Towards Self-Healing Smart Grid via Intelligent Local Controller Switching under Jamming

Hongbo Liu, Yingying Chen
Department of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
{hliu3, yingying.chen}@stevens.edu

Mooi Choo Chuah
Department of CSE
Lehigh University
Bethlehem, PA 18015
chuah@cse.lehigh.edu

Jie Yang
Department of CSE
Oakland University
Rochester, MI 48309
yang@oakland.edu

***Abstract*—A key component of a smart grid is its ability to collect useful information from a power grid for enabling control centers to estimate the current states of the power grid. Such information can be delivered to the control centers via wireless or wired networks. We envision that wireless technology will be widely used for local-area communication subsystems in the smart grid (e.g., in distribution networks). However, various attacks with drastic impacts can be launched in wireless networks such as channel jamming attacks and DoS attacks. In particular, jamming attacks can cause a wide range of damages to power grids, e.g., delayed delivery of time-critical messages can prevent control centers from properly controlling the outputs of generators to match load demands. In this paper, we design a communication subsystem with enhanced self-healing capability under the presence of jamming through intelligent local controller switching. Our proposed framework allows sufficient readings from smart meters to be continuously collected by various local controllers to estimate the states of a power grid under various attack scenarios. In addition, we provide guidelines on optimal placement of local controllers to ensure effective switching of smart meters under jamming. Via theoretical, experimental and simulation studies, we demonstrate that our proposed system is effective in maintaining communications between smart meters and local controllers even when multiple jammers are present in the network.**

I. Introduction

Smart grid is proposed to improve the efficiency and reliability of existing power grids by adding automated monitoring, communication, self-diagnosis, and demand-response capabilities. Technically, the smart grid [1] can be divided into smart infrastructure, smart management, and smart protection systems. The smart infrastructure which supports bidirectional flow of electricity and information is further subdivided into smart energy, information, and communication subsystems [1]. The smart energy subsystem takes care of advanced electricity generation and delivery, whereas the smart information subsystem involves advanced metering, monitoring and management. The smart communication subsystem facilitates information exchanges among systems, devices, and applications.

We focus on the smart communication subsystem that is used to support smart information subsystem for distribution networks. Since among all available network technologies, wireless technology is promising as it eliminates efforts on the installation of wirelines, and also supports high-rate data transmissions, e.g., up to 100 Mbps in a range of 50 km with the IEEE 802.16 protocol [2]. Hence it is expected that the last mile of the communication subsystem, e.g., the communication between smart meters and controllers, will often be wireless in nature. Such a highly distributed wireless system in the smart grid makes it more vulnerable to various adversary attacks [3], [4]. In particular, jamming attacks aim to disrupt the data communication between smart meters and local controllers, which is considered as an important first step in an adversary's attempt to launch a variety of attacks. For instance, an adversary can delay or block smart meter reading collection and jam real-time price signals transmitted in the last mile to undermine the demand-respond system [5]. Even small-scale jamming attacks in local area networks can cause partial unavailability of data samples for state estimation [6], [7]. Furthermore, an attacker can launch a malicious jamming attack which prevents a substation from collecting complete data, and also simultaneously launch a false data injection attack to provide fabricated data to the substation. Such combined attacks can cause the substation to use the corrupted information for state estimation and result in producing the wrong control actions, causing dire consequences on the smart grid operations.

Compared to the legacy power systems, the smart grid operates in a more open communication network covering large geographical areas. Due to the critical importance of power infrastructures, resilience operation in communication networks is essential to sustain network availability. Given the large geographical coverage of the smart grid, eliminating jammers manually by dispatching technicians is resource consuming and less practical. The smart grid needs to have enhanced self-healing capability to maintain normal network operations in the presence of attacks. Thus, coping with jamming serves as the first line of defense to achieve reliable, secure, and real-time data delivery and customer management in the smart grid. Adopting the traditional channel hopping techniques [8], [9] in smart meters and local controllers is useful to alleviating jamming effects. However, smart attackers may adjust their jamming strategies based on the observations they gather from the on-going communications between smart meters and controllers. For example, a jammer with fast hopping speed can quickly identify the channel in use between smart meters and a local controller, making the employment of pure channel hopping scheme less effective. Therefore, more intelligent defense strategies need to be devised.

Our basic idea is to exploit all the available channels between smart meters and controllers that can be used to

978-1-4799-0895-0/13/$31.00 ©2013 IEEE

communicate and maintain data delivery rate under jamming. In this paper, we propose a framework that enables smart meters to identify nearby local controllers in addition to its primary local controller. It allows smart meters and local controllers to determine appropriate channels to communicate with one another when jamming is present. Our framework provides the enhanced flexibility, which allows smart meters to communicate with any nearby controllers that they can hear on any available channel, and hence increases the successful data delivery rate in the distribution network under jamming attacks. Through theoretical analysis, experimental study and simulation evaluation, we show that our framework is effective in allowing smart meters and controllers to continue their communications even under malicious attacks when multiple and colluded jammers are employed. Our work confirms the feasibility of effectively coping with jamming using intelligent local controller switching in the smart communication subsystem and is the first step towards providing the self-healing feature in a smart grid under adversarial conditions. Our main contributions in this paper are summarized as follows:

- We propose a framework which exploits intelligent controller switching together with channel hopping to provide resilience of data delivery under jamming in a distribution network.
- We build a testbed using Micaz motes implementing the proposed intelligent controller switching strategy to show the feasibility of such a framework.
- We conduct large-scale performance evaluations of our framework with multiple independent and colluded jammers using simulation studies.
- We analyze the optimal placement of local controllers to ensure effective switching of smart meters under jamming.

The rest of the paper is organized as follows. We put our work in the broader context in Section II. In Section III, we describe the smart grid network architecture and the attack model adopted in this work. We then present our proposed framework enabling intelligent local controller switching in Section IV. Next, we provide the theoretic analysis of our proposed strategy in Section V. We describe the testbed implementation of local controller switching with channel hopping and our experimental result in Section VI. The extensive performance evaluation is conducted through simulation in Section VII. In Section VIII, we analyze the the optimal coverage of local controller placement that supports intelligent local controller switching. Finally, we conclude our work in Section IX.

II. Related Work

Jamming attacks are serious security threats disrupting reliability of wireless communication, and have been extensively studied in wireless networks [8], [10]. For example, jamming attack detection was studied by Liu et al. [10] in the context of commodity wireless devices and wireless sensor networks. Besides jamming attack detection, spread spectrum techniques including both Frequency Hopping and (FH), Direct Sequence Spread Spectrum (DSSS) have been widely used to defend against jamming attacks in wireless communications [9], [11], [12] at the expense of advanced transceivers. In particular, Frequency-Hopping Spread Spectrum (FHSS) [9] technique transmits radio signals by switching among many frequency channels, using a pseudo-random sequence known to both transmitter and receiver, while direct Sequence Spread Spectrum (DSSS) [11], [12] spreads data over a wider bandwidth by multiplying the data (RF carrier) being transmitted and a Pseudo-Noise (PN) digital signal. Furthermore, several uncoordinated frequency hopping (UFH) schemes were proposed to enables the jamming-resistant communication in the presence of jamming attacks without a pre-shared secret [13]–[15].

Recently, a few work has been focused on studying jamming attack in the context of the smart grid applications. Li et al. discussed the Denial-of-Service (DoS) jamming of the wireless communication in the smart grid and studied the possibility of manipulating the power market by jamming the pricing signal [5], [16]. Lu et al. provided a study on the impact of jamming attacks against time-critical network applications (e.g. power grids), and observed that generating a fair amount of camouflage traffic in the network could minimize the message delay for the smart grid applications under jamming attacks [4], [17]. Different from the previous work, we focus on designing a self-healing communication subsystem with local controller switching that is robust against jamming attacks. Our work is novel in that we exploit all the available channels between smart meters and controllers to increase the data delivery rate under jamming.

III. System Overview

A. Smart Grid Network Architecture

In this work, we adopt the smart grid architecture described in [1] which consists of three major systems, namely smart infrastructure, smart management and smart protection systems.

We focus on the smart communication subsystem which supports the smart information subsystem within the smart infrastructure system for distribution networks as shown in Figure 1. Typically, such a communication subsystem is hierarchical in nature with devices within each geographical region forming different subnetworks. A typical smart grid communication subsystem consists of one or more substations, with each substation supervising the operations of multiple local controllers in a particular region. The substation is responsible for the information aggregation from all the local controllers. Each local controller interacts with multiple smart meters for supporting power consumption reading collection, operation data management, and data acquisition control. The smart meters within a geographical region communicate with a local controller via ZigBee-based radios while the local controllers communicate with one another via wireless mesh network. Furthermore, the local controllers communicate with the substation controller via power line communications or cellular networks. Thus, the smart grid communication subsystem comprises the ZigBee networks, the wireless mesh networks and the cellular networks

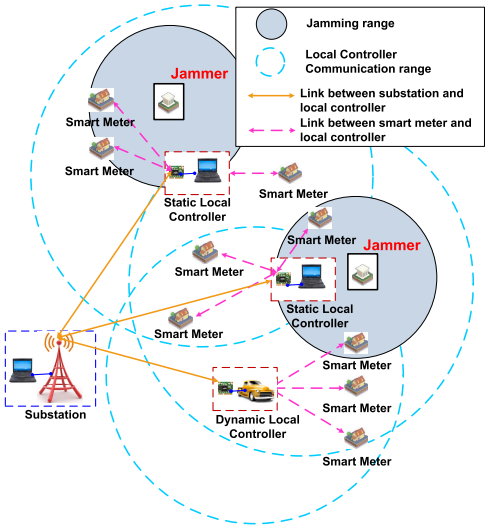


Fig. 1. Architecture of the smart grid distribution network and illustration of jammer deployment.

We assume that the smart grid communication subsystem is designed such that any smart meter can communicate with several local controllers, but it has only one primary local controller to which it delivers power consumption readings during normal operations. Smart meters do not communicate with one another. Under normal operations, a local controller broadcasts beacons in a particular channel and smart meters scan all channels to find nearby local controllers to associate with.

B. Attack Model

The shared nature of the wireless medium creates opportunities for adversaries employing jammers to disrupt data delivery between smart meters and local controllers in the smart grid, from delayed delivery of time-critical messages to complete denial-of-service [3], [18]. As the network has multiple channels, the jammer can adopt a wide range of strategies to disrupt message delivery. The attacker possesses the knowledge of the available channels between a local controller and smart meters under its coverage. Thus, a jammer could target a particular local controller to disrupt its communication. Furthermore, we assume that a jammer can only disturb the message communication in one channel at each time slot.

We consider two major jamming types: *random* and *reactive*. A random jammer randomly selects a channel used between a local controller and smart meters at each time slot and disrupts the data communication without monitoring the channel activities, while a reactive jammer monitors a channel and only launches the attack when there are activities on the channel.

In addition, we consider both single and multiple stationary jammers. With multiple jammers, we further consider independent versus colluded jammers. With multiple independent jammers, the communications between smart meters and local controllers in multiple channels could be disrupted at each time slot. Multiple colluded jammers can collaboratively launch an attack targeting a particular channel at a time slot, causing severe channel interference.

IV. Framework of Intelligent Local Controller Switching with Channel Hopping (LCS-CH)

Previous studies mainly rely on channel hopping techniques [8], [9], [14], [15] to mitigate jamming attacks in wireless networks. The basic idea of the channel hopping technique is: the communication between the sender and receiver at any particular time slot takes place using a particular channel chosen from a sequence of pre-defined channels (referred to as a *hopping sequence*), which are pre-loaded into communication devices. Typically communications between smart meters and local controllers are based on 802.15.4-equivalent radios which only have a fixed number of available channels. For a large deployment scenario where we need to consider having multiple local controllers operating on independent channels, each local controller can only be assigned a limited number of channels. Thus, despite the recent success of employing channel hopping techniques to achieve jamming resilient wireless communication, limited channel resources available on each local controller make the channel hopping technique insufficient to defend against jamming attacks in a smart grid. The jammers with fast hopping speed would make a pure channel hopping scheme less effective, since the jammer can quickly find the channel in use between the local controller and smart meters. Therefore, we propose a framework that actively performs local controller switching with channel hopping to thwart jamming attacks. With our proposed framework, a smart meter can utilize all available channels from nearby local controllers to send its readings, and hence increase the chances of such readings being successfully collected by one of the nearby local controllers under jamming, and subsequently by the substation.

A. Framework Design

In this work, we focus on alleviating jamming effects on smart meters and local controllers after an attack is detected. Thus, we assume that the network is able to detect the presence of jammers using existing techniques [8], [10]. For instance, the interference from jammers degrades the signal-to-noise ratio (SNR) of any received packet from a smart meter, the packet may not be decodable at the corresponding local controller. When a consecutive sequence of packets are undecodable, the network concludes that there is a jammer present. We propose a framework such that each smart meter is associated with a primary local controller and can also communicate with a set of nearby local controllers. Each local controller is preconfigured with a number of channel hopping sequences. The length of each channel hopping sequence is the same for all local controllers. The channel used in any particular time slot within a hopping sequence of a particular local controller does not overlap with any nearby local controllers. The channel hopping technique is triggered by the affected local controllers after a jamming attack is detected.

We assume that this communication subsystem runs as a time-slotted system, i.e. at each time slot, the local controller can decide which frequency channel it will use to communicate with smart meters that are associated with it. Our framework

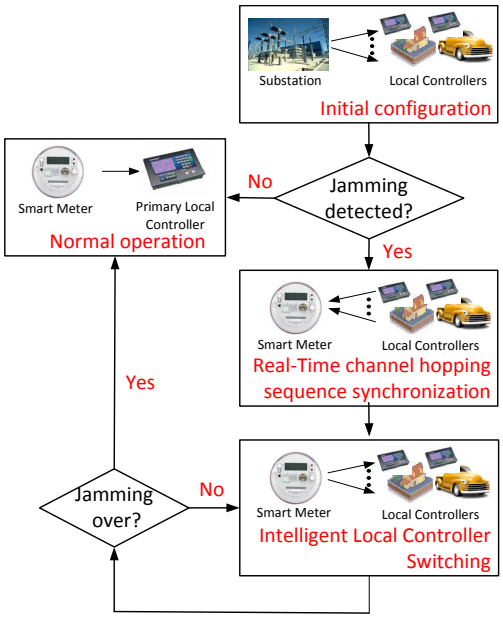


Fig. 2. Framework overview.

contains three main aspects: initial configuration in the smart grid, real-time channel hopping sequence synchronization between smart meters and the local controller under jamming, and intelligent local controller switching to alleviate jamming and increase successful data delivery rate.

Initial Configuration. All the channel hopping sequences are generated and distributed by the substation, which manages a set of local controllers. In our framework, we consider a hybrid deployment of *static* and *dynamic* local controllers. In particular, static local controllers are permanently placed by a utility company, while dynamic local controllers could be utility trucks driving around to collect data from smart meters. During the deployment of a static local controller, it is uploaded with a number of channel hopping sequences, which ensures that nearby local controllers have no collision with each other on channel hopping. The dynamic local controllers are also pre-configured with multiple channel hopping sequences.

Real-Time Channel Hopping Sequence Synchronization. When jamming is detected by the network by employing existing techniques [8], [10], smart meters and local controllers need to synchronize with each other to perform channel hopping. The affected local controllers (including both static and dynamic) utilize the one-time pseudo-random hopping pattern technique [14] to send out new beacons. Each new beacon message includes the channel hopping sequence, selected from the pre-configured set of channel hopping sequences, and the corresponding starting time of channel hopping. Such beacons are transmitted multiple times, each using a different pseudo-random hopping pattern, to ensure the information can be received by all the relevant smart meters.

Intelligent Local Controller Switching. Since smart meters have the opportunity to find more than one available local controllers in our framework, they can choose to switch to the appropriate nearby local controllers once they receive the channel hopping sequences from them. In our framework, each smart meter can actively decide which nearby local controller to connect to at each time slot, and hence increase the successful data delivery rate under jamming. In case no overlapping local controller is available for a particular smart meter, then only frequency hopping technique will be employed.

B. Collision-Free Channel Hopping Sequence Distribution

To defend against the jamming attack via the channel hopping technique, the substation constructs and distributes a set of channel hopping sequences to each local controller. The predefined hopping sequences among nearby local controllers should follow the collision-free principle, where any two channel hopping sequences have no interference with each other. The technique for constructing collision-free channel hopping sequences can be based on finite field theory from existing work [9]. To illustrate the collision-free channel hopping sequence distribution, we use an example when each local controller is assigned with only one channel hopping sequence. Assume 4 local controllers are deployed in the area of interest. There are a total of 20 available channels. Each local controller has one hopping sequence containing 5 channels for communicating with smart meters. The channel hopping pattern for these 4 local controllers can then be designed as follows:

$$\begin{array}{c} LC_1 \\ LC_2 \\ LC_3 \\ LC_4 \end{array} \begin{bmatrix} 1 & 5 & 9 & 13 & 17 \\ 2 & 6 & 10 & 14 & 18 \\ 3 & 7 & 11 & 15 & 19 \\ 4 & 8 & 12 & 16 & 20 \end{bmatrix}.$$

where each row corresponds to the channel hopping sequence of one particular local controller LC_i with $i = 1, \cdots, 4$ at different time slots; each column corresponds to the channels for 4 local controllers at one particular time slot t_j with $j = 1, \cdots, 5$.

When a jamming attack is detected, each affected local controller chooses from its pre-configured collision-free channel hopping sequence and starts sending out beacons by following a one-time pseudo-random hopping pattern [14]. The beacon message contains the local controller's identifier, the selected channel hopping sequence, and the starting time for channel hopping. The beacon message is transmitted multiple times by following different pseudo-random hopping patterns. Each transmission is independent of each other. Each affected smart meter randomly hops through all channels, and eventually it will have an overlapping channel with a local controller and receive the disclosed channel hopping sequence. Since each smart meter can communicate with several nearby local controllers, it is possible that the smart meter can receive the channel hopping sequence from multiple local controllers. However, merely using the channel hopping technique is not sufficient to maintain high data delivery rate under jamming as a jammer may follow the same procedure as smart meters to learn the channel hopping sequences in the affected area.

C. Intelligent Local Controller Switching with Channel Hopping (LCS-CH)

Our objective is to make use of all the available channels from nearby local controllers so as to maintain regular data delivery under jamming. To achieve this goal, we leverage the collaborative efforts from a smart meter's nearby local controllers. Instead of relying on the pure channel hopping technique, which has limited capability on defending against jamming attacks, we propose active local controller switching on top of channel hopping to increase successful data delivery rate.

We next describe how a smart meter comes up with a strategy to perform active local controller switching under jamming. Let us denote the channel hopping sequence F_i of the local controller LC_i as a k-length vector:

$$F_i = [f_{i,1}, f_{i,2}, \cdots, f_{i,j}, \cdots, f_{i,k}] \tag{1}$$

where $f_{i,j}$ corresponds to a particular channel in the frequency hopping sequence at jth time slot with $1 \leq j \leq k$. Considering all neighboring local controllers with collision-free channel hopping sequences, the smart meter defines its *channel selection* matrix as:

$$F_{I\times k} = \begin{bmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,k-1} & f_{1,k} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,k-1} & f_{2,k} \\ & \cdots & & \cdots & \\ f_{I,1} & f_{I,2} & \cdots & f_{I,k-1} & f_{I,k} \end{bmatrix},$$

where each row corresponds to the selected channel hopping sequence for one nearby local controller and again $f_{i,j}$ represents the channel at jth time slot of a neighboring local controller LC_i. The smart meter constructs $F_{I\times k}$ after real-time channel hopping sequence synchronization.

The smart meter then constructs the *controller switching* matrix $U_{I\times k}$ based on the channel hopping sequence received from nearby local controllers:

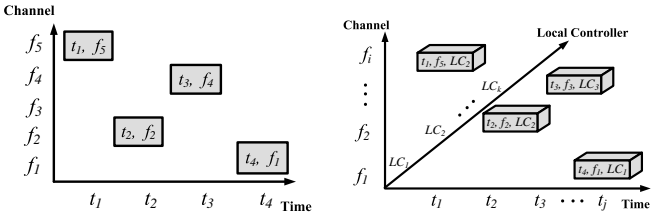
$$U_{I\times k} = [u_1, \cdots, u_j, \cdots, u_k], \tag{2}$$

where u_j represents a I-length column vector that has only one non-zero entry with $u_j^T u_j = 1$ and $j = 1, \cdots, k$ time slots. It represents which local controller is selected at jth time slot during channel hopping. Furthermore, $u_j(i) = 1$ indicates that the smart meter chooses ith local controller at jth time slot with $1 \leq j \leq k$. For instance, $u_2 = [00010]$ means the smart meter choose the fourth local controller at the second time slot.

Integrating the channel selection and controller switching matrices, the smart meter can then derive its channel hopping strategy as follows:

$$S_{1\times k} = 1_{1\times I}(F_{I\times k} \odot U_{I\times k}) \tag{3}$$

where $\odot$ represents element-wise product. Such a strategy ensures the smart meter finds an available channel to deliver data at any time slot under jamming. Although the jammers may have the capability to learn all the selected channel hopping sequences by eavesdropping in the affected area, jammers do not have the ability to jam all the channels at the same time. Figure 3 illustrates our intelligent local controller switching scheme. When only channel hopping is used as shown in Figure 3 (a), a smart meter hops among multiple channels of the primary local controllers. When there are multiple local controllers nearby, a smart meter can switch among these local controllers for data delivery. Using active local controller switching with channel hopping, a smart meter can take advantages of all available channels from different nearby local controllers as shown in Figure 3 (b).



(a) Channel hopping (b) LCS-CH

Fig. 3. Illustration of intelligent local controller switching scheme.

V. Analysis of Local Controller Switching with Channel Hopping (LCS-CH)

In this section, we derive the probability that a smart meter cannot deliver its data to a local controller under jamming. We refer such a probability as *jamming probability*. We compare the jamming probability when using merely channel hopping technique to applying local controller switching with channel hopping (LCS-CH) after the jamming attack is detected.

Under jamming, the received power at a local controller is from both the smart meter it communicates with (P_{LC_i,SM_j}) and the jammer ($P_{LC_i,J}$). We use a single jammer as an example and describe the received power at local controller LC_i using a log-distance path loss propagation model:

$$\begin{aligned} P_{LC_i,SM_j} &= P_T - PL_0 - 10\gamma 1og_{10}(\frac{d_{LC_i,SM_j}}{d_0}) - X_g \\ P_{LC_i,J} &= P_J - PL_0 - 10\gamma 1og_{10}(\frac{d_{LC_i,J}}{d_0}) - X_g, \end{aligned} \tag{4}$$

where P_T and P_J represent the transmission power of the smart meter and the jammer. X_g is a Gaussian random variable with distribution $N(0, \sigma^2)$, reflecting the attenuation caused by flat fading. $d_{LC_i,J}$ and d_{LC_i,SM_j} are the distances from smart meter and jammer to local controller respectively.

When the communication between the local controller LC_i and the smart meter SM_j on the channel f_k is disrupted by the jammer, the signal-to-noise ratio (at the local controller LC_i from smart meter SM_j) $SNR^k_{LC_i,SM_j}$ is less than a threshold γ_0. This signal-to-noise ratio can be represented as:

$$\begin{aligned} SNR^k_{LC_i,SM_j} &= P_{LC_i,SM_j} - P_{LC_i,J} \sim N(\mu, 2\sigma^2) \\ &\sim N(P_T - P_J - 10\gamma 1og_{10}(\frac{d_{LC_i,SM_j}}{d_{LC_i,J}}), 2\sigma^2). \end{aligned} \tag{5}$$

Then the possibility that a jammer successfully disrupts the communication between SM_j and LC_i on channel f_k depends on the propagation model. And the jamming probability can be

represented as:

$$Prob(SNR^k_{LC_i,SM_j} < \gamma_0) = \int_{-\infty}^{\gamma_0} \frac{1}{2\sigma\sqrt{\pi}} e^{-\frac{(SNR^k_{LC_i,SM_j} - \mu)^2}{4\sigma^2}}. \quad (6)$$

When only the traditional frequency hopping technique is used under jamming, SM_j can communicate with its primary local controller LC_i through a set of independent channels from the selected channel hopping sequence. The jamming probability $Prob(SM_j)^{CH}$ between LC_i and SM_j at time slot t can then be derived as:

$$\begin{aligned} &Prob(SM_j)^{CH} \\ =&Prob(\, f^J(t) = f_k \;\&\; f^{SM_j}(t) = f_k \Big|\, SNR^k_{LC_i,SM_j} < \gamma_0) \\ &\times Prob(SNR^k_{LC_i,SM_j} < \gamma_0) \\ =&Prob(f^J(t) = f_k) Prob(f^{SM_j}(t) = f_k) Prob(SNR^k_{LC_i,SM_j} < \gamma_0) \\ =&\frac{1}{N_i \times n} \int_{-\infty}^{\gamma_0} \frac{1}{2\sigma\sqrt{\pi}} e^{-\frac{(SNR^k_{LC_i,SM_j} - \mu)^2}{4\sigma^2}}, \end{aligned} \quad (7)$$

where $f^J(t)$ and $f^{SM_j}(t)$ represent the channels used by the jammer and smart meter SM_j at time slot t. n indicates the number of channels that the jammer tries to disrupt, and N_i is the total number of channels in the selected hopping sequence on LC_i. f_k is one of the available channels on single local controller.

When our proposed LCS-CH framework is applied, the smart meter SM_j actively perform local controller switching. Assume there are I nearby local controllers (with $LC_i, i = 1, \cdots, I$) available for the smart meter SM_j to switch independently. The jamming probability $Prob(SM_j)^{LCS-CH}$ for SM_j becomes:

$$\begin{aligned} &Prob(SM_j)^{LCS-CH} \\ =&\sum_{i=1}^{I} Prob(\, f^J(t) = f_k \;\&\; f^{SM_j}(t) = f_k \Big|\, SNR^k_{LC_i,SM_j} < \gamma_0) \\ &\times Prob\left(SNR^k_{LC_i,SM_j} < \gamma_0 \Big|\, LC_i\right) \times Prob(LC_i) \end{aligned} \quad (8)$$

The first term in equation 8 represents the jamming probability for a single local controller, which is the same as equation 7. In addition, the probability for a particular smart meter switching among I local controllers can be represented as $Prob(LC_i) = \frac{1}{I}$. Therefore, we can further derive as follows:

$$\begin{aligned} &Prob(SM_j)^{LCS-CH} = \sum_{i=1}^{I} \frac{1}{n \times N_i} Prob(SNR^k_{LC_i,SM_j} < \gamma_0) \times \frac{1}{I} \\ =&\frac{1}{I \times n} \sum_{i=1}^{I} \left(\frac{1}{N_i} \int_{-\infty}^{\gamma_0} \frac{1}{2\sigma\sqrt{\pi}} e^{-\frac{(SNR^k_{LC_i,SM_j} - \mu)^2}{4\sigma^2}} \right) \\ <&Prob(SM_j)^{CH}. \end{aligned} \quad (9)$$

Therefore, the jamming probability of a smart meter under the LCS-CH scheme is lower than that under the CH scheme. And smart meters have higher possibility to deliver the data successfully to local controllers.

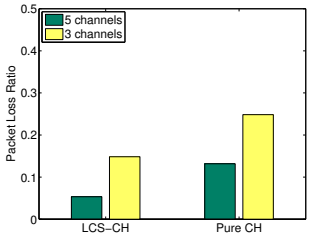


Fig. 4. Experimental Evaluation of LCS-CH in ZigBee Network

VI. Implementation of Controller Switching Scheme in ZigBee Network

The smart communication subsystem for smart meters and local controllers is usually deployed using a ZigBee network [1]. It is thus essential to show the feasibility of applying the proposed local controller switching scheme in the ZigBee network besides providing theoretical analysis for our framework in Section V. We build a testbed using MicaZ motes that implement our local controller switching scheme and evaluate its performance when a jammer is present. MicaZ sensor nodes have a $2.4 - 2.48GHz$ Chipcon $CC2420$ Radio and communicate using the ZigBee protocol.

A. Testbed Setup

Our testbed consists of 6 motes with 4 acting as smart meters ($SM_j, j = 1, \cdots, 4$) and 2 as local controllers ($LC_i, i = 1, \cdots, 2$), and a 7th mote deployed as a jammer. The two local controllers can forward the collected data from smart meters to the substation, which is represented by a mote base-station. Each smart meter communicates to one primary local controller with SM_2 and SM_3 covered by both local controllers. During our experiments, the jammer transmits with a higher transmission power ($7dBm$) than smart meters ($5dBm$). Two testing scenarios with each local controller having 3 and 5 available channels respectively are conducted.

B. Implementation and Results

We implement LCS-CH on motes and compare it with pure channel hopping technique. We emulate two operating scenarios in the smart grid under jamming: (1) smart meters communicate with their primary local controllers using a predefined channel hopping sequence; and (2) smart meters actively switch between local controllers using their respective channel hopping sequences. During testing, we allow the system to operate using pure channel hopping and LCS-CH schemes for 5 minutes each with a packet sending rate from the smart meter set at $4pkt/sec$. We then examine the packet loss ratio at the substation. The results are presented in figure 4. We observe that our proposed LCS-CH scheme significantly outperforms pure channel hopping scheme with much lower packet loss ratio under jamming with over 40% and 60% improvement for 3 and 5 channel cases respectively. This small-scale testbed study confirms the feasibility of implementing local controller switching technique in the ZigBee network.

VII. Simulation Evaluation

In this section, we evaluate the effectiveness of our LCS-CH scheme under different types and different numbers of jammers through a simulated smart grid communication subsystem.

A. Simulation Setup

We simulate a smart grid communication subsystem in a $500m \times 500m$ area, where 200 smart meters are deployed with 40 and 60 local controllers, respectively. We adopt the log-normal shadowing model for signal propagation and the parameters are set following a typical outdoor environment [19]: $PL_0 = 4$, $\gamma = 0.6$, $d_0 = 5$ and X_g is the shadow fading which follows the zero mean Gaussian distribution with the variance varying from 0 to $3dBm^2$. The default transmission power of jammers is $20dBm$, while it is $17dBm$ for smart meters. Each local controller is assigned with 5 channels. The SNR threshold is set to $3dB$ for jamming detection. We set the jammer hopping rate as $12pkt/sec$, which is three times that of a smart meter's hopping rate (i.e., $4pkt/sec$). In our simulation, we consider both random and reactive jammers with different deployment numbers when present in the network: single and multiple. For multiple jammers, we study both independent and colluded jammers and use two jammers as a representative example. To obtain the statistic results, each scenario is run for $10,000$ times.

B. Metrics

We define Jammed Slot Ratio (JSR) to evaluate the effectiveness of our proposed LCS-CH scheme. We first define $\kappa_i(t)$ as the status (i.e., jammed or not jammed) at the smart meter SM_i during time slot t:

$$\begin{aligned} \kappa_i(t) &= 1 \quad jammed; \\ \kappa_i(t) &= 0 \quad not\ jammed. \end{aligned} \tag{10}$$

We further use $\kappa_i^s(t)$ to represent the status of the smart meter SM_i at time slot t when our proposed LCS-CH scheme (i.e., with local controller switching) is applied.

The JSR is then defined as the ratio between the number of jammed time slots to the number of un-jammed ones of the smart meter under jamming is present.

Jammed Slot Ratio (JSR). When LCS-CH is applied, the JSR is represented as:

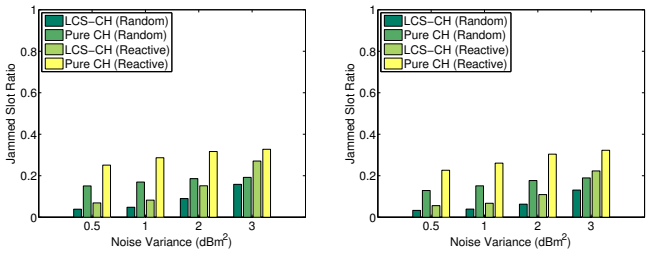
$$JSR^s = \frac{\sum_{t=1}^{T}\sum_{i=1}^{M}\kappa_i^s(t)}{M \times T}, \tag{11}$$

where T is the total number of time slots under study and M is the number of smart meters. Similarly, when only the channel hopping (CH) technique is applied, the JSR becomes:

$$JSR = \frac{\sum_{t=1}^{T}\sum_{i=1}^{M}\kappa_i(t)}{M \times T}. \tag{12}$$

Improvement Percentage (η). We further define the JSR improvement percentage, which represents the percentage of jamming slot ratio reduced under the LCS-CH scheme when compared with the pure channel hopping scheme, as:

$$\eta = \frac{JSR - JSR^s}{JSR}. \tag{13}$$



(a) 40 LCs (b) 60 LCs

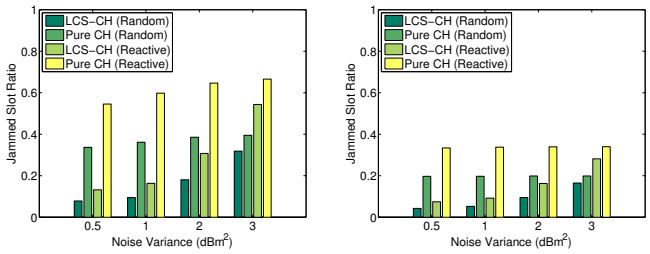
Fig. 5. Single jammer case: Comparison of Jammed Slot Ratio (JSR) between LCS-CH and Pure CH.

C. Results

1) Single Jammer case: We first study the performance of our proposed framework when a single jammer is present. Figure 5 (a) and (b) depict the JSR comparison between the proposed LCS-CH scheme and pure frequency hopping (i.e., Pure FH) scheme under both random and reactive jammers when the variance of shadowing is varied from $0dBm^2$ to $3dBm^2$ with 40 and 60 local controllers, respectively. We observe that the JSR of the LCS-CH scheme is substantially less than that of the pure FH scheme under both 40 and 60 local controllers settings. This observation indicates that the proposed scheme has a much lower jammed slot ratio, and thus has significantly performance improvement over the Pure FH scheme. Specifically, JSR drops from 17.1% (15.1%) to 4.8% (3.9%) with 40 (60) local controllers when the variance of shadowing is $1dBm^2$ under random jamming. Similarly, for the reactive jammer, JSR drops from 29% (26%) to 8.3% (6.7%) with 40 (60) local controllers when the variance of shadowing is $1dBm^2$. This is because the proposed LCS-CH scheme provides more flexibility on channel hopping among multiple local controllers. It is thus harder for a jammer to disrupt the communication between smart meters and local controllers. We also find that the JSR of the proposed scheme under 60 local controllers is smaller than that of under 40 local controllers, indicating each smart meter having more choices for channel switching when more local controllers are deployed.

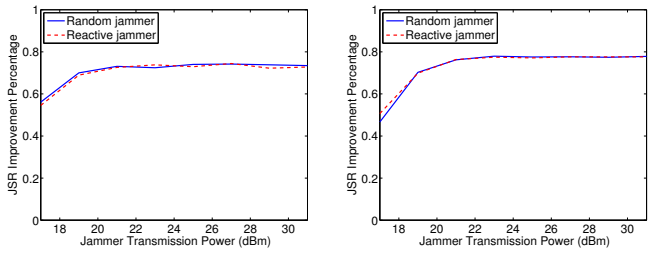
Furthermore, we observe that the JSR is increasing as the noise power (i.e., variance of shadowing) increases. This is because a higher noise power results in a lower signal-to-noise ratio, which affects the communication between local controllers and smart meters even in normal conditions. This causes the decreasing of the number of local controllers that a smart meter can communicate with, especially those which are located relatively farther away from the smart meter. When the noise power is large enough (e.g., larger than $3dBm^2$), the smart meter could only maintain the communication with its primary local controller (assuming the primary local controller is the closest controller to the smart meter). This will make the JSR under the LCS-CH scheme approaching to that of Pure FH scheme. But still, the performance of LCS-CH is better than that of Pure FH scheme.

Additionally, we find that the reactive jammer is more harmful than the random jammer. Once the reactive jammer captures one active channel, it could disrupt all the packets transmitted during the whole time slot. This is different from



(a) Independent jammers (b) Colluded jammers

Fig. 6. Two jammers case: Comparison of JSR between LCS-CH and Pure CH with 40 local controllers.



(a) 40 LCs (b) 60 LCs

Fig. 7. The JSR improvement percentage for single jammer under different jammer transmission power with 40 and 60 local controllers, respectively.

a random jammer, who only disrupts the communication in a portion of one time slot due to the fast hopping rate of jammers. Therefore, the JSR under a reactive jammer is higher than that of a random jammer.

2) Multiple Independent Jammers case: We next examine how our framework reacts when there are multiple independent jammers present in the smart grid communication subsystem. Figure 6(a) presents the JSR comparison of the proposed LCS-CH scheme and pure FH scheme when two jammers are present with 40 local controllers. We observe that the JSR of the LCS-CH scheme is significantly lower than that of the pure FH scheme for all studied cases using random and reactive jammers respectively. As expected, when compared to the single jammer case, the JSR of pure FH scheme increases sharply under two jammers case due to more channels are affected by multiple jammers. The JSR of our proposed LCS-CH under two jammers is about twice of that under a single jammer case. This is because having two jammers independently disrupt the channels on a local controller results in similar performance as the summation of JSRs from two independent jamming scenarios with a single jammer. The performance under 60 local controllers exhibits better performance than the 40 local controllers case but was omitted due to space limitation.

3) Multiple Colluded Jammers Case: We further examine the case with multiple colluded jammers in the smart grid communication subsystem. The JSR comparison of the proposed LCS-CH scheme and pure FH scheme under two colluded jammers with 40 local controllers are presented in figure 6 (b). The performance under 60 local controllers is again omitted due to space limitation. We find that the JSR of our proposed LCS-CH is much better than that of pure FH. When compared to the JSR under a single jammer, we observe that the JSR of LCS-CH under two colluded jammers increases about only 0.5%, which indicates that colluded jammers have accumulated impact on the channels between smart meters and local controllers. Since the two jammers are randomly distributed in the testing area, the accumulated impact is not that obvious compared with a single jammer case. It also shows the robustness of our proposed LCS-CH scheme when dealing with colluded jammers. Further, we observe that having two colluded jammers is less harmful than having two independent jammers for both LCS-CH and Pure FH schemes from our simulation results.

4) Impact of Jamming Power: Finally, we study how our proposed framework behaves when the jammer's transmission power increases. We vary the jammer's transmission power from $17dBm$ to $30dBm$, while maintaining the transmission power of smart meters at $17dBm$ with constant noise power level set at $1dBm^2$. Figure 7 depicts the JSR improvement percentage of LCS-CH over Pure FH with both a single random and reactive jammer cases respectively the transmission power of the jammer is varied. We observe that our LCS-CH achieves large JSR improvement (over 50%) under different number of local controllers for both random and reactive jammers. This is very encouraging as it indicates our framework is highly effective when the adversary increases the jammer's transmission power. The JSR improvement becomes stable beyond $22dBm$ of jammer transmission power. This is because the jammers with low transmission power have limited impact on the signal-to-noise ratio of the communication links between smart meters and local controllers. They can mostly affect the communication links between a smart meter and far away controllers. When the jamming power increases, more communication links will get affected. Once the transmission power of jammer becomes large enough, the communication links between the smart meter and all the local controllers will get affected resulting in low SNR if they are on the same channel as the jammer. As the jamming power increases, the jamming capability becomes saturated.

VIII. Optimization of Local Controller Placement

The deployment of smart meters in a geographical area is usually fixed. Given the total number of local controllers planned in this geographical area, it is useful to perform the deployment in such a way that each smart meter can communicate with the maximum number of nearby controllers to facilitate active local controller switching under jamming. To address this challenge in the self-healing smart grid, our framework proposes the optimal placement of a fixed number of local controllers to maximize the overlapping coverage of each smart meter.

Assume there are M smart meters and I local controllers in a specific geographic region. We formulate the smart grid communication subsystem network in this region into a connected, undirected graph, which is represented by a *neighborhood adjacency matrix* $C_{I\times M}$ between smart meter and local controller as follows:

$$C_{I\times M} = \begin{bmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,M} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,M} \\ & \cdots & \cdots & \\ l_{I,1} & l_{I,2} & \cdots & l_{I,M} \end{bmatrix},$$

where each element of the graph $l_{i,j}$ (with $i = 1, \cdots, I$ and $j = 1, \cdots, M$) represents a communication link between a local controller LC_i and a smart meter SM_j under normal operations. When a smart meter SM_j can communicate with a local controller LC_i, the corresponding element $l_{i,j}$ in the matrix $C_{I\times M}$ is 1, otherwise it is 0.

Whether a smart meter SM_j is covered or not by a local controller LC_i depends on the signal propagation model and the distance between them. The received power at the local controller LC_i should exceed the predefined threshold γ_0, which guarantees successful packet delivery. Therefore, the communication link $l_{i,j}$ should satisfy the following condition:

$$l_{i,j} = \begin{cases} 1 & P_{LC_i,SM_j} > \gamma_0; \\ 0 & otherwise; \end{cases}$$

$$P_{LC_i,SM_j} = P_T - PL_0 - 10\gamma 1og_{10}(\frac{\left\|q_i^{LC} - q_j^{SM}\right\|}{d_0}) - X_g, \tag{14}$$

where q_j^{SM} (with $j = 1, \cdots, M$,) and q_i^{LC} (with $i = 1, \cdots, I$,) represent the position of a smart meter SM_j and local controller LC_i respectively.

Our objective is to find the optimal placement of the I local controllers with positions $q_i^{LC}, i = 1, \cdots, I$, in the network such that each smart meter can be covered by at least k local controllers. Therefore, the optimization problem of local controller placement can be formulated as:

$$\begin{aligned} &\underset{q_i^{LC}, i=1,\cdots,I}{\textbf{arg max}}\ 1_{1\times I} C_{I\times M} 1_{M\times 1} \\ &s.t.\ \ 1_{1\times I} C_{I\times n} v_j \geq k \end{aligned} \tag{15}$$

where $1_{1\times I}$ and $1_{M\times 1}$ are I-length column and M-length row vector with all 1's elements. v_j is a M-length column vector with only jth element equals to 1 and all other elements are 0. Note that the positions of smart meters q_j^{SM} are known.

Equation 15 searches for the optimal positions of all local controllers, LC_i, until the summation of all the link state $l_{i,j}$ in the neighborhood adjacency matrix $C_{I\times M}$ is maximized. To avoid the optimization process from falling into a local optimal solution, we enforce that each smart meter should be covered by at least k local controllers. This optimization problem of searching for the positions of local controllers can be solved using the integer programming technique [20]. The optimal placement of local controllers serves as inputs into our proposed framework to facilitate intelligent local controller switching under jamming.

IX. Conclusion

Jamming attacks in the last mile of the smart grid aim to disrupt the data communication between smart meters and local controllers and further launch a variety of adversarial activities. We exploit local controller switching to provide resilience of data delivery under jamming in the distribution network. The proposed framework enables smart meters to utilize all the available channels from nearby local controllers to ensure successful data delivery. Theoretic analysis shows that our proposed intelligent local controller switching with channel hopping (LCS-CH) scheme reduces the jamming probability compared to the pure channel hopping approach. Furthermore, our testbed using MicaZ motes shows the feasibility of implementing the intelligent local controller switching scheme in a ZigBee network. And our large-scale simulation results confirm the effectiveness of our approach even when multiple jammers are present. Finally, we provide a guideline on the optimal placement of local controllers to ensure effective switching of smart meters under jamming, leading toward a self-healing communication subsystem in the smart grid. In our future work, we may design a mechanism for negotiating dynamic channel hopping sequences.

Acknowledgements: Yingying Chen would like to acknowledge the support by NSF grant CNS-0954020. Mooi Choo Chuah would like to acknowledge the support by Lehigh Startup Grant.

References

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *IEEE Communications Surveys Tutorials*, 2012.

[2] "WiMax 802.16 Tutorial," http://www.radio-electronics.com/info/wireless/wimax/wimax.php.

[3] T. Goodspeed, S. Bratus, R. Melgares, R. Speers, and S. W. Smith, "Apido: Tools for exploring the wireless attack surface in smart meters." in *HICSS*, 2012.

[4] Z. Lu, W. Wang, and C. Wang, "Hiding traffic with camouflage: Minimizing message delay in the smart grid under jamming," in *IEEE INFOCOM*, 2012.

[5] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *IEEE GLOBECOM*, 2011.

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

[7] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *IEEE SmartGridComm*, 2010.

[8] A. Wood, J. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," in *IEEE SECON*, 2007.

[9] Q. Zeng, H. Li, Z. Zhang, and D. Peng, "A frequency-hopping based communication infrastructure for wireless metering in smart grid," in *IEEE CISS*, 2011.

[10] D. Liu, J. Raymer, and A. Fox, "Efficient and timely jamming detection in wireless sensor networks," in *IEEE MASS*, 2012.

[11] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: Jamming-resistant wireless broadcast communication," in *IEEE INFOCOM*, 2010.

[12] B. DeBruhl and P. Tague, "Mitigation of periodic jamming in a spread spectrum system by adaptive filter selection," in *PECCS*, 2012.

[13] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Symposium on Security and Privacy*, 2008.

[14] A. Liu, P. Ning, H. Dai, and Y. Liu, "USD-FH: Jamming-resistant wireless communication using Frequency Hopping with Uncoordinated Seed Disclosure," in *IEEE MASS*, 2010.

[15] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated FHSS anti-jamming communication," in *ACM MobiHoc*, 2009.

[16] H. Li, L. Lai, and R. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *IEEE CISS*, 2011.

[17] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *IEEE INFOCOM*, 2011.

[18] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, 2006.

[19] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[20] S. Yang, F. Dai, M. Cardei, and J. Wu, "On multiple point coverage in wireless sensor networks," in *IEEE MASS*, 2005.