2012 IEEE/ACM Third International Conference on Cyber-Physical Systems

On False Data Injection Attacks against Distributed Energy Routing in Smart Grid

Jie Lin*, Wei Yu†, Xinyu Yang*, Guobin Xu† and Wei Zhao‡
*Xi'an Jiaotong University, Shaanxi, China, Email: Dr.linjie@stu.xjtu.edu.cn,yxyphd@mail.xjtu.edu.cn
†Towson University, MD 21252, Email: wyu@towson.edu , tigerguobin@gmail.com
‡University of Macau, Macau SAR, China, Email: WeiZhao@umac.mo

***Abstract*—Smart Grid is a new type of energy-based cyber-physical system (CPS) that will provide reliable, secure, and efficient energy transmission and distribution. The way to secure the distributed energy routing process that efficiently utilizes the distributed energy resources and minimizes the energy transmission overhead is essential in smart grid. In this paper, we study the vulnerability of the distributed energy routing process and investigate novel false data injection attacks against the energy routing process. We consider several general attacks, in which the adversary may manipulate the quantity of energy supply, the quantity of energy response, and the link state of energy transmission. The forged data injected by those attacks will cause imbalanced demand and supply, increase the cost for energy distribution, and disrupt the energy distribution. We formally model these attacks and quantitatively analyze their impact on energy distribution. Our evaluation data show that those attacks can effectively disrupt the effectiveness of energy distribution process, causing significant supplied energy loss, energy transmission cost and the number of outage users.**

***Keywords*—Smart grid, Distributed energy routing, False data injection attacks, Energy distribution.**

I. Introduction

The smart grid uses modern advanced communication technologies to make the power grid more efficient, reliable, secure and resilient. Smart grid is one typical example of cyber-physical system (CPS) [2]. One critical service of smart grid is to effectively integrate the distributed energy resources to balance the energy supply and demand. To this end, some nodes in smart grid, namely energy-suppliers, could provide residual energy to other nodes, namely energy-demanders. Obviously, transmitting energy from energy suppliers to energy-demanders will incur energy loss and resource consumption cost during the transmission.

To fully utilize the distributed energy resources and reduce the energy transmission cost caused by energy transmission among nodes, considerable research efforts have been made in the past [12], [5], [16], [10]. While these research efforts can improve the smart grid operational efficiency, the potential risk of security needs to be seriously studied before deploying these techniques into the smart grid. There have been some efforts to mitigate false date injection attacks in smart grid [14], [17], [8], [21], [11], [22], [7]. For example, Liu *et al.* proposed the false data injection attack against the state estimation of power system [14]. McMillin *et al.* [4] proposed the approach to provide a unique direction of formalizing the information flow properties for power system with inherent complexity and security requirements. Xie *et al.* [20] and Jia *et al.* [7] investigated the impact of false data injection attacks in deregulated electricity market operations, and showed that the adversary could obtain unlawful financial benefits. Nevertheless, the risks and impact of false data injection attacks against the distributed energy routing in smart grid have not been studied in the past. To fulfill this gap, in this paper we study the vulnerability of distributed energy routing process, investigate novel false data injection attacks against distributed energy routing, and systematically model and analyze their impact on energy routing process.

We study the vulnerabilities of the distributed energy routing process and investigate a number of generic attacks, in which the adversary can manipulate the quantity of energy supply, the quantity of energy request, and the link state of energy transmission. The forged data injected by attacks will cause imbalanced demand and response and incur the increased cost for energy transmission and distribution and disrupt the stability of energy service in smart grid. We formally model these attacks and quantitatively analyze their impact on the distributed energy routing process. We consider several metrics, including the supplied energy loss, the increased energy transmission cost, and the number of outage users.

We simulate the impact of these analyzed attacks. Our data consistently confirm our theoretical findings and illustrate that our proposed attacks can effectively disrupt the effectiveness of distributed energy routing, posing significant supplied energy loss, an increase in energy transmission and distribution cost and the number of outage users. For example, our results show that the supplied energy loss increases in a linear fashion with the compromised demand-node rate. The energy transmission cost increases as the compromised demand-node rate or the compromised supply-node rate increases. The user outage ratio increases as the compromised demand-node rate or the compromised supply-node rate or the compromised energy link rate increases.

The remainder of the paper is organized as follows: In Section II, we present the network and threat models. In Section III, we review the distributed energy routing process and investigate the false data injection attacks on the energy routing process. In Section IV, we analyze the impact of the proposed attacks. In Section V, we show experimental results to validate the effectiveness of those attacks. We conclude the paper in Section VI.

II. Network and Threat Models

In a smart grid, a number of users are connected to the grid via communication and energy transmission links. Each user in a smart grid can transform the distributed energy resources into power and store the power locally, and energy-rich users can provide power to energy-poor users. Fig. 1 illustrates a

978-0-7695-4695-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCPS.2012.26

graph model of a smart grid. The node here represents the energy demander or supplier. Due to the difference in locations and efficiency of energy generation, each node in the grid generates and consumes different quantities of energy. When a node consumes more energy than it can generate, the node is denoted as an energy demand-node and needs to pull energy from the grid. When a node consumes less energy than it generates, the node is denoted as an energy supply-node and can push residual energy into the grid and meet the demand from demand-nodes. The energy distribution among nodes can balance the energy supply and demand in smart grid.

In this paper, we use nodes to represent users. The measuring components can determine whether the node should be a supply-node or demand-node. To balance the demand and response, the node could connect to the grid and communicate with other nodes, sharing the measurements, energy demands and requests.

Because the measurement component supported by smart equipment (e.g., smart meter), plays an important role in smart grid, it can also be a target for cyber attacks. Because those measuring devices may connected through open network interfaces, the adversary can possibly launch attacks against those devices [15], [6]. The adversary may modify data and compromise the measuring component via injecting malicious codes into the memory of measuring component [18]. The adversary then injects false energy demand and supply messages into the grid via the compromised measuring components. Note that, if a node is denoted as compromised node, we mean that the measuring component of the node is compromised by the adversary.

We assume that each node can connect to energy storage devices, and the grid offers energy for the demand node based on its demand, and the node may receive more energy than it really needs and stores the extra energy locally. Because the topology of the grid is static, it is possible for all nodes in grid to know the topology information of the grid. If the grid is large and complex, the topology information stored in each node can be large. To reduce the size of topology information in each node, we can divide the large grid into clusters or regions and each node can store the topology information of the grid by clusters or regions. In this way, each node can have a view of the grid even if the energy grid is large and complex. We also consider that the adversary knows the topology of the grid and can only compromise a small number of nodes with limited attack resources.

III. Distributed Energy Routing and False Data Injection Attacks

A. Overview of Distributed Energy Routing Schemes

In the energy generation and consumption processes, the nodes in the grid may be imbalanced. To resist the imbalance, some nodes could be supply-nodes and provide residual energy to demand-nodes. Nevertheless, if multiple demand-nodes exist in the grid, they would affect each other to obtain energy, posing inefficiency in energy distribution. To address this issue, we proposed novel distributed energy routing schemes [12] to determine the optimal energy route for transmitting energy among nodes in the grid. With the optimal energy routes, supply-nodes can effectively supply energy to demand-nodes with low transmission cost.

The basic idea of our distributed energy routing schemes is described below. In the grid, multiple supply-nodes, demand-nodes, communication links, and energy links are considered and energy links connecting to the nodes have capacity constraints. Deriving the optimal energy routes becomes a challenging task because numerous constraints need to be satisfied simultaneously. First, to ensure the reliable supply of energy for demand-nodes, the input energy of demand-nodes and energy transmitted by the energy links to which demand-nodes connect should be equal to their demanded energy. Second, the output energy of supply-nodes should be no more than the energy they can provide. Hence, in the energy transmission we only need to determine the amount of energy that each link should transmit based on the above constraints. According to the above analysis, the problem of selecting the optimal routes can be formalized as an optimization problem, which can determine the amount of energy transmitted through energy links based on the supply and demand requests of all nodes along with energy link capacity, and the overall transmission cost is minimized. The formalization of distributed energy routing schemes is listed below.

$$\textbf{\textit{Objective.}} \quad \textit{Min} \left\{ \textit{Cost} = \frac{1}{2} \cdot \sum_{L_{ij} \in L} (|E_{ij}| \cdot Cost_{ij}) \right\}$$

$$\textbf{\textit{S.t.}} \quad \begin{cases} \forall v \in N_P, & \sum\limits_{i \in N_v} E_{vi} \le P_v \\ \forall u \in N_D, & \sum\limits_{j \in N_u} E_{uj} = -D_u \\ \forall L_{ij} \in L, & E_{ij} = -E_{ji} \end{cases}, \tag{1}$$

where i and j are the IDs of nodes, $Cost_{ij}$ is the transmission cost on energy link L_{ij}, E_{ij} is the energy needed to transmission on energy link L_{ij}, L is the set of all energy links in the grid, N_P is the set of supply-nodes, N_D is the set of demand-nodes, N_v and N_u are the sets of neighbor-nodes of node v and node u, respectively, and P_v is the energy that supply-node v can provide, D_u is the request energy of demand-node u. Equation (1) formalizes the distributed energy routing schemes, and the optimal scheme will be obtained by solving this optimization problem. The optimization function is non-linear programming (NLP) with linear constraints and non-linear objective functions. Numerous approaches have been developed to solve this problem in the past, e.g., simulated annealing [9] and genetic algorithm [19].

Based on Equation (1), the optimal energy routes can be obtained. Note that in Section III.C, we formalize the optimization problems to show the damage to the routing process in different attack scenarios. All of these optimization problems are basically derived from Equation (1) here. The energy that each supply-node needs to provide for demand-nodes can be denoted as

$$P'_v = \sum_{i \in N_v} E_{vi}. \tag{2}$$

B. Energy Distribution Process

Recall that the measuring component at the node (e.g., smart meter) plays an important role in the energy distribution process, and it can determine whether the node belongs to a supply-node or demand-node over time. Based on the

role of the node, it will coordinate with each other via communication networks and ensure that the energy will be distributed efficiently to meet the demand and supply with the minimal overhead. The basic workflow of energy routing process is described below. Note that, we assume that the energy transmission among nodes is implemented periodically. All notations used in this paper are defined in Table I.

Step 1: At the beginning of new cycle (t+1), a measuring component determines the local node's energy storage S_u, and predicts the energy generation G_u and energy consumption C_u in the next cycle.

Step 2: Based on the result of *Step 1*, if the node is supply-node, the measuring component can determine the quantity of energy, say P_u, which it can provide to the grid. We have $P_u = S_u - C_u$. If the node is demand-node, the measuring component determines the quantity of energy, say D_u, which it needs to obtain from the gird. We have $D_u = C_u - S_u - G_u$.

Step 3: When a node is identified as a demand-node, its measuring component broadcasts the energy request message including the demanded energy, say D_u, to other nodes in the grid. Note that because the grid will be divided into several small grids if the grid becomes large, the demand-nodes could not necessarily send the information to supply nodes which are far away (located in different region).

Step 4: All nodes receiving the request message will send the response message back to the demand-node. The response message includes the energy that the node can supply, the set of cost for transmitting the energy on all energy links that the node connects to, and the set of states of all energy links that node connects to, say P_v, $Cost_v$, LS_v, respectively. Note that, P_v can be zero, representing the node could provide no energy into the grid.

Step 5: When the demand-node u receives the response messages from all nodes, it derives the optimal energy routes via the distributed energy routing process [12]. The optimal energy routing process will provide the requested energy with minimum resources to be consumed. Then, the demand-node sends the routes, obtained by energy routing process, for all nodes, which includes the energy to be transmitted on all energy links.

Step 6: Based on the routes generated by the energy routing schemes, each node either supplies the scheduled energy for each connected energy link or gets requested energy from each connected energy link.

C. False Data Injection Attacks

We now systematically investigate the false data injection attacks against the distributed energy routing process. Recall that using these compromised measuring components, the adversary could launch a new class of false data injection attacks, namely the energy deceiving attacks discussed here, to disrupt the energy distribution process. Once again, if a node is denoted as compromised, we mean that the measuring component in the node is compromised by the adversary.

Definition 1: The *Energy Deceiving Attack* is defined as a typical false data injection attack. In this attack, the adversary can inject either the forged energy or link-state information into the energy request and response message among nodes in order to disrupt the distributed energy distribution process.

Based on the compromised measuring components, the adversary can inject the false data in the following ways: (i) the false quantity of energy that demand-nodes demand (denoted as D_u^*), (ii) the false quantity of energy that supply-nodes could provide (denoted as P_v^*), and (iii) the false states of the energy links (denoted as LS_{uv}^*). Note that u and v are denoted as the IDs of demand-node and supply-node, respectively. Hence, based on the types of forged data, the energy deceiving attacks can be categorized into the following two groups: (i) injecting false energy data, and (ii) injecting false link-state data, which will be discussed next.

TABLE I
NOTATION

u, v:	The ID of normal node.
$u*, v*$:	The ID of compromised node.
t:	The energy transmission cycle.
S_u:	The energy storage of node u.
G_u:	The predicted energy generation of node u.
C_u:	The predicted energy consumption of node u.
P_u:	The energy that node u can provide.
D_u:	The energy that node u requests.
K:	The key used to encrypt message.
MAC:	Message Authentication Code (MAC).
L_{ij}:	The energy link between node i and node j.
$Cost_{ij}$:	The transmission cost consumed in energy link L_{ij}.
LS_{ij}:	The link state of the energy link L_{ij}.
P'_v:	The energy that node v needs to provide based on the distributed energy routing process.
E_{ij}:	The energy transmitted on energy link L_{ij} as normal.
E^*_{ij}:	The energy transmitted on energy link L_{ij} when the false data injection attack exists.
P^*_v:	The false energy that compromised node v provides.
P'^*_v:	The energy that compromised node v needs to provide based on the distributed energy routing process.
D^*_u:	The false energy that compromised node u requests.
LS^*_{ij}:	The false link-state of energy link L_{ij}.
T_E:	The energy threshold.

1) Injecting False Energy Data: As the different roles in the energy distribution process, the adversary may compromise either supply-nodes or demand-nodes and launch the energy deceiving attacks. We now discuss those attacks in details.

Energy-request Deceiving Attack: When the adversary compromises the demand-nodes, the energy deceiving attack could be launched on *Step 3* in the energy distribution process. That is, the adversary could forge a large quantity of demanded energy, say D_u^*, and send the energy-request messages to all energy-demand nodes in the grid via the compromised measuring components. We denote this type of attack as the energy-request deceiving attack. In this way, the distributed energy routing process will give the false requested energy from the demand-node. When the claimed quantity of demanded energy increases, more energy will be wasted because of the limited storage capacity of the demand-node. As the quantity of demanded energy increases, the energy transmission cost will increase as well. In addition, because the quantity of energy that all supply-nodes can provide is limited, a number of nodes will not receive enough energy and energy outage will occur because of the large false quantity of requested energy from demand-nodes.

Energy-supply Deceiving Attack: When the adversary compromises the supply-nodes, the energy deceiving attack could be launched on *Step 4* in the energy distribution process. That is, the adversary could forge a false quantity of energy it can truly provide, say P_v^*, and send back the response to demand-nodes. We denote this type of attack as the energy-supply deceiving attack, which could incur the increase in energy transmission cost and the number of outage users. In particular, when the adversary forges and claims less energy

than the supply-node can truly provide, the total claimed energy that all supply-nodes could provide will be less than the requested energy. When this occurs, more users will be denied of energy, and the total energy transmission cost caused by the energy distribution may increase as well. When the adversary forges and claims more energy than the supply-node can truly provide, the supply-node cannot provide enough claimed energy and make some demand-nodes fail to obtain enough requested energy. When this occurs, the supply of energy in the grid is disrupted.

2) Injecting False Link-state Data: Besides forging the energy information, the energy deceiving attacks can forge the false state of energy links, and inject the false link-state information into the energy routing process. The consequence of injecting false link-state data could incur high energy transmission cost and imbalance of energy supply because of transmitting energy on invalid energy links, and establishing the energy-acnode defined below.

Definition 2: Energy-acnode is defined as one or multiple nodes, which are isolated from the grid in terms of energy supply and demand. The adversary could inject the forged invalid state of energy links associated with the compromised nodes into the grid. As such, some nodes in the grid will become isolated and cannot exchange energy with other nodes in the grid.

As shown in Fig. 1, when the adversary injects the false information of link states, and makes energy link L_{BE} and L_{EH} invalid, the node E will become an energy-acnode. When a node (or a group of nodes) becomes energy-acnode, it will not be able to obtain energy from the grid and provide residual energy to the grid. As we can see, the more the energy-acnodes exist in the grid, the better chances are that the grid will not provide effective energy distribution to users.

When the adversary injects the false state information of the energy link (no matter whether the adversary launches the attack from supply-nodes or demand-nodes), we have the following two options: (i) *Claiming an invalid energy link as valid*. When this occurs, the energy routing process will assign the energy transmission task to invalid energy links. This causes some demand-nodes to fail in receiving enough requested energy; (ii) *Claiming a valid energy link as invalid*. When this occurs, it will increase the energy transmission cost and the chance of nodes to become energy-acnode.

IV. Modeling and Analysis

We now model and analyze the impact of proposed attacks on the distributed energy routing process in the grid.

A. Impact of Injecting False Energy Data

1) Impact of Energy-request Deceiving Attack: When the adversary compromises the demand-nodes, the adversary could forge a large quantity of requested energy, say D_u^*, to replace the normal demanded energy, say D_u, and send the false energy-request messages to energy-supply nodes in the grid via the compromised nodes on *Step 3* during the energy routing process.

Supplied Energy Loss: The adversary can compromise a demand-node and forge the demanded energy from the compromised node. The forged requested energy, say D_u^*, will be always larger than the true requested energy, say D_u, in order to pose the supplied energy loss. When the grid has enough energy to meet the demands of all demand-nodes, the compromised node will receive more energy than it truly requests due to the energy-request deceiving attack. As we stated in Section II, each node may connect to an energy storage device, and the grid offers energy for the demand node based on its demand, and thus node may receive more energy than it really needs and saves extra energy locally. If a large quantity of supplied energy is received and stored by compromised nodes, the available energy of the grid would be largely reduced, leading to some demand-nodes to be outage. From this viewpoint, we consider that the supplied energy received and stored by compromised nodes is lost from the grid and may have impact on the grid stability. The quantity of supplied energy loss can be denoted as $\Delta D_u = D_u^* - D_u$. Obviously, if n demand-nodes are compromised in the grid, the quantity of supplied energy loss in the grid is

$$\Delta D^n = \sum_{u_i \in N_{D^*}} \Delta D_{u_i}. \tag{3}$$

where N_{D^*} is the set of compromised node and u_i is the ID of the compromised node. Obviously, when the grid has enough energy for demand-nodes, to cause more supplied energy loss, the larger number of demand-nodes needs to be compromised and the larger forged demanded energy needs to be claimed. Unfortunately, a node could not persistently claim too much quantity of demanded energy because this will lead to the detection of attacks.

To avoid the detection, the claimed quantity of demanded energy should be limited by an energy threshold. It is defined as the upper limit of requested energy of a demand-node that the adversary can forge, denoted as T_E, without being detected. Because the energy threshold limits the forged requested energy, another parameter that the adversary may play is to increase the number of compromised nodes. Nevertheless, the adversary only has limited attacking resources. Note that we only analyzed the supplied energy loss with the assumption that the grid can provide enough energy to all demand-nodes here even if the grid is affected by energy-request deceiving attacks. We will further analyze the supplied energy loss in subsection IV.A-1 in the scenario, where the grid could not provide enough energy to all demand-nodes.

Energy Transmission Cost: When the compromised nodes claim themselves as demand-nodes, it will not only cause the loss of supplied energy, but also incur the increase in energy transmission cost. Unfortunately, when the grid has enough energy to meet the requests from all demand-nodes, the false energy request data from compromised demand-node could mislead the energy distribution decision. As the consequence, the obtained routes will incur a higher energy transmission cost.

If n demand-nodes are compromised in the grid and all compromised nodes claim forged request energy, the formalization of the affected energy routing can be derived from

Equation (1) and listed as following,

$$\textbf{\textit{Objective.}} \quad Min \left\{ Cost_n^* = \frac{1}{2} \cdot \sum_{L_{ij} \in L} (|E_{ij}| \cdot Cost_{ij}) \right\}$$

$$\textbf{\textit{S.t.}}$$

$$\begin{cases} \forall v \in N_P, & \sum\limits_{i \in N_v} E_{vi} \leq P_v \\ \forall u \in N_D, & \sum\limits_{j \in N_u} E_{uj} = -D_u \\ \forall u^* \in N_{D^*}, & \sum\limits_{j \in N_{u^*}} E_{u^*j} = -D_{u^*}^* \leq T_E \\ \forall L_{ij} \in L, & E_{ij} = -E_{ji} \end{cases}, \tag{4}$$

where $D_{u^*}^*$ is the forged demanded energy at compromised node $u*$, and $Cost_n^*$ is the minimum cost of energy transmission under the attack. According to Equations (1) and (4), the increased cost for transmitting energy become

$$\Delta Cost_n = Min(Cost_n^*) - Min(Cost). \tag{5}$$

According to Equation (5), only if $\Delta Cost_n > 0$, the cost of energy transmission will increase due to the energy-request deceiving attack.

Assume that the normal and effected energy assignment in the grid are E and E^* obtained by Equations (1) and (4), respectively. To ensure the existence of solutions of Equation (4), Equation (6) listed below must have solutions and we have

$$\begin{cases} \forall v \in N_P, & A_v \cdot (E^* - E) \leq P_v - P_v' \\ \forall u \in N_D, & A_u \cdot (E^* - E) = 0 \\ \forall u^* \in N_{D^*}, & A_{u^*} \cdot (E^* - E) = -D_{u^*}^* + D_{u^*} \end{cases}, \tag{6}$$

where E^* is $[E_1^*, E_2^*, \cdots, E_l^*]^T$, E_i^* represents the energy transmitted on energy link L_i, and l is the number of energy links in the grid, A_i is $[a_{ij_1}, a_{ij_2}, \cdots, a_{ij_M}]$, a_{ij} is $\{-1, 0, 1\}$, M is the number of nodes in the grid. When $a_{ij} = 0$, there is no energy link between node i and node j. When $a_{ij} = -1$, the energy is transmitted from node j to node i via the energy link. When $a_{ij} = 1$, the energy is transmitted from node i to node j via the energy link.

Equation (6) shows that, when the grid can provide enough energy to all demand-nodes and the grid is under the attack, the demanded-energy raised by the deceiving attack could obtain the false energy routes by injecting false requested energy information. The increased cost of energy transmission should be the minimum cost of energy transmission caused by transmitting $|E^* - E|$, based on Equations (4) and (6). In addition, with the increase of forged requested energy $D_{u^*}^*$ and the number of compromised nodes, $|E^* - E|$ increases. Then the increased cost of energy transmission $\Delta Cost_n$ increases as well and we have $\Delta Cost_n > 0$. Hence, the energy-request deceiving attack can certainly increase the energy transmission cost.

Number of Outage Users: The above analysis is based on the assumption that all supply-nodes can provide enough energy to all demand-nodes in the grid, even if the grid is affected by the energy-request deceiving attack. However, supply-nodes may not provide enough energy to demand-nodes in some cases, such as suffering from disaster or during the surge in electricity demand or affected by energy-request deceiving attack. Because of the insufficient supply of energy, some nodes in the grid will become outage to ensure reliable energy supply to other nodes.

Recall that when supply-nodes could not provide enough energy to demand-nodes, the distributed energy process will maximize the number of demand-nodes that could receive enough requested energy and minimize the number of outage demand-nodes. The problem can be represented by

$$\textbf{\textit{Objective.}} \quad Min \{\|N_D'\|\}$$

$$\textbf{\textit{S.t.}}$$

$$\sum_{u \in N_D'} D_u \geq \sum_{u \in N_D} D_u - \sum_{v \in N_P} P_v, \tag{7}$$

where $\|N_D'\|$ denotes as the number of elements in N_D', N_D' is the set of outage demand-nodes, N_D is the set of all demand-nodes, and we have $N_D' \subseteq N_D$. In our paper, we consider a prioritization scheme in the grid, where the distributed energy routing process will maximize the number of demand-nodes that could receive enough requested energy and minimize the number of outage demand-nodes.

Obviously, to increase the number of outage nodes in the grid, the adversary should increase the minimum $\|N_D'\|$ via the energy-request deceiving attack. To pose a serious damage, the adversary is prone to let more normal demand-nodes into set N_D' and more compromised demand-nodes into set $N_D - N_D'$. In this case, more normal demand-nodes will become outage, and more compromised demand-nodes provided claimed requested energy to be used by the adversary to pose other damages such as supplied energy loss. Because the elements of set N_D' are identified by the requested energy from the demand-node, the adversary could select a proper $D_{u^*}^*$ for the compromised demand-node u^*. This sets more normal demand-nodes in set N_D' and more compromised demand-nodes in $N_D - N_D'$. In the following, we first describe how the distributed energy routing process selects these demand-nodes for set N_D' in the normal case. We then describe how to select compromised demand-nodes to launch the energy-request deceiving attack such that more nodes become outage.

Assume that the number of demand-nodes and supply-nodes in the grid are x and y, respectively. Then, we have $x+y \leq M$, where M is the total number of nodes in the grid. In the normal case, all demand-nodes could be sorted based on their requested energy. The order should be

$$D_{u_1} \geq D_{u_2} \geq \cdots \geq D_{u_x}, \tag{8}$$

where u_i is the ID of demand-node. To ensure the minimum number of demand-nodes to become outage, the distributed energy routing process will not provide energy for these nodes from demand-node u_1 to demand-node u_s, where u_s will meet the condition listed below

$$\sum_{j=s}^{x} D_{u_j} \geq \sum_{v \in N_P} P_v \geq \sum_{j=s+1}^{x} D_{u_j}. \tag{9}$$

Based on the above scheme, the distributed energy process selects demand-nodes from u_1 to u_s to establish set N_D' in the normal case.

With the energy-request deceiving attack which controls n compromised nodes, based on Equations (8) and (9), compromising demand-nodes with lower requested energy will

make more compromised demand-nodes in set $N_D - N'_D$ and more normal demand-nodes in set N'_D. With the compromising demand-nodes, the relationship between the maximum number of outage nodes and the increased requested energy of compromised demand-nodes is listed below, which is derived from Equations (7), (8)and (9).

$$\textbf{\textit{Objective.}} \quad Max\{k\}$$
$$\textbf{\textit{S.t.}}$$
$$\begin{cases} \sum_{j=s}^{x} D_{u_j} \geq \sum_{v \in N_P} P_v \geq \sum_{j=s+1}^{x} D_{u_j} \\ \forall u_j^* \in N_{D^*}, \qquad D_{u_k} \geq D_{u_j^*} \\ \sum_{j=s+1}^{k-1} D_{u_j} \leq \sum_{u_j^* \in N_{D^*}} (D_{u_j^*}^* - D_{u_j^*}) \leq \sum_{j=s+1}^{k} D_{u_j} \end{cases}, \quad (10)$$

where k is the number of outage nodes when the grid is under energy-request deceiving attack, $(D_{u_j^*}^* - D_{u_j^*})$ is the increased requested energy at compromised demand-node u_j^*, and N_{D^*} is the set of compromised demand-nodes. Equation (10) tells that when the forged energy from each compromised node is smaller than the normal requested energy of kth demand-node based on Equation (8) (i.e., node u_k in Equation (8)), the number of outage nodes should increase from s to k, where $x > k > s$. That is, with the energy-request deceiving attack, the number of outage nodes will increase by $(k - s)$.

The damages of energy-request deceiving attack would be maximum only if the normal demanded energy of these n compromised demand-nodes are n smallest ones in all demand-nodes. Hence, we assume that the adversary compromise n demand-nodes, which request n least amount of energy. When $n + k < x$, all n compromised demand-nodes are in set $N_D - N'_D$. In this case, the energy requests from all n compromised demand-nodes will be satisfied by the distributed energy routing process, and the supplied energy loss will occur, and the quantity of supplied energy loss becomes

$$\Delta D^n = \sum_{u_j^* \in N_{D^*}} (D_{u_j^*}^* - D_{u_j^*}) \quad \leq \sum_{u_j^* \in N_{D^*}} (D_{u_k} - D_{u_j^*}). \quad (11)$$

When $n + k \geq x$, only $(x - k)$ compromised demand-nodes are in set $N_D - N'_D$. In this case, only energy requests from $(x - k)$ compromised demand-nodes will be satisfied, and the quantity of supplied energy loss becomes

$$\Delta D^n = \sum_{j=k+1}^{x} (D_{u_j^*}^* - D_{u_j^*}) \leq \sum_{j=k+1}^{x} (D_{u_k} - D_{u_j^*}). \quad (12)$$

2) Impact of Energy-supply Deceiving Attack: When the adversary compromises the nodes and manipulates them to become supply-nodes, the adversary could forge false energy, say P_v^*, for the compromised supply-nodes to replace the normal one, say P_v. and send them to all demand-nodes on *Step 4* during the energy routing process. In this subsection, we consider only the compromised supply-nodes exist and the impact of energy deceiving attack with both compromised demand-nodes and supply-nodes can be derived by combining the analysis in subsections IV.A-1 and IV.A-2.

When the grid is under the energy-supply deceiving attack, the formalization of the affected energy routing become

$$\textbf{\textit{Objective.}} \quad Min \left\{ Cost_n^* = \frac{1}{2} \cdot \sum_{L_{ij} \in L} (|E_{ij}| \cdot Cost_{ij}) \right\}$$
$$\textbf{\textit{S.t.}}$$
$$\begin{cases} \forall v \in N_P, & \sum_{i \in N_v} E_{vi} \leq P_v \\ \forall u \in N_D, & \sum_{j \in N_u} E_{uj} = -D_u \\ \forall v^* \in N_{P^*}, & \sum_{i \in N_{v^*}} E_{v^* i} \leq P_{v^*}^* \\ \forall L_{ij} \in L, & E_{ij} = -E_{ji} \end{cases}, \quad (13)$$

where $P_{v^*}^*$ is the energy that compromised supply-node v^* claims to provide.

In the energy-supply deceiving attack, by either claiming larger or smaller energy than the normal energy that these compromised supply-nodes can provide, the energy distribution process will be disrupted. Hence, we analyze the damages of energy-supply deceiving attack in two cases: (i) *Claiming more energy than the supply-node can provide,* and (ii) *Claiming less energy than the supply-node can provide*. The damages of energy-supply deceiving attack analyzed in this subsection only include the energy transmission cost and the number of outage users, while the supplied energy loss will not be considered. Note that as the supplied energy loss depends on the quantity of increased requested energy of compromised demand-nodes, the loss of supplied energy will not occur if no compromised demand-nodes exist.

Claiming more energy than the supply-node can provide: When the adversary claims more energy than what the compromised supply-nodes can provide, the cost of energy transmission may not increase, but instead decrease. This is because to disrupt the normal energy routes, the energy-supply deceiving attack should create new energy routes, which are more optimal than the normal energy routes, and then the normal energy routes will be replaced by the new ones. When the adversary only claims more energy than the compromised supply-nodes can provide, by comparing Equations (1) and (13), the solutions of Equation (1) are included in the solutions of Equation (13). Hence, the new energy routes obtained by Equation (13) must be more optimal than the normal ones obtained by Equation (1). Otherwise, the normal energy routes would not be replaced by the new energy routes, and no damage will occur. Hence, when the adversary fakes some supply-nodes and wants to disrupt the energy transmission in the grid, the forged energy $P_{v^*}^*$ must make the new energy routes, which are more optimal than the normal energy routes. That is, the cost for transmitting energy will be reduced.

Although claiming more energy than what supply-nodes can provide will not pose the supplied energy loss and the increase in energy transmission cost, it may disrupt the supply of energy to demand-nodes and cause nodes outage. *Theorem 1* shows the condition for the energy-supply deceiving attack to disrupt the energy transmission process.

Theorem 1: To disrupt the energy transmission in the grid (i.e., replacing the normal energy routes by the new energy routes caused by energy-supply deceiving attack), a compro-

mised supply-node should be asked by energy routing process to provide more energy than it can truly provide.

The detailed proof of *Theorem 1* can be found in our technical report [13]. When compromised supply-nodes claims more energy than it can provide, some demand-nodes will not receive the expected requested energy, and ultimately cause the imbalance of energy supply in the grid. Note that, it may not disrupt the energy transmission if the adversary randomly compromises supply-nodes and launches the energy-supply deceiving attack, because it may not satisfy the condition defined in *Theorem 1*. As only compromising some special supply-nodes could make the condition to be met and disrupt the energy distribution, we will consider how to construct these specific supply-nodes in details.

Recall that in the distributed energy routing process, its main goal is to find the optimal energy routes to distribute energy with the minimum cost of energy transmission. To this end, *Theorem 2* shows the condition where each supply-node must use the shortest path to transmit energy to demand-nodes.

Theorem 2: In the distributed energy routing process, each supply-node uses the shortest path to transmit energy to demand-nodes. In particular, for each demand-node u, each supply-node v uses the shortest path between u and v to transmit energy, and the transmitted energy is P'_{vu}, and $P'_{vu} \in [0, P_v]$, where the weight of each energy link is the cost of energy transmission.

The detailed proof of *Theorem 2* can be found in our technical report [13]. Assume that the weight of the path between v_i and u is $W_{v_i u}$, we can sort the shortest paths of all supply-nodes to the demand-node u in an ascending order by

$$W_{v_1 u} \leq W_{v_2 u} \leq \cdots \leq W_{v_y u}, \tag{14}$$

where y is the number of supply-nodes in the grid. As we can see, the basic idea of distributed energy routing process is to find an optimal set of P'_{vu}, which can make the minimum cost of energy transmission. The total cost of energy transmission will be minimal one, when a demand-node receives as much energy as possible from a supply-node, and the shortest path from the supply-node to the demand-node is the smallest one comparing with the shortest paths from other supply-nodes to the demand-node. For example, in the normal case, the distributed energy routing process makes demand-node u receiving as much energy as possible from supply-node v_1 to minimize the total energy transmission cost, because the shortest path between v_1 and u has the smallest weight. Hence, if supply-node v_1 is compromised and claims more energy than it can provide, i.e., $P^*_{v_1} > P_{v_1}$, the distributed energy routing process, for a demand-node u, will increase the $P'_{v_1 u}$ and reduce $P'_{v_i u}$ to decrease the total cost of energy transmission, where v_i represents the set of supply-nodes except v_1. Then, the supply-node v_1 may not provide enough energy $P'_{v_1 u}$ for demand-node u because of $P^*_{v_1} > P_{v_1}$, and the energy transmission will be broken. The impacted demand-nodes should be ones on the shortest path between v_1 and u. Note that the shortest path between two nodes could be obtained by Dijkstra's algorithm.

Because the adversary may obtain the topology of the grid, the adversary can obtain a subset of supply-nodes, say V. For each supply-node in V, a demand-node must exist in the grid, such that the shortest path between the supply-node and the demand-node is the shortest one comparing with the shortest paths between other supply-nodes and the demand-nodes. For example, based on Equation (14), supply-node v_1 should in set V.

According to above analysis, if the adversary compromises supply-nodes in set V and launches the energy-supply deceiving attack by claiming more energy than these compromised supply-nodes can provide, the attack will disrupt the energy transmission. This will make some demand-nodes fail to obtain requested energy. The more supply-nodes to be compromised, the more serious damage will occur. Because the grid topology is relatively static, the adversary may obtain set V and compromise the corresponding supply-nodes.

Claiming less energy than the supply-node can provide: In the energy-supply deceiving attack, the adversary can claim less amount of energy than what the supply-nodes can provide. In this case, it may increase the energy transmission cost and the number of outage nodes.

As shown by the analytical results in the previous subsection, with the increase of $P'_{v_1 u}$, the total cost of energy transmission decreases. With the decrease of $P'_{v_1 u}$, the total cost of energy transmission increases. Hence, when the adversary obtains set V and compromises some supply-nodes in set V and makes these node claim less amount of energy than they can provide, i.e., $P^*_{v^*} < P_{v^*}$, the total cost of energy transmission in the grid will increase. The increased cost can be denoted as $(Cost^*_n - Cost)$, where $Cost^*_n$ and $Cost$ are the total cost of energy transmission with the attack and without the attack, and they can be derived by Equations (13) and (1), respectively.

More seriously, if

$$\sum_{v^* \in N_{P^*}} P^*_{v^*} + \sum_{v \in N_P} P_v < \sum_{u \in N_D} D_u, \tag{15}$$

where N_{P^*} is the set of compromised supply-nodes, N_P is the set of normal supply-nodes, and N_D is the set of all demand-nodes, the attack would make some demand-nodes outage. Assume that the number of outage nodes in the grid without the attack is s, where s is in $[0, x]$, and x is the number of demand-nodes in the grid. When s is equal to "0", no outage node exists in the grid without the attack. When the energy-supply deceiving attack meets the condition in Equation (15), the increased number of outage nodes caused by the attack is $(k - s)$, where k represents the total number of outage nodes and can be obtained by solving the following optimization problem, which is derived from Equation (7):

$$\begin{aligned} &\textbf{\textit{Objective.}} \quad k = Min\,\{\|N'\|\} \\ &\quad \textbf{\textit{S.t.}} \\ &\sum_{u \in N_D} D_u \geq \sum_{u \in N_D} D_u - \sum_{v \in N_P} P_v - \sum_{v^* \in N_{P^*}} P^*_{v^*}. \end{aligned} \tag{16}$$

B. Impact of Injecting False Link-state Data

Through the compromised nodes, the adversary can also inject false link-state information to disrupt the energy distribution in the grid. Because energy links are commonly deployed in open fields, the broken circuit may happen due to many reasons. In this case, the adversary may claim the invalid energy links as valid one, and the distributed energy routing process may still assign the energy transmission task

to these links. Then, some demand-nodes could not receive energy because these links cannot accomplish the assigned task, and the energy transmission in the grid will be disrupted. In addition, when the states of all energy links associated with a node are claimed as invalid, the node will become an energy-acnode defined in *Definition 2*. That is, the node cannot get energy from other nodes and provide energy to other nodes. Besides claiming invalid energy links as valid, the adversary may claim valid energy links as invalid, which will incur the increase of total cost of energy transmission in the grid. In the following, we analyze the impact of this attack in the following two cases: (i) claiming valid energy links as invalid, and (ii) claiming invalid energy links as valid.

1) Claiming invalid energy links as valid: If an invalid energy link is claimed as a valid one by the adversary, the distributed energy routing process may transmit energy through this link, which may disrupt the energy transmission in the gird. According to *Theorem 2*, only if the claimed valid link is the part of the shortest path between a pair of demand-nodes and supply-nodes in set V, the energy link may be assigned any energy to transmit, where set V has the same definition in subsection IV.A-2. In this case, all demand-nodes in the shortest path will be affected by the injected false link-state information and cannot receive enough requested energy. Hence, to disrupt the supply of energy in the grid, the claimed valid link must be a part of the shortest path described above. Fortunately, it is difficult for the invalid links to meet the above conditions, and then the adversary could not claim these invalid links as valid to disrupt the supply of energy. Thus, the damage caused by claiming invalid links as valid would occur with a lower probability.

2) Claiming valid energy links as invalid: If a valid energy link is claimed as an invalid one by the adversary, energy that should be transmitted on the link will be assigned for other links by the distributed energy routing process, posing the increase of total energy transmission cost. However, randomly selecting a valid link and claiming it as invalid one may not cause the increased cost, because the distributed energy routing process may not assign any energy transmission task for the randomly selected link in the normal case. Based on *Theorem 2*, as long as the selected link is part of the shortest path between a pair of demand-nodes and supply-nodes in set V, the distributed energy routing process will assign the energy transmission task for the selected link in the normal case. Then, claiming the selected links as an invalid one will cause the increased cost because the energy that was originally transmitted on the link will be reassigned to other links. This can be explained as following: when the adversary claims the selected link as the invalid one, the shortest path including the selected link will be invalid, and energy originally transmitted on the shortest path will be retransmitted on other paths, and total cost will be increased. This is because, based on *Theorem 2*, the cost of energy transmission on the shortest path is smaller than the cost on other paths. Note that, the selected link could be part of several shortest-paths between several pairs of demand-nodes and supply-nodes in set V. In a normal case, energy link with lower transmission cost may transmit more energy, and thus the results of selecting compromised energy links based on the way mentioned above will be similar to the results of selecting these links based on their capacity, i.e., the great quantity of energy transmitted on the links.

Claiming multiple links as invalid ones may lead to energy-acnode as defined in *Definition 2*. Energy-acnode cannot exchange energy with other nodes in the grid, and thus a demand-node will be outage if it becomes the energy-acnode. The chance of a normal node becoming an energy-acnode is determined by the number of energy links that it connects to, because a node becomes an energy-acnode only if all energy links that the node connects to are claimed as invalid ones. Multiple connecting demand-nodes may be treated as one logical-node. The adversary may let the logical-node become an energy-acnode, such as demand-node D and F shown in Fig. 1, where more serious damage to the grid will occur, and the greater chance of successfully launching attack will be achieved with less attack resources. The increased number of energy-acnodes in the grid will reduce the energy transmission cost because of the smaller number of demand-nodes and the quantity of demanded energy.

V. Performance Evaluation

We conduct performance evaluation based on the simplified version of the US smart grid [1] shown in Fig. 2. We select one major city of individual states as a node in the topology. The backbone of the interstate power transmission is based on the connection between these nodes. The fifty US states are selected as simulation objects, which are divided into five regions during the simulations as shown in Fig. 2. Note that such a simplified topology can validate our ideas and show the consequences of such threats. In the future, we will definitely conduct more evaluations on more real grids.

The data set used for the simulation is based on "2009 US Energy Information Administration State Electricity Profiles" [3]. To access the capacity of energy link, the averaged real-time data per second on each link, is computed based on averaged 2009 US interstate energy transmission data. The length of the energy link which represents the distance between two paired nodes is computed using Google map. Besides the number of compromised nodes, another parameter to measure the strength of attacks is the quantity of energy data to be manipulated.

To measure the impact of energy deceiving attacks, we consider the increased transmission cost, the user outage rate and supplied energy loss as the key metrics. The detailed definition of the metrics are listed as follows : (i) *Increased transmission cost:* It is defined as the increased total energy transmission cost caused by forged energy data, which is defined in Section IV.A-1. (ii) *User outage rate*: With the manipulated quantity of energy information, the total energy supply may not satisfy all the requests from the nodes, and some nodes will become outage to ensure the reliable energy support of other nodes in the grid. (iii) *Supplied energy loss*: The forged energy requests will make the waste of the energy supply. Our simulation data will focus on these metrics to evaluate the impact of attacks.

The energy transmission cost between two nodes can be derived by Equation (2) in [12]. All simulations in this paper were conducted using Matlab 7.0. We assume the energy threshold is 20 units power, which is the upper limit to avoid the detection. The energy threshold was defined as the upper limit of requested energy of a demand-node that the adversary

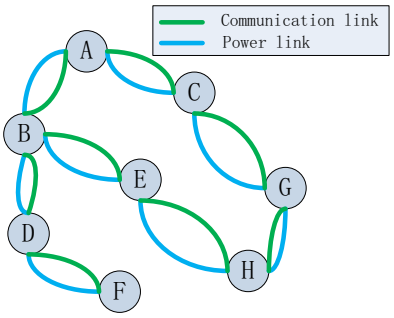

Fig. 1. A Graph Model of Smart Grid

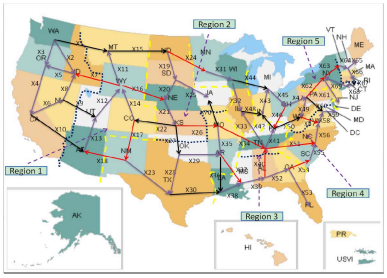

Fig. 2. The US Smart Grid Topology

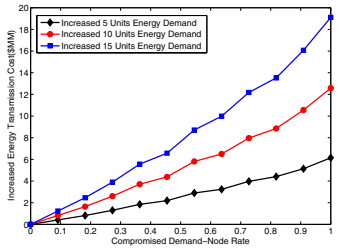

Fig. 3. Increased Energy Transmission Cost vs. Compromised Demand-Node Rate

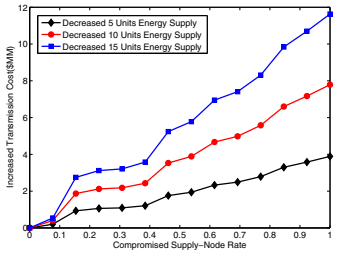

Fig. 4. Increased Energy Transmission Cost vs. Compromised Supply-Node Rate

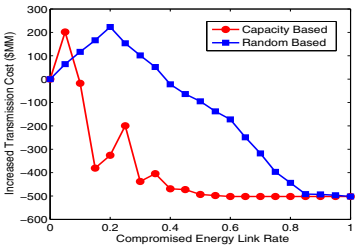

Fig. 5. Energy Transmission Cost vs. Compromised Energy Link Rate

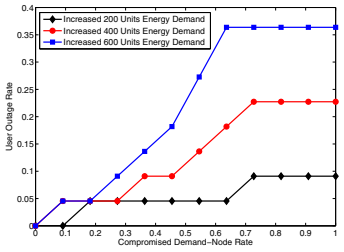

Fig. 6. User Outage Ratio vs. Compromised Demand-Node Rate

can forge, and the 20 units used here was obtained by the definition and experimental settings. When the total energy supply cannot satisfy the total energy demand, we ensure that the number of outage demand-nodes are minimal.

Impact on Increased Energy Transmission Cost: In this set of simulations, we designate 22 states of US as energy-demand states. Fig. 3 shows the impact of the compromised demand-node rate on the increased energy transmission cost. As we can see, with the increase in the compromised demand-node rate, the energy transmission cost increases almost linearly. The different curves in the figure show the different quantity of forged energy request. Obviously, the larger the quantity of energy request data to be manipulated, the more energy transmission cost is increased. When all demand nodes are compromised and forged 15 units energy request, there is $19.11\$MM$ cost increase. The result matches with the analytical result in Section IV.A-1.

When the energy-supply nodes are compromised, Fig. 4 depicts the impact of the compromised supply node rate on the increased energy transmission cost. As we can see, with the increase in the compromised supply-node rate, the energy transmission cost increases as well. When more quantity of energy data is manipulated to reduce the energy supply, the energy transmission cost becomes higher.

For forging the false state of energy links, Fig. 5 shows that when the link is claimed as invalid, the attack impact on the energy transmission cost. We can observe that, when the compromised energy link rate is small, the energy transmission cost grows linearly. With the increase in compromised energy link rate, energy transmission cost reduces because the number of energy-demand nodes and energy-supply nodes reduces. For example, Fig. 5 shows that the increased transmission cost would drop off, when 20% links are compromised. The data "20%" is obtained through the performance evaluation and it is related to network setting (e.g., topology and others). When all states of the links are manipulated as invalid, there is no energy transmission in the grid so the energy transmission cost will approach zero. As shown in Fig. 5, selecting compromised energy links based on capacity lead to more serious effect for transmission cost than selecting compromised links randomly, because randomly selecting compromised links will not always cause energy routing changes as we shown in Section IV.B-2.

Impact on User Outage Rate: The forged energy data will result in imbalance between energy-supply and energy-demand nodes. Fig. 6 depicts the user outage rate vs. the compromised demand-node rate. As we can see, when the quantity of energy data in the compromised node is small, the user outage rate is not significant. When the large energy requests caused by the attack, the user outage rate increases rapidly with the increase in the compromised demand-node rate. When all demand-nodes are compromised, 600 units demand is manipulated at each compromised node, the user outage rate approaches 36.3%.

Fig. 7 depicts the impact of user outage rate vs. the number of supply-nodes being compromised. When a small number of supply-nodes are compromised or the small quantity of energy supply is manipulated, the total energy supply can meet the total energy demand. Obviously, in the beginning of these curves in the figure, because there is no influence on demand-nodes, user outage rate is almost zero. When around 15% supply-node is compromised, the user outage rate increases rapidly.

Fig. 8 shows the user outage rate vs. the compromised energy link rate. As we can see, with the increase in the compromised energy link rate, the outage nodes increases smoothly at the beginning. This indicates that the small number of the energy links claimed as invalid has a little impact on the effectiveness of energy distribution process. Nevertheless, with the increase in the compromised energy link rate, more nodes cannot obtain enough energy from the grid, leading to more nodes becoming outage. When the compromised link ratio is around 30%, the user outage rate grows rapidly. It also shows

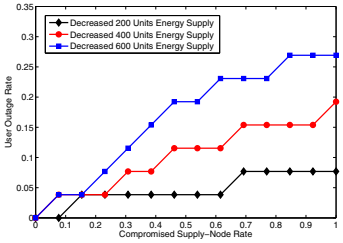

Fig. 7. User Outage Rate vs. Compromised Supply-Node Rate

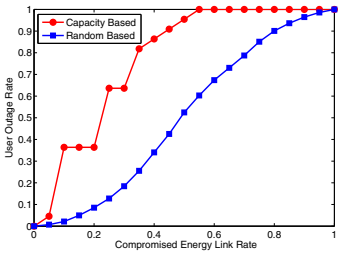

Fig. 8. User Outage Rate vs. Compromised Energy Link Rate

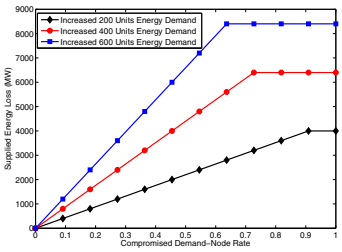

Fig. 9. Supplied Energy Loss vs. Compromised Demand-Node Rate

that selecting compromised energy links based on capacity leads to greater user outage rate than selecting compromised links randomly, which matches our analytical results well in Section IV.B-2.

Impact on Supplied Energy Loss: To investigate the impact on energy supply loss, we show the relationship between the supplied energy loss and the compromised demand-node rate in Fig. 9. When forged energy request increases, more energy is supplied to meet these forged energy requests. As we can see, the supplied energy loss increases in a linear fashion with the compromised demand-node rate. When the supplied energy loss grows to a point, it will stay in the same value. For example, for the 600 units demand manipulated in each node, when all the demand-nodes are compromised, the energy supply loss will be $8400MW$, which is the same supplied energy loss as the scenario, where 63.6% of demand-nodes are compromised. Because the quantity of the energy requests is manipulated, more demand-nodes are outage. When compromised demand-nodes become outage, the forged energy requests cannot be generated by these nodes.

VI. Conclusion

In this paper, we investigated the security of distributed energy routing process. We considered several attacks, in which the adversary may manipulate the quantity of energy supply, the quality of energy response, and the link state of energy transmission, respectively. We modeled and analyzed the impact of those attacks on the effectiveness of energy routing. Via extensive simulation, our data shows that our investigated attacks could significantly disrupt the effectiveness of energy distribution process. As an ongoing research topic, we plan to study the false charges to users due to the false data injection attacks and defense against those attacks.

Acknowledgment

The work was also supported in part by the following funding agencies in China: National 973 Basic Research Program of China under grant No. 2011CB302801, the Fundamental Research Funds for the Central Universities (xjj2011078), Xian industrial applied technology research project (CXY1017(4)). This work was also supported in part by US National Science Foundation (NSF) under grants CNS 1117175. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] http://www.oe.energy.gov/smartgrid.htm.
[2] NSF workshop on new research directions for future cyber-physical energy systems. Technical report, http://www.ece.cmu.edu/ nsf-cps/, Baltimore, MD, 2009.
[3] U. E. I. Administration. *State Electricity Profiles 2009*. http://www.eia.gov/, April 2011.
[4] R. Akella and B. M. McMillin. Information flow analysis of energy management in a smart grid. *Lecture Notes in Computer Science*, 6351:263–276, 2010.
[5] M. Baghaie, S. Moeller, and B. Krishnamachari, editors. *Energy Routing on the Future Grid: A Stochastic Network Optimization Approach*. Power System Technology (POWERCON), Oct. 2010.
[6] F. Cleveland. Cyber security issues for advanced metering infrastructure (AMI). In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.
[7] L. Jia, R.J.Thomas, and L. Tong, editors. *Malicious data attack on real-time electricity market*. 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), May 2011.
[8] T. Kim and H. Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326–333.
[9] S. Kirkpatrick, C. Gelatt, and M. P. Vecchi. Optimal by simulated annealing. *Science*, 220(4598):671–680, 1983.
[10] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang. Smart transmission grid: vision and framework, September 2010.
[11] H. Li, L. Lai, and S. Djouadi. Combating false reports for secure networked control in smart grid via trustiness evaluation. In *2011 IEEE International Conference on Communications (ICC)*, 2011.
[12] J. Lin, G. Xu, W. Yu, X. Yang, and S. Bhattarai. On distributed energy routing protocols in smart grid. In *http://pages.towson.edu/wyu/lxyybReportJuly2011.pdf*, 2011.
[13] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao. On false data injection attacks against distributed energy routing in smart grid. In *http://pages.towson.edu/wyu/lyyxzOctober2011.pdf*, 2011.
[14] Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, November 2009.
[15] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. In *Critical Information Infrastructures Security, vol. 6027 of Lecture Notes in Computer Science*, 2010.
[16] P. H. Nguyen, W. L. Kling, G. Georgiadis, and M. Papatriantafilou, editors. *Distributed routing algorithms to manage power flow in agent-based active distribution network*. Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES, Oct. 2010.
[17] H. Sandberg, A. Teixeira, and K. H. Johansson. On security indices for state estimators in power networks. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, 2010.
[18] K. Song, D. Seo, H. Park, H.Lee, and A. Perrig. Omap: One-way memory attestation protocol for smart meters. In *2011 Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW)*, 2011.
[19] D. Whitley. A genetic algorithm tutorial. *Statistics and computing*, 4:65–85, 1994.
[20] L. Xie, Y. L. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *Proceedings of 1st IEEE International Conference on Smart Grid Communications*, October 2010.
[21] H. Yi, H. Li, K. Campbell, and H. Zhu. Defending false data injection attack on smart grid network using adaptive cusum test. In *2011 45th Annual Conference on Information Sciences and Systems (CISS)*, 2011.
[22] Y. Yuan, Z. Li, and K.Ren. Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, 2(2):382–390, June 2011.