met. The latter represents EVSEs that are most likely to be compromised and help spread the attack, but are not properly detected. Our approach aims to slow down the propagation pace even further until the network is fully inspected and recovered.

The proposed response approach is formulated as a mixed integer linear programming (MILP) model that determines which EVSEs should be taken out of service such that the maximum threat level of the EVSEs connected to the network by the time of inspection is minimized while the risk of lack of supply is within a certain threshold.

After detection alarm goes off, the system operator needs to spend some time to inspect the network and make sure the alarm was not false, during which the attack is spreading in the communication network. Therefore, the threat levels, calculated by equation (7), need to be modified to consider disconnection of the likely-compromised EVSEs at the end of inspection. After inspection, these EVSEs are no longer connected to the network and cannot propagate the cyber-attack. The remaining connected and likely compromised EVSEs will continue to spread the attack until trusted patches are successfully installed and the network is fully recovered. We use the binary decision variable, x_j, to address the disconnection of the EVSEs in the threat levels formulation. Therefore, we can obtain equation (8).

$$\begin{aligned} \theta_j(0) = 1 \quad &- \quad \prod_{\substack{i \in \Theta \\ i \neq j}} \big(1 - \beta \frac{L_{ij}}{L_i}\big) \\ \theta_j(n\Delta t) = 1 \quad &- \quad \Big(1 - \theta_j((n-1)\Delta t)\Big) \\ &\times \quad \Big(\prod_{\substack{i \notin \Theta \\ i \neq j}} \big(1 - \theta_i((n-1)\Delta t) \times \alpha_{ij} \times x_j\big)\Big) \end{aligned}$$
$$\forall j \notin \Theta; 1 \leq n \leq K \tag{8}$$

Equation (8) is nonlinear for $n \geq 1$. To represent this equation linearly, the equivalent equation (10) is derived as follows using the method described in [21] .

$$\begin{aligned} \ln\Big(1 - \theta_j(n\Delta t)\Big) &= \sum_{\substack{i \notin \Theta \\ i \neq j}} \ln\Big(1 - \theta_i((n-1)\Delta t)\alpha_{ij}x_j\Big) \\ &+ \ln\Big(1 - \theta_j((n-1)\Delta t)\Big) \end{aligned} \tag{9}$$

Notice that $\ln(1 - Nx_j) = x_j \ln(1 - N)$ where N is a constant [21]. Therefore, we can rewrite equation (9) in an equivalent linear fashion given in equation (10).

$$\begin{aligned} \ln\Big(1 - \theta_j(n\Delta t)\Big) &= \sum_{\substack{i \notin \Theta \\ i \neq j}} x_i \ln\Big(1 - \theta_i((n-1)\Delta t)\alpha_{ij}\Big) \\ &+ \ln\Big(1 - \theta_j((n-1)\Delta t)\Big) \end{aligned} \tag{10}$$

The objective function is to minimize the maximum threat level of all connected EVSEs by the time of inspection, $t = K\Delta t$. The objective function is given in equation (11).

$$Z = \min_{\mathbf{x}} \max_{j} (\theta_j(K\Delta t) \times x_j) \qquad \forall j \notin \Theta \tag{11}$$

Clearly, the objective function is nonlinear. To represent the objective function linearly, its equivalent provided in equation (12) can be utilized [21]. This objective function is represented by the linear equations (13)-(18).

$$Z = \min_{\mathbf{x}} \max_{j} \Big(-ln\big(1 - \theta_j(K\Delta t)\big) \times x_j\Big) \qquad \forall j \notin \Theta \tag{12}$$

We define $y_j = -ln\Big(1 - \theta_j(K\Delta t)\Big) \times x_j$ and accordingly $W = \max_j(y_j)$. Therefore, the objective function can be

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

written as equation (13). Moreover, we need constraints, as given in equations (14)-(18), to represent these new definitions in a linear fashion.

$$Z = \min_{\mathbf{x}} W \tag{13}$$

Subject to:

$$y_j \leq x_j \qquad \forall j \notin \Theta \quad (14)$$
$$y_j \leq -ln\big(1-\theta_j(K\Delta t)\big) \qquad \forall j \notin \Theta \quad (15)$$
$$y_j \geq -ln\big(1-\theta_j(K\Delta t)\big) - (1-x_j) \qquad \forall j \notin \Theta \quad (16)$$
$$y_j \geq 0 \qquad \forall j \notin \Theta \quad (17)$$
$$y_j \leq W \qquad \forall j \notin \Theta \quad (18)$$

Notice that the linear equivalent of $-ln\big(1-\theta_j(K\Delta t)\big)$, given in equation (10), replaces it in equations (15)-(16).

The objective function tends to disconnect EVSEs which have positive threat levels. Hence, equation (19) is used to keep the EVSEs with threat levels less than a threshold value of T_j connected to the network. The threshold value depends on how risk taker the power system operators are [21].

$$\theta_j(K\Delta t) > T_j - x_j \qquad \forall j \notin \Theta \quad (19)$$

To represent equation (19) linearly, we follow the next steps, discussed in [21], and utilize equation (10) and obtain equation (23).

$$1-\theta_j(K\Delta t) < 1-T_j+x_j \tag{20}$$
$$\ln(1-\theta_j(K\Delta t)) < \ln(1-T_j+x_j) \tag{21}$$
$$\ln(1-\theta_j(K\Delta t)) < (1-x_j)\ln(1-T_j) + x_j \ln(2-T_j) \tag{22}$$

$$\sum_{\substack{i\notin\Theta \\ i\neq j}} x_i \ln\Big(1-\theta_i((K-1)\Delta t)\alpha_{ij}\Big) + \ln\Big(1-\theta_j((K-1)\Delta t)\Big) < (1-x_j)\ln(1-T_j) + x_j\ln(2-T_j) \tag{23}$$

Disabling EVSEs from the network may affect the power supply to EVs, so there should be constraints to ensure that the risk of unsatisfied demand exceeding a certain threshold value would be statistically controlled, e.g. the risk of unmet demand exceeding 10 EVs should be less than 5%.

$$Pr\Big(D_{EV} - \sum_{j\in\Upsilon} C_j x_j > \rho\Big) \leq \psi \tag{24}$$

where C_j is the number of electric vehicles that can be charged simultaneously at $EVSE_j$. D_{EV} is the forecasted demand for the EV charging stations during the recovery period. As suggested in [22], [23], we assume that demand is uniformly distributed between zero and D_{max}, i.e. $U(0, D_{max})$. Considering the cumulative uniform distribution function of $F(x) = \frac{x}{D_{max}}$, equation (25) can be written as follows.

$$\begin{aligned} &Pr\Big(D_{EV} - \sum_{j\in\Upsilon} C_j x_j > \rho\Big) = \\ &Pr\Big(D_{EV} > \rho + \sum_{j\in\Upsilon} C_j x_j\Big) = \\ &1 - Pr\Big(D_{EV} \leq \rho + \sum_{j\in\Upsilon} C_j x_j\Big) = \\ &1 - \frac{1}{D_{max}}\Big(\rho + \sum_{j\in\Upsilon} C_j x_j\Big) \leq \psi \end{aligned} \tag{25}$$

Equivalently, we can write the supply risk constraint as equation (26):

$$\sum_{j\notin\Theta} C_j x_j \geq D_{max}(1-\psi) - \rho \tag{26}$$

V. Numeric Results

We test the performance of the proposed model on the 5-EVSE and 20-EVSE test systems. We use the small test system to describe the cyber attack propagation problem and our methodology. We use the larger system to test the efficiency of our approach.

In our experiments, we assume that a cyber attack to an EVSE propagates through a relay with probability $\eta = 0.05$, and it effectively compromises the EVSE at destination with probability $\gamma = 0.05$ [21]. We set $\Delta t = 0.5$ (s), $\beta = 0.1$ and the threshold values to 0.05, $T_j = 0.05$. The inspection time is set to 2 minutes.

A. 5-EVSE Test System

The 5-EVSE test system is modeled using the EVSE layout in Potsdam-Canton area of New York where five EVSEs are located at SUNY at Potsdam (P1), Clarkson University (P2), Best Western University Inn (C1), Saint Lawrence University (C2), and SUNY at Canton (C3). Table I shows randomly-generated proportion of EVs moving between EVSEs. This impacts the threat level calculation since the likelihood of being compromised increases for EVs charging at an EVSE, after a compromised EV has charged at the same EVSE. Hop distances in the communication network are also randomly generated and provided in Table II. The greater the hop distance between two EVSEs, the less likely a cyber-attack propagates from one EVSE to another according to the propagation probability.

TABLE I: Proportion of EV Movement between EVSEs

EVSE	P1	P2	C1	C2	C3	Others
P1	0.3	0.2	0.2	0.1	0.15	0.05
P2	0.2	0.1	0.3	0.1	0.1	0.2
C1	0.2	0.3	0.2	0.1	0.1	0.1
C2	0.1	0.1	0.1	0.1	0.3	0.3
C3	0.15	0.1	0.1	0.3	0.2	0.15
Others	0.05	0.2	0.1	0.3	0.15	0.2

In this case study, we assume that EVSEs P1 and C1 are detected as compromised at time $t = 0$. We use equation (2) to calculate initial threat levels of EVSEs P2, C2 and C3 at

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

TABLE II: Hop Distances in the EVSE network

EVSE	P1	P2	C1	C2	C3
P1	—	1	2	1	3
P2	1	—	2	3	1
C1	2	2	—	1	1
C2	1	3	1	—	1
C3	3	1	1	1	—

time $t = 0$, given in equations (27)-(29). Notice that the initial threat level of EVSE P2 is greater since a higher percentage of EVs from compromised EVSEs P1 and C1 was recharged at EVSE P2. Note that EVSEs in Potsdam are tagged by the letter P and the ones in Canton are tagged by the letter C.

$$\theta_{P2}(0) = 0.04940 \quad (27)$$

$$\theta_{C2}(0) = 0.01990 \quad (28)$$

$$\theta_{C3}(0) = 0.02485 \quad (29)$$

At the time of detection, the detected compromised EVSEs are disconnected from the network. However, the other EVSEs are likely to be compromised, with probabilities given in equations (27)-(29), and continue to further infect other EVSEs through the communication network. Figure 2 shows the threat level of EVSEs P2, C2 and C3 over time if no further action is taken. Notice that the threat levels increase nonlinearly and all EVSEs are compromised with probability 1 in less than 30 minutes. The threat level of EVSE C3 increases at a faster pace although its initial threat level is not the greatest. The reason is that its hop distance to the other two likely compromised EVSEs is shorter in the communication network. Figure 3

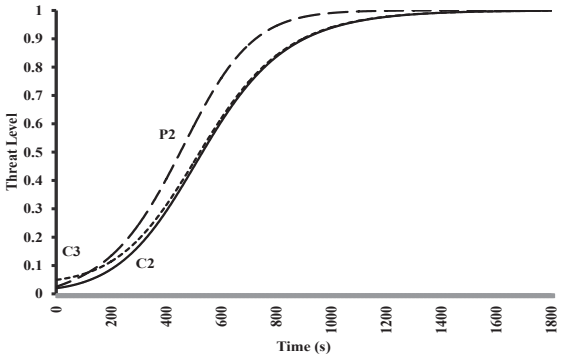


Fig. 2: Threat levels when no action is taken.

shows the impact of β which is the probability that an attack propagates without being detected. We take the threat level for EVSE P2 as an example for illustration. The same trend is observed for all other EVSEs. As shown in Fig. 3, the initial threat levels increase as β increases. Accordingly, the threat levels increase at a faster pace since the initial threat levels are higher.

Figure 4 shows the impact of parameter η which is the probability that an attack propagates through a relay. We again use EVSE P2 as an example. The threat levels increase at a faster pace as η increases since the chance of successful propagation from one relay to another increases. The proposed

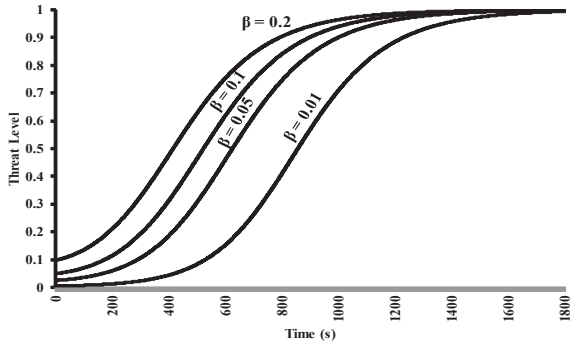


Fig. 3: Impact of parameter β on threat levels

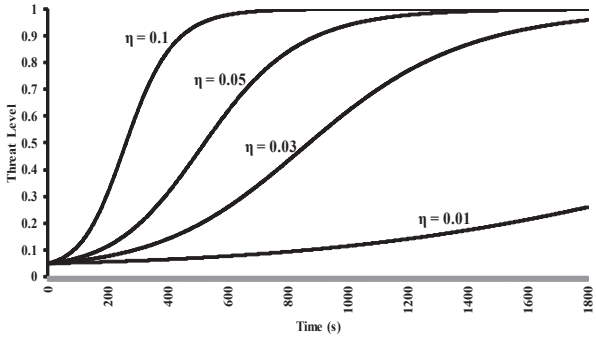


Fig. 4: Impact of parameter η on threat levels

response model suggests that it is beneficial to disconnect a subset of likely-compromised EVSEs at the time of inspection as long as the risk constraint on supply insufficiency is satisfied. Since there are three likely-compromised EVSEs in this case, there are eight potential solutions, as shown in Table III. In this case, we assume that demand is uniformly distributed between 0 and 10, $D_{max} = 10$. Also, the risk of demand exceeding the available capacity by two units is set to be less than 10%, i.e. $\rho = 2$, $\psi = 10\%$. In other words, the available charging capacity should be greater than or equal to 7 based on equation (26).

Table III shows potential solutions in which the last four solutions are infeasible due to the constraint on available capacity. The objective function is to minimize the maximum threat level. Hence, solution 3, disconnecting EVSEs C2 and C3, seems to be the best candidate among the remaining solutions. However, the threat level of EVSE C2 equals to 0.04816 which is less than the threshold value of 0.05. Thus, it should be kept connected to the network based on the threshold value constraint, given in equation (19). The next candidate is solution 4, disconnecting EVSE C3. Solution 4 satisfies all constraints and is the optimal solution. Figure 5 compares the threat levels after implementing our optimal solution and the non-action approach. The threat levels still increase after implementing the optimal solution but at much lower pace.

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

TABLE III: Candidate solution for the 5-EVSEs system

EVSE Status	Candidate Solution 1	2	3	4	5	6	7	8
x_{P2}	1	1	1	1	0	0	0	0
x_{C2}	1	0	0	1	1	0	1	0
x_{C3}	1	1	0	0	1	1	0	0
Threat Levels at t=120 seconds								
θ_{P2}	0.07696	0.07694	0.07675	0.07677	0	0	0	0
θ_{C2}	0.04834	0	0	0.04816	0.04834	0	0.04815	0
θ_{C3}	0.07760	0.07749	0	0	0.07743	0.07732	0	0
Max(θ_j)	0.07696	0.07694	0.07675	0.07677	0.07743	0.07732	0.04815	0
Remaining Capacity	11	10	7	8	4	3	1	0

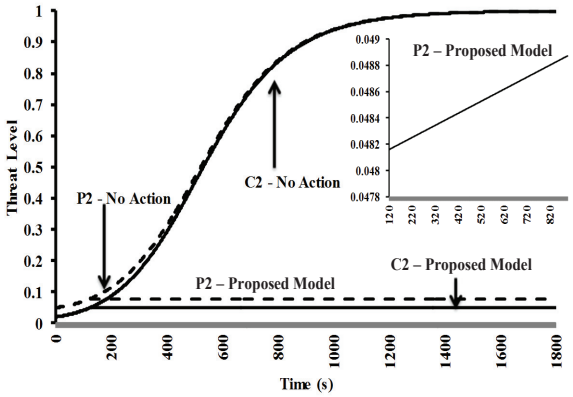


Fig. 5: Impact of implementing the response model on threat levels

TABLE V: Hop Distances

EVSE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	—	5	1	4	2	3	3	1	5	3	1	2	5	3	5	1	5	4	4	4
2	5	—	3	4	1	2	4	5	1	5	4	3	2	4	3	3	4	4	5	4
3	1	3	—	5	4	1	5	2	5	3	2	4	5	2	4	5	5	2	3	3
4	4	4	5	—	4	2	4	1	5	2	2	2	1	1	2	3	1	3	5	1
5	2	1	4	4	—	2	4	3	2	4	5	1	1	4	2	5	4	1	4	4
6	3	2	1	2	2	—	5	4	5	4	1	1	3	1	3	5	2	3	2	2
7	3	4	5	4	4	5	—	4	2	2	2	3	1	3	5	3	1	1	5	5
8	1	5	2	1	3	4	4	—	5	4	3	4	5	3	1	3	3	5	1	3
9	5	1	5	5	2	5	2	5	—	4	1	4	3	1	1	5	1	3	1	1
10	3	5	3	2	4	4	2	4	4	—	5	2	2	3	4	4	4	3	4	5
11	1	4	2	2	5	1	2	3	1	5	—	4	1	4	3	1	5	5	5	5
12	2	3	4	2	1	1	3	4	4	2	4	—	1	4	1	5	2	3	1	5
13	5	2	5	1	1	3	1	5	3	2	1	1	—	4	5	2	1	1	2	4
14	3	4	2	1	4	1	3	3	1	3	4	4	4	—	3	1	1	4	5	3
15	5	3	4	2	2	3	5	1	1	4	3	1	5	3	—	3	3	5	5	3
16	1	3	5	3	5	5	3	3	5	4	1	5	2	1	3	—	1	5	4	2
17	5	4	5	1	4	2	1	3	1	4	5	2	1	1	3	1	—	5	4	3
18	4	4	2	3	1	3	1	5	3	3	5	3	1	4	5	5	5	—	4	3
19	4	5	3	5	4	2	5	1	1	4	5	1	2	5	5	4	4	4	—	2
20	4	4	3	1	4	2	5	3	1	5	5	5	4	3	3	2	3	3	2	—

TABLE VI: EVSEs Capacity

EVSE	Capacity	EVSE	Capacity
1	2	11	3
2	4	12	1
3	3	13	4
4	2	14	1
5	3	15	3
6	1	16	3
7	3	17	2
8	2	18	4
9	4	19	2
10	1	20	2

B. 20-EVSE Test System

The performance of the proposed response model is tested using 20-EVSE test network. The input data, proportion of EV movement between EVSEs, hop distances, and charging capacities are randomly generated and summarized in Table IV, Table V, Table VI, respectively.

We assume that at time $t = 0$ EVSEs 1 and 2, arbitrarily chosen, are detected as compromised and parameter D_{max} is set to 40. Figure 6 shows the threat levels of EVSEs if our proposed response model is not implemented. Notice that the threat level of EVSE 10 is increasing at a slower pace

TABLE IV: Proportion of EV Movement between EVSEs

EVSE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0.07	0.03	0.03	0.07	0.04	0.09	0.05	0.03	0.03	0.04	0.09	0.03	0.03	0.05	0.07	0.05	0.07	0.05	0.01	0.07
2	0.03	0.06	0.05	0.04	0.02	0.05	0.09	0.02	0.04	0.04	0.02	0.04	0.07	0.02	0.07	0.02	0.09	0.09	0.05	0.09
3	0.03	0.05	0.07	0.07	0.04	0.02	0.02	0.04	0.09	0.07	0.06	0.09	0.09	0.02	0.02	0.07	0.03	0.04	0.04	0.04
4	0.07	0.04	0.07	0.06	0.02	0.09	0.04	0.08	0.02	0.01	0.06	0.06	0.06	0.04	0.04	0.04	0.09	0.06	0.04	0.01
5	0.04	0.02	0.04	0.02	0.08	0.01	0.05	0.04	0.05	0.07	0.05	0.07	0.08	0.07	0.02	0.04	0.05	0.05	0.08	0.07
6	0.09	0.05	0.02	0.09	0.01	0.02	0.03	0.08	0.05	0.08	0.05	0.09	0.06	0.06	0.02	0.02	0.08	0.05	0.02	0.03
7	0.05	0.09	0.02	0.04	0.05	0.03	0.07	0.04	0.04	0.05	0.06	0.05	0.02	0.06	0.05	0.07	0.02	0.04	0.05	0.10
8	0.03	0.02	0.04	0.08	0.04	0.08	0.04	0.05	0.03	0.03	0.06	0.05	0.03	0.03	0.06	0.05	0.08	0.09	0.09	0.02
9	0.03	0.04	0.09	0.02	0.05	0.05	0.04	0.03	0.03	0.02	0.03	0.06	0.08	0.06	0.14	0.02	0.08	0.02	0.06	0.05
10	0.04	0.04	0.07	0.01	0.07	0.08	0.05	0.03	0.02	0.08	0.02	0.08	0.06	0.02	0.04	0.03	0.07	0.05	0.02	0.12
11	0.09	0.02	0.06	0.06	0.05	0.05	0.06	0.06	0.03	0.02	0.06	0.05	0.08	0.05	0.02	0.05	0.08	0.02	0.02	0.07
12	0.03	0.04	0.09	0.06	0.07	0.09	0.05	0.05	0.06	0.08	0.05	0.01	0.08	0.05	0.02	0.04	0.08	0.02	0.01	0.02
13	0.03	0.07	0.09	0.06	0.08	0.06	0.02	0.03	0.08	0.06	0.08	0.08	0.01	0.02	0.04	0.06	0.07	0.03	0.02	0.01
14	0.05	0.02	0.02	0.04	0.07	0.06	0.06	0.03	0.06	0.02	0.05	0.05	0.02	0.02	0.10	0.02	0.03	0.10	0.06	0.12
15	0.07	0.07	0.02	0.04	0.02	0.02	0.05	0.06	0.14	0.04	0.02	0.02	0.04	0.10	0.01	0.02	0.03	0.06	0.15	0.02
16	0.05	0.02	0.07	0.04	0.04	0.02	0.07	0.05	0.02	0.03	0.05	0.04	0.06	0.02	0.02	0.07	0.01	0.13	0.15	0.04
17	0.07	0.09	0.03	0.09	0.05	0.08	0.02	0.08	0.08	0.07	0.08	0.08	0.07	0.03	0.03	0.01	0.01	0.01	0.01	0.01
18	0.05	0.09	0.04	0.06	0.05	0.05	0.04	0.09	0.02	0.05	0.02	0.02	0.03	0.10	0.06	0.13	0.01	0.03	0.04	0.02
19	0.01	0.05	0.04	0.04	0.08	0.02	0.05	0.09	0.06	0.02	0.02	0.01	0.02	0.06	0.15	0.15	0.01	0.04	0.02	0.06
20	0.07	0.09	0.04	0.01	0.07	0.03	0.10	0.02	0.05	0.12	0.07	0.02	0.01	0.12	0.02	0.04	0.01	0.02	0.06	0.03
Sum	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

comparing to other EVSEs. The reason is that EVSE 10 has the largest average hop distance and is the only EVSE that does not have a 1-hop distance with the other EVSEs.

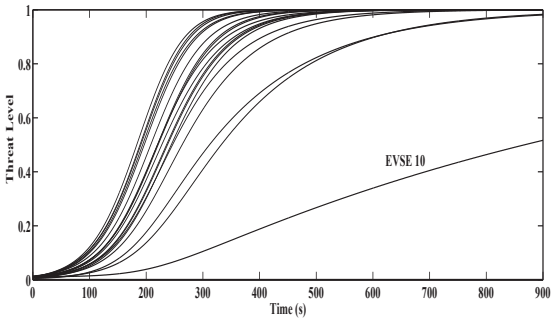


Fig. 6: Threat levels - No Action

We applied our proposed response model and the optimal solution is provided in Table VII.

TABLE VII: Optimal Solution

Disabled EVSE	Objective Function	Available Capacity
1, 2, 9, 13, 17	0.1581	34

Table VIII shows the impact of the risk parameter ψ on optimal solution. The higher the risk of unsatisfied demand, the lower the maximum threat level of connected EVSEs.

TABLE VIII: Trade-off between supply risk and optimal solution

ψ	Disabled EVSEs	Objective Function	Available Capacity
0.10	1, 2, 9, 13, 17	0.1581	34
0.15	1, 2, 4, 9, 13, 17	0.1545	32
0.20	1, 2, 4, 9, 12, 13, 14, 17	0.1312	30
0.25	1, 2, 4, 6, 9, 12, 13, 14, 17	0.1305	29
0.30	1, 2, 4, 9, 11, 12, 13, 14, 17	0.1188	27
0.50	1, 2, 4, 6, 7, 9, 11, 12, 13, 14, 16, 17, 20	0.1008	18

We also examined the impact of inspection time on the objective function value. The results, represented in Figure 7, confirm that earlier response to attack will slow down the propagation more effectively.

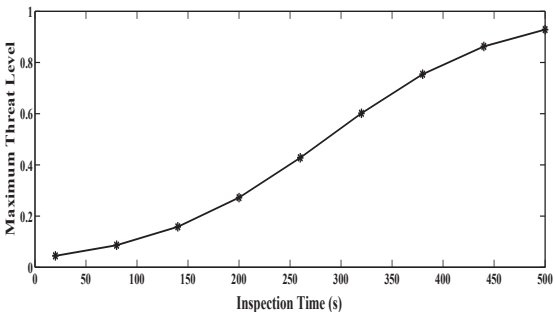


Fig. 7: Impact of inspection time on optimal solution

Furthermore, it is necessary to study how the demand forecast errors affect the trade-off between the objective function value, the maximum threat level of the connected EVSEs, and the risk of unsatisfied demand exceeding the threshold value. The results, summarized in Table IX, show that when the chosen D_{max} parameter is greater than the actual maximum demand, the objective function value could have been improved since more EVSEs could have become disconnected from the network. In contrary, the response model returns a better objective function value at the cost of more unsatisfied demand exceeding the threshold value when the chosen D_{max} parameter is less than the actual maximum demand.

TABLE IX: The impact of demand forecast errors on the objective function value and EVSEs availability

Demand Forecast Error (%)	Objective Function Improvement (%)	Additional Risk of Unsatisfied Demand Exceeding Threshold (%)
25.0%	25.4%	18.0%
22.5%	25.4%	16.5%
20.0%	25.3%	15.0%
17.5%	25.1%	13.4%
15.0%	21.6%	11.7%
12.5%	21.3%	10.0%
10.0%	1.8%	8.2%
7.5%	1.6%	6.3%
5.0%	1.6%	4.3%
2.5%	1.5%	2.2%
0.0%	0.0%	0.0%
-2.5%	0.0%	-2.3%
-5.0%	-0.3%	-4.7%
-7.5%	-2.2%	-7.3%
-10.0%	-16.3%	-10.0%
-12.5%	-17.0%	-10.0%
-15.0%	-17.2%	-10.0%
-17.5%	-17.2%	-10.0%
-20.0%	-24.9%	-10.0%
-22.5%	-24.9%	-10.0%
-25.0%	-24.9%	-10.0%

C. Computational Time Analysis

All experiments were performed on a 64-bit laptop with an Intel Core i5 2.4 GHz processor and 4GB RAM. The computation time consists of two components, the threat level calculation and the optimization solver. We used MATLAB R2012a to calculate the threat levels and IBM ILOG CPLEX Optimization Studio 12.6 as the optimization solver. For the 20-EVSE test system, the threat level calculations took 7.4 seconds and the optimization was done in 2.8 seconds.

The computational time is important when applying the proposed model on larger networks. We have tested the performance of our response model on a larger network with 100 EVSEs and randomly-generated data and studied the computational time. The threat level calculations took 9.2 seconds and the optimization was done in 3.3 seconds. The computational time analysis on the larger network shows that the algorithm can indeed be used for cyber-securing EVSE networks of practical sizes.

VI. Discussion and Future Research

In this section, we clarify the difference between the bad data and the attacks to EVSE networks studied in this paper. Bad data attacks usually aim to steer the operations of the power grid and the EVSE network towards the attackers' objectives such as setting lower or higher prices and causing

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/TSG.2017.2705188, IEEE Transactions on Smart Grid

frequency instability [41]. Our proposed response model will be effective in dealing with bad data attacks when they are purposefully designed to spread throughout the network. Bad data could also happen unintentionally. The unintentional bad data could be a result of the misconfiguration or malfunction of devices. Indeed, the unintentional bad data stays local and does not spread to other components. Hence, this type of bad data generated by EVs or EVSEs is not identified as an attack and does not trigger the proposed response method.

In this paper, we assumed that EVSE demand is uniformly distributed. As stated in [42], the probability density functions of loads in distribution centers show variations and a specific distribution may not represent all cases. Our model is still valid if EVSE demand follows other distribution functions. In this case, equations (25)-(26) need to be revised as given in equation (30). F and F^{-1} represent the cumulative distribution and inverse cumulative distribution functions, respectively.

$$\begin{aligned} &Pr\left(D_{EV} \leq \rho + \sum_{j\in\Upsilon} C_j x_j\right) \geq 1-\psi \\ &F\left(\rho + \sum_{j\in\Upsilon} C_j x_j\right) \geq 1-\psi \\ &\rho + \sum_{j\in\Upsilon} C_j x_j \geq F^{-1}(1-\psi) \\ &\sum_{j\in\Upsilon} C_j x_j \geq F^{-1}(1-\psi) - \rho \end{aligned} \tag{30}$$

Let's assume that D_{EV} follows a Poisson distribution function with the rate parameter of λ. Considering the two facts that Poisson is a discrete distribution function and λ is a known parameter, there exist the smallest value J_ψ such that the Poisson cumulative distribution function evaluated at J_ψ equals or exceeds $1-\psi$. Notice that J_ψ becomes a known parameter as well. Therefore, we can rewrite equation (30) as follows. The same method can be used to implement our proposed model where demand follows other distribution functions. As the case in our experiments, J_ψ equals to $D_{max}(1-\psi)$ when demand is uniformly distributed.

$$\sum_{j\in\Upsilon} C_j x_j \geq J_\psi - \rho \tag{31}$$

Furthermore, we have considered the risk parameter ψ as a predetermined input parameter to the proposed response model. In our future work, we will study the idea of integrating the risk parameter as a tunable parameter to the model such that the tradeoff decision between the risk and availability will be considered. We are also planning to extend our attack model to include EV-to-EV communications and use a more granular mobility model.

VII. Conclusion

Electrical power systems have become more vulnerable to cyber attacks due to the integration of information and communication technologies. The interdependent electric transportation system and the vulnerabilities in vehicles complicate the cyber security of smart grid and open up new opportunities for malicious actors. Attackers may compromise loads, smart meters, transmission and distribution equipment, PMUs, sensors, computers, Electric Vehicles (EVs), Electric Vehicle Supply Equipment (EVSEs) and so on. EVs may pose high risk of security due to a number of reasons. Their mobility, heavy load, communication capability make them vulnerable to attacker, they are as well as an ideal tool to implement infectious attacks.

In this paper, we propose a response model that jointly minimizes risk and maximizes availability of the smart grid under infectious attacks initiated from the EV infrastructure. EV initiated attacks can spread faster than other attacks due to vehicle-to-infrastructure and intra infrastructure (EVSE network) communications. The mobility of vehicles play a critical role in attack propagation. In this paper, we consider an attack model where malware can spread due to both vehicle-to-infrastructure and EVSE communications. Using this model, we propose a response strategy that prevents attacks to propagate further into the power grid. Our proposed response model is formulated as a Mixed Integer Linear Programming problem that minimizes the risk of attack propagation while considering the EV loads, EV threat levels and demand profile in a certain distribution system. Our results show that, the proposed response strategy addresses the interdependency of electric vehicles and smart grid.

References

[1] C. Carryl, M. Ilyas, I. Mahgoub, M. Rathod, "The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies," International Conference on Connected Vehicles and Expo (ICCVE), pp.300-305, 2-6 Dec. 2013.

[2] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, "Study of Security Attributes of Smart Grid Systems - Current Cyber Security Issues," April 2009. [Online] http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf.

[3] U.S. Department of Energy Office, Electricity Subsector Cybersecurity Risk Management Process. [Online] http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

[4] S. Mousavian, M. Erol-Kantarci, T. Ortmeyer, "Cyber Attack Protection for a Resilient Electric Vehicle Infrastructure," IEEE Globecom-Workshop on Smart Grid Resilience, San Diego, CA, December 2015, pp. 1-6.

[5] G. Chen, Z. Y. Dong, D. J. Hill and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," IEEE Transactions on Power Systems, vol. 26, no. 3, pp. 10001009, Aug. 2011.

[6] A. L. Motto, J. M. Arroyo and F. D. Galiana, "A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security Under Disruptive Threat," in IEEE Transactions on Power Systems, vol. 20, no. 3, pp. 1357-1365, Aug. 2005.

[7] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networksPhysica A: Statistical Mechanics and its Applications," Volume 389, Issue 3, 1 February 2010, Pages 595603.

[8] A.C. Chan, J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," IEEE Communications Magazine, vol.51, no.1, pp.58-65, January 2013.

[9] A.C. Chan, J. Zhou, "CyberPhysical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," IEEE Journal on Selected Areas in Communications, Vol. 32, No. 7, 2014.

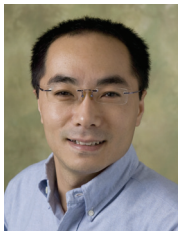
[10] H. Su, M. Qiu, H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," IEEE Communications Magazine, vol.50, no.8, pp.62-68, August 2012.

[11] E. Choo, Y. Park, and H. Siyamwala, "Identifying malicious metering data in advanced metering infrastructure," in Proc. IEEE 8th Int. Symp. Service Orient. Syst. Eng., Oxford, MS, USA, Apr. 2014, pp. 490-495.

[12] F. M. Cleveland, "Cybersecurity issues for advanced metering infrastructure (AMI)," in Proc. IEEE Power Energy Soc. Gen. Meeting Pittsburgh, PA, USA, Jul. 2008, pp. 1-5.
[13] A.K. Farraj, E. M. Hammad, A. Al Daoud, D Kundur, "A game-theoretic control approach to mitigate cyber switching attacks in Smart Grid systems," in IEEE International Conference on Smart Grid Communications, pp.958-963, 3-6 Nov. 2014.
[14] H. Mohsenian-Rad, A. Leon-Garcia, Distributed Internet-based Load Altering Attacks against Smart Power Grids, IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 667-674, December 2011.
[15] M. Esmalifalak, Z. Han, and L. Song, Effect of stealthy bad data injection on network congestion in market based power system, in Proc. IEEE Wireless Communications Network Conference, Sh anghai, China, 2012,pp. 2468-2472.
[16] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, Detecting stealthy false data injection using machine learning in smart grid, IEEE Syst. Journal, 2014.
[17] Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, Z. Han, Resilient PHEV charging policies under price information attacks, IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp.389,394, 5-8 Nov. 2012.
[18] M. Altunay, S. Leyffer, J. T. Linderoth, and Z. Xie, "Optimal response to attacks on the open science grid," Computer Networks, vol. 55, pp. 61-73, Jan. 2011.
[19] C. Shuguang, H. Zhu, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," IEEE Signal Processing Magazine, vol. 29, pp. 106-115, Sep. 2012.
[20] B. Sun, G. Yan, Y. Xiao, and T. A. Yang, "Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications," Ad Hoc Networks., vol. 7, pp. 1489-1500, 2009.
[21] S. Mousavian, J. Valenzuela, J. Wang, "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks," in IEEE Transactions on Power Systems, vol. 30, no. 1, 2014.
[22] D. S. Callaway and I. A. Hiskens, "Achieving Controllability of Electric Loads," in Proceedings of the IEEE, vol. 99, no. 1, pp. 184-199, Jan. 2011.
[23] L. Gan, U. Topcu and S. H. Low, "Optimal decentralized protocol for electric vehicle charging," in IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 940-951, May 2013.
[24] Y. Yao, T. Edmund, D. Papageorgiou , R. Alvarez,"Trilevel optimization in power network defense," IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews, 37:712-718, 2007.
[25] N. Alguacil, A. Delgadillo, J. M. Arroyo, "A trilevel programming approach for electric grid defense planning," Computers and Operations Research, Volume 41, pp. 282-290, 2014.
[26] S. Shenoy, D. Gorinevsky, "Stochastic Optimization of Power Market Forecast Using Non-Parametric Regression Models," IEEE Power and Energy Society General Meeting, July 2015.
[27] H. Liang , W. Zhuang, "Stochastic Modeling and Optimization in a Microgrid: A Survey," Energies, vol. 7, pp. 2027-2050, 2014.
[28] M. Golari, N. Fan, J. Wang, "Two-stage stochastic optimal islanding operations under severe multiple contingencies in power grids," Electric Power Systems Research, vol. 114, pp. 68-77, 2014.
[29] S. Zonouz, C.M. Davis, K.R. Davis, R.; Berthier, R.B. Bobba, W. H. Sanders, "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures," IEEE Transactions on Smart Grid, vol.5, no.1, pp.3-13, Jan. 2014.
[30] S. Uppoor, M. Fiore, J. Hrri, "Synthetic Mobility Traces for Vehicular Networking," Vehicular Networks (eds A.-L. Beylot and H. Labiod), John Wiley & Sons, Inc., 2013.
[31] J.A.P. Lopes, F. J. Soares, P. M. R. Almeida,"Integration of Electric Vehicles in the Electric Power System," Proceedings of the IEEE, Vol. 99, No. 1, January 2011.
[32] W.C. Su, H. Rahimi-Eichi, W.T. Zeng, M.Y. Chow, "A survey on the electrification of transportation in a smart grid environment," IEEE Transactions on Industrial Informatics, vol. 8, pp.1-10, 2012.
[33] D. Niyato, N. Kayastha, E. Hossain, and Z. Han, "Smart grid sensor data collection, communication, and networking: A tutorial," Wireless Communications and Mobile Computing (Wiley), vol. 14, no. 11, 2014.
[34] K. Mets, T. Verschueren, W. Haerick, C. Develder, F. De Turck, "Optimizing smart energy control strategies for plug-in hybrid electric vehicle charging," IEEE/IFIP Network Operations and Management Symposium Workshops, pp.293-299, April 2010.
[35] K. Clement, E. Haesen, J. Driesen, "Coordinated charging of multiple plug-in hybrid electric vehicles in residential distribution grids," IEEE Power Systems Conference and Exposition, pp.1-7, March 2009.
[36] E. Sortomme, M.M. Hindi, S. D. J. MacPherson, S. S. Venkata, "Coordinated Charging of Plug-In Hybrid Electric Vehicles to Minimize Distribution System Losses," IEEE Transactions on Smart Grid, vol.2, no.1, pp. 198-205, March 2011.
[37] C. Wu, H. Mohsenian-Rad, J. Huang, "Vehicle-to-Aggregator Interaction Game," IEEE Transactions on Smart Grid, vol. 3, no. 1, pp. 434-442, March 2012.
[38] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," IEEE Communications Surveys and Tutorials, Vol.14, Issue 4, pp.998-1010, 4th Quarter 2012.
[39] A. C-F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," IEEE Communication Magazine, vol. 51, no. 1, pp. 58-65, Jan. 2013.
[40] Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, Z. Han, "Resilient PHEV charging policies under price information attacks," IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp.389-394, 5-8 Nov. 2012.
[41] Y. Huang et al., "Bad data injection in smart grid: attack and defense mechanisms," in IEEE Communications Magazine, vol. 51, no. 1, pp. 27-33, January 2013.
[42] R. Singh, B. C. Pal, R. A. Jabr, "Statistical representation of distribution system loads using Gaussian mixture model", IEEE Transactions on Power Systems, vol. 25, no. 1, pp. 29-37, February 2010.

Seyedamirabbas Mousavian is an Assistant Professor of Engineering and Management in the School of Business at Clarkson University, Potsdam, NY. He received his B.S. degree in industrial engineering from Sharif University of Technology, Tehran, Iran, in 2007. After his M.B.A. degree in 2010, he received a Masters degree in industrial and systems engineering in 2012 from Auburn University, Auburn, AL. His research interests include smart grid, cyber-physical systems security, cyber-physical systems investment, power systems operations and planning, electric vehicles, and operations research. He is a member of IEEE, INFORMS, and PMI.

Melike Erol-Kantarci is an assistant professor at the School of Electrical Engineering and Computer Science at the University of Ottawa. Prior to joining University of Ottawa, she was an assistant professor at Clarkson University, NY. She received her Ph.D. and M.Sc. degrees in Computer Engineering from Istanbul Technical University in 2009 and 2004, respectively. She is currently the vice-chair of Green Smart Grid Communications special interest group of IEEE Technical Committee on Green Communications and Computing. Her main research interests are wireless networks, smart grid communications, cyber-physical systems, electric vehicles and Internet of things.



Lei Wu received the B.S. degree in electrical engineering and the M.S. degree in systems engineering from Xian Jiaotong University, Xian, China, in 2001 and 2004, respectively, and the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2008. From 2008 to 2010, he was a Senior Research Associate with the Robert W. Galvin Center for Electricity Innovation, IIT. He worked as summer Visiting Faculty at NYISO in 2012. Currently, he is an Associate Professor with the Electrical and Computer Engineering Department, Clarkson University, Potsdam, NY, USA. His research interests include power systems operation and planning, energy economics, and community resilience microgrid.

Thomas Ortmeyer is Professor of Electrical and Computer Engineering at Clarkson University, Potsdam, NY. He chaired Clarkson's Electrical and Computer Engineering Department for more than eight years, and developed and managed Clarkson's Experiential Learning Program. His research includes power quality, power system protection, and power distribution systems.