IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 14, 2017, accepted April 10, 2017, date of publication April 18, 2017, date of current version May 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2695520

Impact of the Wireless Network's PHY Security and Reliability on Demand-Side Management Cost in the Smart Grid

AHMED EL SHAFIE[1], (Member, IEEE), DUSIT NIYATO[2], (Fellow, IEEE), RIDHA HAMILA[3], (Senior Member, IEEE), AND NAOFAL AL-DHAHIR[1], (Fellow, IEEE)

[1]Electrical Engineering Department, The University of Texas at Dallas, Richardson, TX 75080-3021, USA
[2]School of Computer Engineering, Nanyang Technological University, Singapore 639798
[3]Electrical Engineering Department, Qatar University, Doha 2713, Qatar

Corresponding author: Ahmed El Shafie (ahmed.salahelshafie@gmail.com)

This work was supported by the NPRP from the Qatar National Research Fund (a member of Qatar Foundation) under Grant NPRP 8-627-2-260. The statements made herein are solely the responsibility of the authors.

ABSTRACT We investigate the impact of the wireless network's physical layer (PHY) security and reliability on demand-side management operation in the smart grid. We assume that consumers communicate their energy demands with the utility, and we investigate the tradeoff between the wireless network's PHY security and reliability. We consider passive and active attacks on the smart grid, and show their impacts on both the wireless communications system's reliability and security. To improve the wireless communications system's security, we propose an artificial-noise (AN)-aided scheme for orthogonal-division multiplexing-based wireless systems. We show that increasing the PHY security of the legitimate transmissions decreases the communication reliability between the smart meters and the meter data-management system since to secure the transmissions, a portion of the transmit powers will be assigned to AN signal transmissions. To further secure the smart meters' transmissions and enhance their reliability, we propose a new encoding scheme where the data are encoded over the available smart meters' communication (i.e., non-idle) times in a given hour.

INDEX TERMS Active and passive attacks, artificial noise, DSM, OFDM, security.

I. INTRODUCTION

The smart grid (SG) modernizes the aging energy grid by making it more efficient. Secure and reliable two-way communication networks are central to the SG to enable automation, active operation, and efficient demand response. In particular, wireless communications will play an important role in measuring the status (e.g. energy-consumption, alarm, voltage-fluctuation, and damage to power equipment) from different devices (e.g. substations, smart meters, and sensors), and in exchanging information and control signals between the different system components to support continuous, reliable and secure SG operation.

Demand-side management (DSM) refers to algorithms and programs performed by the utilities to control the energy flow and consumption at the consumer side and use the available energy more efficiently without installing a new generation and transmission infrastructure. The SG's wireless communications system must be able to operate under the failure of some of its components (e.g. gateways and wireless smart meters) so that the impact of this failure on the performance of the electrical grid is minimized.

A. RELATED WORK

Reliability analysis of the SG's wireless communications system determines how long the energy generation, transmission, distribution, and consumption tasks will perform efficiently given the target performance requirements. A smart meter is assumed to be installed in each house to estimate and schedule the energy-consumption of electric appliances [1], [2]. A service area is assumed to be divided into multiple subareas where in each subarea, there are multiple houses using electric appliances. Reliability analysis has been applied to wireless networks [3]–[5], conventional control and information networks for energy systems [6], [7], and wide-area measurement systems (WAMS) in the SG [5], [8]. Reliability analysis of the SG wireless communications system that supports DSM, which is generally implemented by a utility as part of the advanced metering

infrastructure (AMI), was performed in [9]. Moreover, in [9], the cost due to the unavailability and redundancy of such a system were investigated.

There has been an increasing interest in SG security analysis, see, e.g., [10]–[12]. In [10], the authors provided an overview of the issues related to the SG architecture including its security. In [11], the authors presented a cyber-physical security overview of the SG communication infrastructure. In [12], the author presented security threats for electric vehicle networks. The SG security attacks are either passive attacks such as eavesdropping and traffic analysis, or active attacks such as denial-of-service (DoS) attacks [13]. Passive attacks attempt to access the information exchanged within a network, while active attacks disrupt the normal functionality of a network. Essentially, these attacks impact the most basic security service requirements in the SG, namely: (1) availability (blocking the communications between the utility and the consumers); (2) confidentiality (preventing the attackers from obtaining private information); (3) integrity (blocking unauthorized users from changing the data); and (4) authenticity (validating a user's identity).

Security of a shared medium is a critical issue since an eavesdropping node can infer and analyze the identity of the communicating nodes. Moreover, an eavesdropper can obtain important information regarding the activity and data shared between these legitimate nodes. Hence, many research efforts have been carried out to analyze and investigate the physical layer (PHY) security of the wireless communication systems due to their broadcast nature. The secrecy of communications between two legitimate parties in an information-theoretic sense was first investigated in the seminal work of Wyner [14] which is known as the PHY security. The system's PHY security is measured by the secrecy capacity of the link connecting the legitimate parties, which represents the maximum rate of the legitimate parties with zero information leakage at the eavesdropping node.

The authors of [15] derived the secrecy capacity for orthogonal frequency-division multiplexing (OFDM) systems. In [16], the authors defined the system's security as a lower-bound on the minimum mean squared error between the transmitted and decoded data at the eavesdropping node. The authors of [17] modeled the OFDM wiretap channel as a special instance of the multiple-input multiple-output (MIMO) wiretap channel and its secrecy rates were studied for asymptotically high and low signal-to-noise ratio (SNR) regimes.

Linear precoding for PHY security was investigated in several recent publications such as [18]–[22]. The authors of [18], under the optimistic assumption of global channel state information (CSI) knowledge at the transmitting node, proposed an efficient Vandermonde precoding scheme that enables the transmitter to send the information signal in the null space of the equivalent eavesdropper's MIMO channel matrix. In [19], the power-allocation scheme for artificial noise (AN)-aided precoding transmissions was investigated. Unlike [18], the legitimate transmitter was assumed to have perfect CSI of the link to its legitimate receiver and knows only the statistics of the potential eavesdropper's CSI. In [20], the author investigated the PHY security of MIMO wiretap channels. He proposed to guarantee a predefined signal-to-noise ratio (SNR) for successful decoding at the legitimate receiver, and then allocate the remaining transmit power for AN injection to degrade the eavesdropper's channel.

The authors of [23] investigated temporal AN injection for the single-input single-output single-antenna eavesdropper (SISOSE) OFDM system where a precoded time-domain AN signal is added to the data signal before transmission. Extensions of the problem presented in [23] were proposed in [24] and [25]. The authors of [24] investigated a temporal AN injection scheme for the multiple-input multiple-output multi-antenna eavesdropper (MIMOME) OFDM system, whereas the authors of [25] proposed a hybrid spatio-temporal AN for MIMOME-OFDM systems.

Active malicious attacks such as denial-of-service (DoS) [26] and data-injection attacks [27] have a severe impact on the communications system. In particular, the DoS attack, which blocks the communication between legitimate nodes, is the most accomplishable [26], [28], [29] and is realized by injecting a jamming interfering signal within the information signal transmission bandwidth [30]. In [26], [31], and [32], the authors investigated linear quadratic Gaussian (LQG) control cost function problems under DoS attack. The authors of [26] proposed a semi-definite programming-based solution to obtain a feedback controller that minimizes a cost function subject to energy constraints. Reference [31] investigated the scenario where a controller communicates with a plant in the presence of an adversary jammer and modeled the problem as a zero-sum game between the controller and the jammer. The authors of [32] derived an event-trigger control strategy in the presence of an energy-limited periodic jamming attacker.

B. CONTRIBUTIONS

The contributions of this paper are summarized as follows:

- Motivated by the importance of reliable communications between the smart meters and the meter data-management system (MDMS) (see Fig. 1) and the critical need to analyze the SG network under security constraints of active and passive attacks, we investigate the impact of the PHY security and reliability of the wireless communications link on DSM operation. The passive attacks can reduce reliability since the smart meters will use portion of their transmit powers to inject AN to increase the secrecy rate, which is defined as the number of bits that can be sent securely to the legitimate receiver without any information leakage at the passive eavesdropping attackers.
- We propose an AN-aided transmission scheme to mitigate the passive eavesdropping attacks and optimize the power fraction assigned to data and AN to increase the secrecy rate. By varying this power fraction, we study the tradeoff between reliability and PHY security of

the communications between the smart meters and the MDMS.

- To further secure the wireless communications system and enhance its reliability, we propose a new encoding scheme where the data is securely encoded over the smart meters' transmission times in a given hour. The proposed scheme can efficiently decrease the outage probability (i.e., increase the data decoding reliability) and decrease the secrecy outage probability (i.e., increase the system PHY security).
- We propose an analysis framework that connects the outage probability of the wireless transmissions with the energy-demand estimation-error cost measured in dollars.

Notation: Unless otherwise stated, lower- and upper-case bold letters denote vectors and matrices, respectively. $\mathbf{I}_N$ and $\mathbf{F}$ denote, respectively, the identity matrix whose size is $N \times N$ and the fast Fourier transform (FFT) matrix. $\mathbb{C}^{M\times N}$ denotes the set of all complex matrices of size $M \times N$. $(\cdot)^\top$ and $(\cdot)^*$ denote transpose and Hermitian (i.e., complex-conjugate transpose) operations, respectively. $|\cdot|$ cardinality of a set. $\mathbb{R}^{M\times N}$ denotes the set of real matrices of size $M \times N$. $\mathbb{E}\{\cdot\}$ denotes statistical expectation. $\mathbf{0}_{M\times N}$ denotes the all-zero matrix with size $M \times N$. $\overline{\theta} = 1 - \theta$. diag $= \{\cdot\}$ denotes a diagonal matrix with the enclosed elements as its diagonal elements. $[\cdot]^+ = \max\{0, \cdot\}$ returns the maximum between the argument and zero.

II. SYSTEM AND NETWORK MODELS AND ASSUMPTIONS

A. NETWORK MODEL

Consider the scenario of an SG with multiple load consumers (Alices) communicating with gateways (Bobs) which forward the energy-demand information of the consumers to a data aggregator unit (DAU), which we refer to as George. George then forwards the received energy-demand information to the MDMS. Each subarea is assigned a gateway where Bob $q \in \{1, 2, \dots\}$ is assigned to forward the consumers' information in subarea q. We assume two-hop communication where in one communication time slot the smart meters transmit their data wirelessly to Bob which decodes-then-forwards the data to George. In the sequel, we assume that consumer (Alice) n is located in subarea q and she forwards her data to the q-th Bob. Each node is equipped with a single antenna. The block diagram of our investigated energy distribution system is depicted in Fig. 1. The set of consumers is denoted by $\mathcal{M}$ with cardinality $|\mathcal{M}| = M$. We assume that each consumer $n \in \mathcal{M}$ is equipped with a smart meter, which we refer to as a home-area network (HAN) smart meter. The HAN smart meter has an automatic energy consumption scheduler (ECS) capability for scheduling the household energy consumption. The smart meters are all connected to the energy source through the power line and all of them have a constant power supply.

A HAN gateway is connected with each of the smart meters. The smart meter sends the energy-demand information to the HAN gateway. Then, the HAN gateway (Alice) forwards this meter data to a data forwarder of a subarea. The network connecting the HAN gateways of the consumers in a subarea is the neighborhood area network (NAN) gateway (Bob). To manage the energy supply in a service area, the energy-demand information from the consumers is then forwarded by the NAN gateways to the DAU, which we refer to as George, and from the DAU to the MDMS. The network connecting the NAN gateways is the wide-area network (WAN).

B. CHANNEL MODEL

We assume a frequency-selective channel model where the channel coefficients remain unchanged during one coherence time duration, but change independently from one coherence time to another. The entire codeword of a legitimate transmitter is transmitted in a coherence time duration. All the channel coefficients are assumed to be independent and identically distributed (i.i.d.) zero-mean circularly-symmetric complex Gaussian random variables with variance $\sigma^2_{m_1-m_2,l}$ for the $m_1 - m_2$ link, where $l \in \{0, 1, 2, \dots, \nu_{m_1-m_2}\}$ with $\nu_{m_1-m_2}$ denoting the delay spread of the $m_1 - m_2$ link. We assume that the legitimate transmitting nodes (i.e., Alices and Bobs) know the CSI of the links connecting them to their legitimate receivers. Hence, Alices and Bobs do not know the CSI of the eavesdropping node(s). The thermal noise samples at node m_2 are modeled as zero-mean complex circularly-symmetric Gaussian random variables with power κ_{m_2} Watts. The total channel bandwidth of W Hz is divided into N orthogonal sub-channels by using OFDM with each sub-channel experiencing frequency-flat slow fading. The total transmit power of an Alice per time slot is constrained to $P_{\rm A}$ Watts. Moreover, the total transmit power of a Bob is assumed to be $P_{\rm B}$ Watts. We assume equal power allocation among the data symbols of the OFDM sub-channels.

We assume that there is no congestion in the network. This is a reasonable assumption since the network topology is well defined and any increase or decrease in the number of transmitters in the network is rare. Moreover, the energy demands of the consumers are sent over one hour duration and change from one hour to another. Hence, there is sufficient time to assign time slots to consumers. A time-division multiple-access (TDMA) scheme is assumed in all the communications between the Alices and their gateway (Bob) and between Bob and George. Hence, each communication time slot is divided into M non-overlapping time subslots and each consumer is assigned one of these subslots. Assuming that the communication time slot has a duration of T seconds, the time assigned to a consumer is $\frac{T}{M/2}$ seconds and that assigned to Bob to forward the data packet of that consumer to George is $\frac{T}{M/2}$ seconds. The consumers communicate with the gateways k times per hour.[1] The communications time

[1]Typically, the smart meters send their information each 15 minutes. For sake of generality, in this paper, we assume that the energy demands are sent k times over an hour duration.

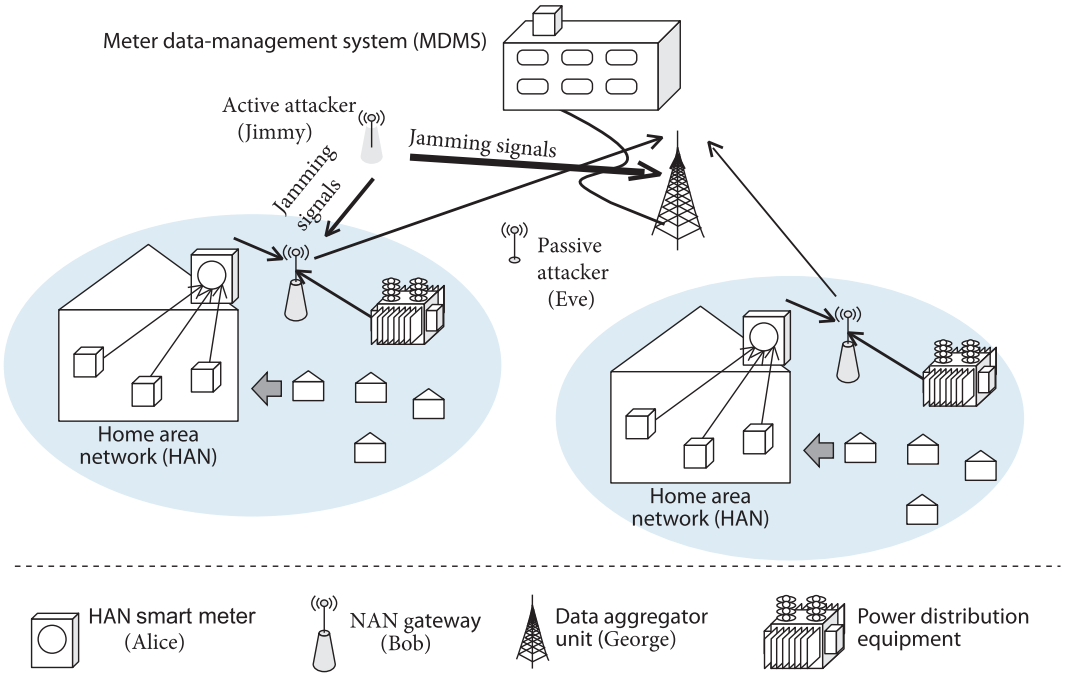

FIGURE 1. System and network models for DSM in SG.

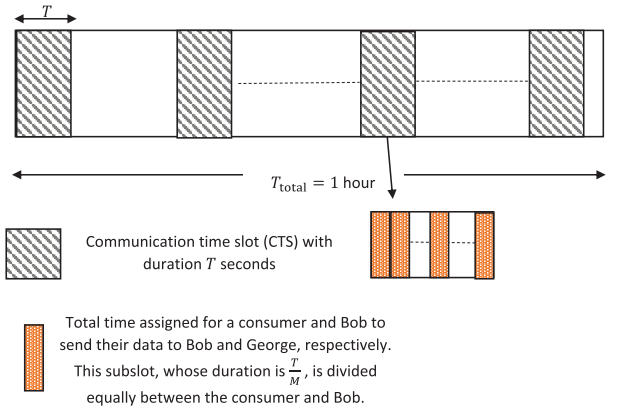

FIGURE 2. Communication during one hour.

structure during one hour is depicted in Fig. 2. Each data packet comes with a cyclic redundancy check (CRC). If the checksum of the CRC is correct, the packet is assumed to be correctly decoded. If the checksum is incorrect, the packet is assumed to be erroneously decoded. After decoding the k data transmissions from Alice to George, George checks the CRC. If the packet is correctly decoded, George sends an acknowledgement (ACK) message. Otherwise, he sends a negative-ACK (NACK) message.

C. ATTACKS MODEL

We assume active and passive attacks. More specifically, we assume that there is an **active attacker** (Jimmy) in the network who continuously transmits jamming signals during the communications intervals between the consumers' smart meters and the gateway and also between the gateway and the aggregator to degrade the reliability of communications. That is, the jammers' transmissions are synchronized with the transmissions of the legitimate system. Moreover, there is a **passive attacker** (Eve) who wishes to intercept the ongoing transmissions and decode the exchanged information. The active and passive attackers help each other and are completely colluding and share the necessary information for hacking the SG wireless communications system.[2] Jimmy transmits jamming signals to degrade the received signal at the MDMS while completely eliminating any interference at Eve. Eavesdropping is a severe security problem since the passive attacker can collect the consumers' information and determine their identities. Moreover, on the SG scale, the eavesdropper can compute and analyze the revenue of the utility.

The active attacker, Jimmy, tries to jam the legitimate system in such a way that he does not hurt the passive attacker Eve. In particular, the main objective of Jimmy is to minimize the rate of the current legitimate transmitting node. Jimmy designs the AN precoding vectors to lie in the null space of the Jimmy-Eve channel matrix. It is assumed that Jimmy only knows the CSI of the channels connecting him to Eve. The total jamming power of Jimmy is P_{J} Watts. In the following, for notation simplicity, we denote the n-th Alice,

[2]If there are multiple passive and active attackers, the best pair of eavesdroppers and jammers will be selected in a given time. This will not change the presented ideas and analysis. However, it will complicate the presentation of the ideas.

q-th Bob, George, Eve, and Jimmy by n, B_q, G, E, and J, respectively.

D. LEGITIMATE NODES TRANSMISSION AND AN-AIDED SCHEMES

Each Alice wishes to transmit her data securely to the MDMS through Bob and George. To achieve this goal, each Alice sends temporal AN vectors in the null space of the equivalent channel matrix at Bob's receiver. Since the n-th Alice sends data and AN vectors, she uses a power fraction $0 \leq \theta \leq 1$ to split her total transmit power between data and AN vectors. If θ_A is close to 1, more power is assigned to data transmission than AN transmission. This may make the legitimate system less secure (i.e., lower its secrecy rate). However, this will also result in a more reliable data decoding at Bob's receiver since the data signal-to-noise ratio (SNR) at Bob will increase. The legitimate parties (i.e., Alices and Bob) may prefer to send the data with high reliability since this results in better decoding of the exact consumers' energy demands at the DSM and, hence, results in less energy-demand estimation monetary loss. Consequently, there is a tradeoff between having reliable communications between the smart meters and the MDMS (which saves money for the utility) and secure transmissions (which is important for the consumers' and utility's confidentialities). Similarly, Bob also transmits data and AN vectors to George. Again, the reliability and security of the communications between the smart meters and the MDMS are determined by the power fraction θ_B that Bob uses to secure his transmissions.

A reliability analysis for the SG wireless communications system described above can be used to quantify the availability of the connectivity from a smart meter to the HAN gateway, the NAN gateway, and the DAU to the MDMS. After we quantify the availability performance, the cost incurred to the utility due to the energy-demand estimation error is evaluated.

III. DSM IN THE SG

Implementing DSM by the utilities is critical to optimizing the energy supply in the SG [9]. The energy demands of the consumers are used to determine the amount of energy supply to be generated, transmitted, and distributed by substations to the energy consumers. Due to the uncertainty of energy consumption, the energy demand may not be determined precisely at the utility.

Towards solving the uncertainty issue, the energy system operation is realized over two stages [2], namely, unit-commitment and economic-dispatch stages. In the unit-commitment stage, the utility reserves the energy supply from a generator according to the estimated energy demand of the consumers during a period of one hour. A forward contract is made in advance between the utility and a generator to acquire the energy supply. Afterwards, the utility checks whether or not the energy supply from the unit-commitment stage meets the actual energy demands from the consumers. If the energy supply does not meet the energy demands from the consumers, in the second (i.e., economic-dispatch) stage, the utility will buy the energy difference between the actual and estimated energies from an expensive generator to avoid the under-supply situation. It is noteworthy that the energy supply price in the unit-commitment stage is lower than that in the economic-dispatch stage since it is reserved in advance. Hence, the utility obtains the energy supply in the unit-commitment stage from a slow-start, such as a coal generator.

On the other hand, energy supply in the economic-dispatch stage must have a quick start and be able to meet the actual energy demand of the consumers. Hence, this energy supply is usually obtained from a more expensive source, e.g., diesel generator or a battery storage. In this case, through the energy market, the energy supply in the unit-commitment stage is reserved with a forward price, while the energy supply in the economic-dispatch stage is bought with an option price. The forward price is lower than the option price. The importance of dividing the energy-delivery operation of an energy system into two stages is that the utility can efficiently schedule the electricity supply to the consumers under uncertainty. In addition, the utility can avoid a penalty for not supplying the exact energy demands of its consumers.

From the above discussion, we have two possible energy uncertainties:

- Energy under-supply in which the generated, transmitted, and distributed energy cannot meet the demand in a particular area at a particular time. The energy under-supply occurs when the reserved MDMS energy in the unit-commitment stage is less than the actual energy demand. As a result, an additional energy supply has to be bought in the economic-dispatch stage as explained earlier. Due to the penalty charged, for example, by a government, the energy under-supply can incur cost to the utility.
- Energy over-supply which occurs when the reserved MDMS energy in the unit-commitment stage is more than the actual demand.

For the SG wireless communications system shown in Fig. 1, the MDMS computes the aggregated energy demand of a service area by summing the energy demands from all consumers in that area. However, if the energy demand of any consumer is not received by the MDMS due to a failure in decoding the data packets at the HAN gateway (Bob) or the aggregator (George), the MDMS uses historical data to compute the aggregated energy demand. In this case, a factor x times the mean energy consumption of those consumers is used as the estimated energy demand. Using the factor x is reasonable to reduce the chance of a power under-supply which results in a relatively higher financial loss than the over-supply.[3] The mean energy consumption for a consumer can be calculated statistically from historical energy usage data of that consumer. Once the aggregated energy demand

[3]We will investigate the impact of x on the energy-demand estimation cost in the numerical results section.

is obtained, the MDMS reserves the energy supply from the generators in the unit-commitment stage and the energy is delivered to the consumers in a service area. Then, the MDMS checks whether the energy supply is sufficient or not (e.g. from voltage drop). If the energy supply is not sufficient, an additional energy supply will be bought in the economic-dispatch stage to meet the actual energy demand.

To measure the impact of the PHY security and reliability of the wireless communication link on the DSM operation, we first need to compute the cost due to channel outages. In the next section, we derive the energy-demand estimation-error cost in terms of the wireless link outage probability. Then, in Section V, we describe possible attacks on the legitimate wireless communications system and present our proposed enhanced-security scheme. In addition, we derive the nodes' rates and secrecy rates as well as the wireless links' outage and secrecy outage probabilities. Our proposed analysis framework is depicted in Fig. 3.

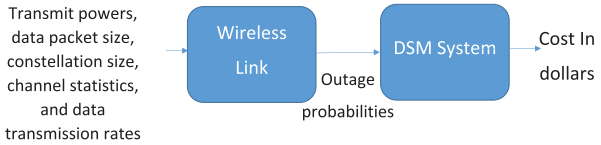

FIGURE 3. Our proposed analysis framework.

IV. COST OF WIRELESS NETWORK OUTAGE

We consider the availability performance measure as the probability that both the wireless communication links between the transmitting node and Bob and that between Bob and George are not in outage **simultaneously**. When the connection between a HAN gateway and a DAU is unavailable, the MDMS cannot collect the actual energy demand information from a smart meter, and the estimated energy demand will be used instead. This can increase cost to the utility due to energy-demand estimation errors which result in energy over- and under-supply. The energy over-supply occurs when the MDMS reserves more energy in the unit-commitment stage than the actual demand. On the other hand, the energy undersupply occurs when the MDMS reserves less energy in the unit-commitment stage than the actual demand, and as a result, an additional energy supply has to be bought in the economic-dispatch stage.

Given the availability of the wireless connection between a HAN gateway and the DAU, the cost of energy-demand estimation error can be analyzed based on the energy demand distribution. The energy demand distribution here refers to the probability density function (PDF) of the actual energy demand. The energy-consumption of each consumer is random and follows a probability distribution[4] with mean μ_n and variance σ_n^2 for consumer n. The cost of demand-estimation error of individual consumer n whose connection to the MDMS is unavailable can be computed as follows

$$\text{Cost}(n) = \underbrace{p_{uc}\int_0^{E_n}(E_n - a)f_A^{(n)}(a)da}_{\text{Cost of energy over-supply}} + \underbrace{p_{ed}\int_{E_n}^{E_n^{\max}}(a - E_n)f_A^{(n)}(a)da}_{\text{Cost of energy under-supply}} \quad (1)$$

where $E_n = x \times \mu_n$ is the energy supply reserved in the unit-commitment stage, μ_n is the mean energy consumption of consumer n, $E_n^{\max}$ is the maximum energy consumption, and $f_A^{(n)}(a)$ is the PDF of actual energy demand a. p_{uc} and p_{ed} denote the energy prices in the unit-commitment and in the economic-dispatch stages, respectively. The first term in Eqn. (1) represents the aggregated cost due to energy over-supply (i.e., the MDMS reserves energy of E_n kWh which is more than the actual demand a, $E_n > a$). On the other hand, the second term in Eqn. (1) represents the aggregated cost due to energy under-supply (i.e., reserved energy E_n kWh is less than the actual demand a, $E_n < a$). Note that this average cost of energy-demand estimation error is per time period.

The average energy-demand estimation-error cost is given by

$$\mathbb{E}\{\text{Cost}(n)\} = \sum_{n\in\mathcal{M}} \text{Cost}(n)P_{\text{outage}}^n \quad (2)$$

where $P_{\text{outage}}^n = 1 - (1 - P_{n-\text{B}_q})(1 - P_{\text{B}_q-\text{G}}^n)$ is the outage probability of the two-hops while transmitting the n-th Alice packet to George through the q-th Bob. $P_{n-\text{B}_q}$ denotes the outage probability of the wireless link between the n-th Alice and the q-th Bob and $P_{\text{B}_q-\text{G}}^n$ denotes the outage probability of the wireless link between the q-th Bob and George while forwarding the data packet of the n-th Alice. In order to compute the total energy-demand estimation-error cost, we need to compute the transmissions outage probabilities. In the following section, we derive the nodes' rates and secrecy rates to compute the outage (no connection) and the secrecy outage probabilities.

V. PROPOSED SCHEME AND SECRECY RATES

A. FIRST HOP

In the first hop, Alice transmits the data signal to Bob and the AN signal to confuse Eve. Moreover, Jimmy transmits AN signals to confuse Bob. The transmitted and received signals at various nodes are derived and explained in the following.

1) TRANSMITTED SIGNAL BY ALICE

The selected Alice for transmission converts the frequency-domain signals to the time-domain signals using an N-point inverse FFT (IFFT). To eliminate inter-block interference, Alice adds a CP of size N_{cp} samples to the beginning of every OFDM block. We assume that the CP length is longer

[4]The energy demands of consumers can follow any distribution. Our analysis does not rely on this assumption. In the numerical results, we assume a normal distribution which is a commonly-used energy-demand distribution [9], [33], [34].

than or equal to the delay spread of the channel between Alice and Bob (Eve), denoted by $\nu_{n-\mathrm{B}_q}$ (ν_{n-E}). This is a best-case assumption for Eve; otherwise, her rate will be degraded due to inter-block and intra-block interference. To secure the legitimate transmissions from eavesdropping, we assume that Alice transmits an AN vector along with her data vector. The AN vector is designed in a way such that its impact will be removed at Bob prior to information decoding as will be discussed shortly. Alice splits her transmit power, P_{A}, between data and AN transmissions. Assuming that a fraction θ_{A} of the total power P_{A} is assigned to data transmission, the power assigned to AN transmission is $\overline{\theta_A}P_{\mathrm{A}}$. Assuming that subslot $t_n \in \{1, 2, \ldots, |\mathcal{M}|\}$ of the communication time slot $\ell \in \{1, 2, \ldots, k\}$ is assigned to consumer n (i.e., Alice n), the n-th Alice's transmitted signal is given by

$$\mathbf{s}_n^{\ell,t_n} = \mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_n^{\ell,t_n} + \mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} \tag{3}$$

where $\mathbf{T}_{\mathrm{cp}} \in \mathbb{R}^{(N+N_{\mathrm{cp}})\times N}$ is the CP insertion matrix, $\mathbf{x}_n^{\ell,t_n} \in \mathbb{C}^{N\times 1}$ is the data vector transmitted by the n-th Alice, $\mathbf{Q}_n^{\ell,t_n} \in \mathbb{C}^{(N+N_{\mathrm{cp}})\times N_{\mathrm{cp}}}$ is the temporal-AN precoder matrix at Alice during the t_n-th subslot of the ℓ-th communication time slot, and $\mathbf{z}_n^{\ell,t_n} \in \mathbb{C}^{N_{\mathrm{cp}}\times 1}$ is the AN vector transmitted by the n-th Alice. Since Eve's instantaneous CSI is assumed to be unknown at the n-th Alice, she distributes the AN power isotropically in all directions (i.e., equal power allocation among the AN symbols in $\mathbf{z}_n^{\ell,t_n} \in \mathbb{C}^{N_{\mathrm{cp}}\times 1}$). Hence, the AN symbol power is $\overline{\theta_A}P_{\mathrm{A}}/N_{\mathrm{cp}}$.

2) TRANSMITTED SIGNAL BY JIMMY

Jimmy jams the received signal at Bob while completely eliminating the interference at Eve. Jimmy's transmitted signal is given by

$$\mathbf{s}_{\mathrm{J}}^{\ell,t_n} = \mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} \tag{4}$$

where $\mathbf{Q}_{\mathrm{J}}^{\ell,t_n} \in \mathbb{C}^{(N+N_{\mathrm{cp}})\times N_{\mathrm{cp}}}$ is the temporal-AN precoding matrix at Jimmy during the t_n-th subslot of the ℓ-th communication time slot, and $\mathbf{z}_{\mathrm{J}}^{\ell,t_n} \in \mathbb{C}^{N_{\mathrm{cp}}\times 1}$ is the AN vector transmitted by Jimmy to jam Bobs with symbol power $\frac{P_{\mathrm{J}}}{N_{\mathrm{cp}}}$ Watts.

3) RECEIVED SIGNAL AT EVE

The received signal vector at Eve is given by

$$\begin{aligned}\mathbf{y}_{\mathrm{E}}^{\ell,t_n} &= \mathbf{H}_{n-E}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_n^{\ell,t_n} + \mathbf{H}_{n-E}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} \\ &\quad + \mathbf{H}_{\mathrm{J}-\mathrm{E}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{n}_{\mathrm{E}}^{\ell,t_n}\end{aligned} \tag{5}$$

where $\mathbf{H}_{n-E}^{\ell,t_n}$ and $\mathbf{H}_{\mathrm{J}-\mathrm{E}}^{\ell,t_n}$ are the time-domain channel matrices between the n-th Alice and Eve and between Jimmy and Eve, respectively, during the t_n-th subslot of the ℓ-th communication time slot. After the CP removal and FFT block, the signal at Eve is

$$\begin{aligned}\mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{y}_{\mathrm{E}}^{\ell,t_n} &= \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_n^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} \\ &\quad + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J}-\mathrm{E}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{n}_{\mathrm{E}}^{\ell,t_n}\end{aligned} \tag{6}$$

where $\mathbf{n}_{\mathrm{E}}^{\ell,t_n} \in \mathbb{C}^{N\times 1}$ is the AWGN vector after the FFT operation at Eve. To cancel the AN at Eve, the AN-precoding matrix at Jimmy, $\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}$, should satisfy the following equation

$$\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J}-\mathrm{E}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n} = \mathbf{0}_{N\times N_{\mathrm{cp}}} \tag{7}$$

Eqn. (7) always has a non-trivial solution since the number of columns of $\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J}-\mathrm{E}}^{\ell,t_n}$ is $N_{\mathrm{T}} = N + N_{\mathrm{cp}}$ and its rank is $N < N_{\mathrm{T}}$.

After cancellation of Jimmy's AN at Eve, the received signal vector at Eve is equal to

$$\tilde{\mathbf{y}}_{\mathrm{E}}^{\ell,t_n} = \mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n}\mathbf{x}_n^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{n}_{\mathrm{E}}^{\ell,t_n} \tag{8}$$

where $\mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n} = \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*$ is the frequency response of the Alice-Eve channel. The achievable rate at Eve is thus given by

$$R_{n-\mathrm{E}}^{\ell,t_n} = \frac{\log_2 \det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{A}}P_{\mathrm{A}}}{N_{\mathrm{T}}}\mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n}\mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n}{}^*(\mathbf{C}_{n-\mathrm{E}}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}} \tag{9}$$

where $\mathbf{C}_{n-\mathrm{E}}^{\ell,t_n} = \frac{\overline{\theta_A}P_{\mathrm{A}}}{N_{\mathrm{cp}}}\mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\left(\mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-E}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\right)^* + \kappa_{\mathrm{E}}\mathbf{F}\mathbf{R}_{\mathrm{cp}}\left(\mathbf{F}\mathbf{R}_{\mathrm{cp}}\right)^*$ is the noise-plus-interference covariance matrix at Eve.

4) RECEIVED SIGNAL AT BOB

The received signal vector at the q-th Bob is given by

$$\begin{aligned}\mathbf{y}_{\mathrm{B}_q}^{\ell,t_n} &= \mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_n^{\ell,t_n} + \mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} \\ &\quad + \mathbf{H}_{\mathrm{J}-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{n}_{\mathrm{B}_q}^{\ell,t_n}\end{aligned} \tag{10}$$

where $\mathbf{H}_{n-B}^{\ell,t_n}$ and $\mathbf{H}_{\mathrm{J}-\mathrm{B}_q}^{\ell,t_n}$ are the time-domain channel matrices between the n-th Alice and the q-th Bob and between Jimmy and the q-th Bob, respectively, during the t_n-th subslot of the ℓ-th communication time slot. After the CP removal and FFT operation, the signal at the q-th Bob is given by

$$\begin{aligned}\mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{y}_{\mathrm{B}_q}^{\ell,t_n} &= \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_n^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n}\mathbf{z}_n^{\ell,t_n} \\ &\quad + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J}-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{n}_{\mathrm{B}_q}^{\ell,t_n}\end{aligned} \tag{11}$$

To cancel the AN signal transmitted by the n-th Alice at the q-th Bob, the AN-precoding matrix at Alice, $\mathbf{Q}_n^{\ell,t_n}$, should satisfy the following condition

$$\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_n^{\ell,t_n} = \mathbf{0}_{N\times N_{\mathrm{cp}}} \tag{12}$$

Eqn. (12) always has a non-trivial solution since the number of columns of $\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}$ is N_{T} and its rank is $N < N_{\mathrm{T}}$. After AN cancellation, the received signal at the q-th Bob is

$$\tilde{\mathbf{y}}_{\mathrm{B}_q}^{\ell,t_n} = \mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n}\mathbf{x}_n^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J}-\mathrm{B}_q}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{n}_{\mathrm{B}_q}^{\ell,t_n} \tag{13}$$

where $\mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n} = \mathbf{F}\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{n-\mathrm{B}_q}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^* \in \mathbb{C}^{N\times N}$ is frequency response of the channel between the n-th Alice and the q-th Bob. The rate of channel between the n-th Alice and the q-th Bob during the ℓ-th communication time slot is thus given by

$$R_{n-\mathrm{B}_q}^{\ell,t_n} = \frac{\log_2 \det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{A}}P_{\mathrm{A}}}{N_{\mathrm{T}}}\mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n}\mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n}{}^*(\mathbf{C}_{\mathrm{J}-\mathrm{B}_q}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}} \tag{14}$$

where $\mathbf{C}_{\mathrm{J-B}_q}^{\ell,t_n} = \frac{P_{\mathrm{J}}}{N_{\mathrm{cp}}}\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-B}_q}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\left(\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-B}_q}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\right)^* + \kappa_{\mathrm{B}_q}\mathbf{FR}_{\mathrm{cp}}\left(\mathbf{FR}_{\mathrm{cp}}\right)^*$ is the noise-plus-interference covariance matrix at Bob.

The secrecy rate of the n-th Alice transmission to the q-th Bob during the ℓ-th communication time slot is given by

$$\begin{aligned} R_{n-\mathrm{B}_q,\mathrm{sec}}^{\ell,t_n} &= \left[R_{n-\mathrm{B}_q}^{\ell,t_n} - R_{n-\mathrm{E}}^{\ell,t_n}\right]^+ \\ &= \left[\frac{\log_2\det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{A}}P_{\mathrm{A}}}{N_{\mathrm{T}}}\mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n}\mathbf{H}_{n-\mathrm{B}_q}^{\mathrm{F},\ell,t_n *}(\mathbf{C}_{\mathrm{J-B}_q}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}}\right. \\ &\quad \left. - \frac{\log_2\det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{A}}P_{\mathrm{A}}}{N_{\mathrm{T}}}\mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n}\mathbf{H}_{n-E}^{\mathrm{F},\ell,t_n *}(\mathbf{C}_{n-\mathrm{E}}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}}\right]^+ \end{aligned} \tag{15}$$

B. SECOND HOP

In the second-hop, Bob transmits data vectors to George and AN vectors to confuse Eve. In addition, Jimmy operates as in the previous hop, but instead of sending the AN vectors to jam Bobs, he sends them to jam George. Under the assumption that there are no direct links between Alices and the data aggregator (George), the best strategy for Bob to decrease the secrecy outage probability is to use codebooks different from those used by Alices as it was shown in the PHY security literature [35] (i.e., randomize-and-forward relaying). The received signal vector at George is thus given by

$$\begin{aligned} \mathbf{y}_{\mathrm{G}}^{\ell,t_n} &= \mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_{\mathrm{B}_q}^{\ell,t_n} + \mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n}\mathbf{z}_{\mathrm{B}_q}^{\ell,t_n} \\ &\quad + \mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{n}_{\mathrm{G}}^{\ell,t_n} \end{aligned} \tag{16}$$

where $\mathbf{x}_{\mathrm{B}_q}^{\ell,t_n}$ is the data signal transmitted from the q-th Bob to George during the ℓ-th communication time slot while forwarding the n-th Alice's data to George, $\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}$ is the time-domain channel matrix between the q-th Bob and George during the t_n-th subslot of the ℓ-th communication time slot, and $\mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}$ is the time-domain channel matrix between Jimmy and George during the t_n-th subslot of the ℓ-th communication time slot. Furthermore, $\mathbf{Q}_{\mathrm{J}}^{\ell,t_n} \in \mathbb{C}^{(N+N_{\mathrm{cp}})\times N_{\mathrm{cp}}}$ is the temporal-AN precoding matrix used by Jimmy during the second phase when the q-th Bob forwards the data of the n-th Alice to George during the ℓ-th communication time slot. The matrix $\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}$ is designed as in the first hop (see (7)). Moreover, $\mathbf{z}_{\mathrm{J}}^{\ell,t_n} \in \mathbb{C}^{N_{\mathrm{cp}}\times 1}$ is the AN vector transmitted by Jimmy during the second hop with symbol power $\frac{P_{\mathrm{J}}}{N_{\mathrm{cp}}}$ Watts, $\mathbf{n}_{\mathrm{G}}^{\ell,t_n} \in \mathbb{C}^{N\times 1}$ is the AWGN vector at George. After the CP removal and FFT operation, the received signal at Bob is given by

$$\begin{aligned} \mathbf{FR}_{\mathrm{cp}}\mathbf{y}_{\mathrm{G}}^{\ell,t_n} &= \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^*\mathbf{x}_{\mathrm{B}_q}^{\ell,t_n} \\ &\quad + \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n}\mathbf{z}_{\mathrm{B}_q}^{\ell,t_n} \\ &\quad + \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{FR}_{\mathrm{cp}}\mathbf{n}_{\mathrm{G}}^{\ell,t_n} \end{aligned} \tag{17}$$

To cancel the AN transmitted by Bob at George, the AN-precoding matrix at Bob, $\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n}$, should satisfy the following condition

$$\mathbf{R}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n} = \mathbf{0}_{N\times N_{\mathrm{cp}}} \tag{18}$$

Again, Eqn. (18) always has a non-trivial solution.

Since Eve's instantaneous CSI is assumed to be unknown at Bob, he distributes his power fraction assigned to AN isotropically in all directions (i.e., equally among the AN symbols in $\mathbf{z}_{\mathrm{B}_q}^{\ell,t_n} \in \mathbb{C}^{N_{\mathrm{cp}}\times 1}$). Hence, the AN symbol power is $\overline{\theta_B}P_{\mathrm{B}}/N_{\mathrm{cp}}$.

After AN cancellation at George's receiver, the signal at George's receiver becomes equal to

$$\tilde{\mathbf{y}}_{\mathrm{G}}^{\ell,t_n} = \mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n}\mathbf{x}_{\mathrm{B}_q}^{\ell,t_n} + \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\mathbf{z}_{\mathrm{J}}^{\ell,t_n} + \mathbf{FR}_{\mathrm{cp}}\mathbf{n}_{\mathrm{G}}^{\ell,t_n} \tag{19}$$

where $\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n} = \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^* \in \mathbb{C}^{N\times N}$ is the frequency response of the channel between the q-th Bob and George. The achievable rate of the channel between the q-th Bob and George is thus given by

$$R_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n} = \frac{\log_2\det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{B}}P_{\mathrm{B}}}{N_{\mathrm{T}}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n *}(\mathbf{C}_{\mathrm{J-G}}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}} \tag{20}$$

where $\mathbf{C}_{\mathrm{J-G}}^{\ell,t_n} = \frac{P_{\mathrm{J}}}{N_{\mathrm{cp}}}\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\left(\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{J-G}}^{\ell,t_n}\mathbf{Q}_{\mathrm{J}}^{\ell,t_n}\right)^* + \kappa_{\mathrm{G}}\mathbf{FR}_{\mathrm{cp}}\left(\mathbf{FR}_{\mathrm{cp}}\right)^*$ is the noise-plus-interference covariance matrix at George.

In a similar fashion, we can obtain the received signal at Eve and the rates of the Bobs-Eve links during the second hop. The secrecy rate of the q-th Bob-George link during the t_n-th subslot of the ℓ-th communication time slot when the q-th Bob forwards the n-th Alice's data packet is given by

$$\begin{aligned} R_{\mathrm{B}_q-\mathrm{G},\mathrm{sec}}^{\ell,t_n} &= \left[R_{\mathrm{B}_q-\mathrm{G}}^{\ell,t_n} - R_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n}\right]^+ \\ &= \left[\frac{\log_2\det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{B}}P_{\mathrm{B}}}{N_{\mathrm{T}}}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n}\mathbf{H}_{\mathrm{B}_q-\mathrm{G}}^{\mathrm{F},\ell,t_n *}(\mathbf{C}_{\mathrm{J-G}}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}}\right. \\ &\quad \left. - \frac{\log_2\det\left(\mathbf{I}_N + \frac{\theta_{\mathrm{B}}P_{\mathrm{B}}}{N_{\mathrm{T}}}\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\mathrm{F},\ell,t_n}\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\mathrm{F},\ell,t_n *}(\mathbf{C}_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n})^{-1}\right)}{N_{\mathrm{T}}}\right]^+ \end{aligned} \tag{21}$$

where $\mathbf{C}_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n} = \frac{\overline{\theta_B}P_{\mathrm{B}}}{N_{\mathrm{cp}}}\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n}\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n}\left(\mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n}\mathbf{Q}_{\mathrm{B}_q}^{\ell,t_n}\right)^* + \kappa_{\mathrm{E}}\mathbf{FR}_{\mathrm{cp}}\left(\mathbf{FR}_{\mathrm{cp}}\right)^*$ is the noise-plus-interference covariance matrix at Eve when the q-th Bob forwards the data packet of the n-th Alice, and $\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\mathrm{F},\ell,t_n} = \mathbf{FR}_{\mathrm{cp}}\mathbf{H}_{\mathrm{B}_q-\mathrm{E}}^{\ell,t_n}\mathbf{T}_{\mathrm{cp}}\mathbf{F}^* \in \mathbb{C}^{N\times N}$ is the frequency response of the channel between the q-th Bob and Eve.

The secrecy rate of the n-th Alice transmission during the ℓ-th communication time slot is determined by the minimum secrecy rate of the two hops. Hence, the secrecy rate of the n-th Alice's transmission during an hour is given by

$$R_{n,\mathrm{sec}} = \min_{\ell\in\{1,2,\ldots,k\}:} \min\left\{R_{n-\mathrm{B}_q,\mathrm{sec}}^{\ell,t_n}, R_{\mathrm{B}_q-\mathrm{G},\mathrm{sec}}^{\ell,t_n}\right\} \tag{22}$$

C. OUTAGE AND SECRECY OUTAGE PROBABILITIES

Each Alice sends fixed-rate data packets that include her energy requirement in each hour. Assuming that a packet has b bits and the time slot duration assigned to a transmitting node for data transmission is $\frac{T}{M/2}$, the target secrecy rate is $\mathcal{R} = b/(2\,MWT)$ bits/channel use. Since Eve's instantaneous CSI is assumed to be unknown at the legitimate transmitting nodes, the **instantaneous** secrecy rate $R_{n,\text{sec}}$ is **unknown** at the transmitting nodes. Consequently, the transmission is secured when $R_{n,\text{sec}} \geq \mathcal{R}$. Otherwise, the system is said to be unsecured and the secrecy is compromised.

Since the same data is transmitted k times in an hour, we have two options with distinct objectives: 1) sending the same packet at each of the k communication time slots but with a different codebook at each time so that the eavesdropper cannot combine the data signals; 2) sending the data at a lower transmission rate to decrease both the outage and secrecy outage probabilities by encoding the packet over the k communication time slots. We conclude this section by discussing the link and secrecy outage probabilities under these two cases.

1) SAME DATA PACKET TRANSMISSIONS

The outage probability of the link between the n-th Alice and the q-th Bob is

$$P_{n-\text{B}_q} = \prod_{\ell=1}^{k} \Pr\left\{R_{n-\text{B}_q}^{\ell,t_n} < \mathcal{R}\right\} \tag{23}$$

which is the probability that all the transmissions of the n-th Alice to the q-th Bob during the k transmissions (i.e., communication time slots) in one hour are in outage.

The outage probability of the q-th Bob's transmission when he forwards the n-th Alice's data packet with target secrecy rate of $\mathcal{R}$ bits/channel use is given by

$$P_{\text{B}_q-\text{G}}^{n} = \prod_{\ell=1}^{k} \Pr\left\{R_{\text{B}_q-\text{G}}^{\ell,t_n} < \mathcal{R}\right\} \tag{24}$$

Thus, the outage probability of the n-th Alice transmission is written as

$$P_{\text{outage}}^{n} = 1 - (1 - P_{n-\text{B}_q})(1 - P_{\text{B}_q-\text{G}}^{n}) \tag{25}$$

The fraction of the n-th Alice's data being in secrecy outage is given by

$$P_{n,\text{sec}} = \Pr\left\{R_{n,\text{sec}} < \mathcal{R}\right\} \tag{26}$$

2) ENCODING THE DATA OVER THE k COMMUNICATION TIME SLOTS

In this case, we assume that the n-th Alice encodes the data over the k communication time slots so that she decreases the target secrecy rate to $\mathcal{R}/k$ bits/channel use. More specifically, Alice divides the data packet, whose size is b bits, into k data blocks. Hence, the transmission rate of each data block is b/k bits/communication time slot (i.e., $\mathcal{R}/k$ bits/channel use). Hence, both the outage probability and secrecy outage probability decrease. The outage probability in this case is the probability that all parts of the packet (i.e., the k transmissions from Alice to Bob and from Bob to George) are decoded correctly at Bob and George. Hence, the minimum of the k rates should be greater than $\mathcal{R}/k$ for successful decoding. In this case, the outage probability of the n-th Alice transmission during the first hop is given by

$$P_{n-\text{B}_q} = 1 - \prod_{\ell=1}^{k} \Pr\left\{R_{n-\text{B}_q}^{\ell,t_n} \geq \frac{\mathcal{R}}{k}\right\} \tag{27}$$

where $\prod_{\ell=1}^{k} \Pr\left\{R_{n-\text{B}_q}^{\ell,t_n} \geq \frac{\mathcal{R}}{k}\right\}$ is the probability that the k transmissions (messages) are decoded at Bob correctly. Moreover, the outage probability of the q-th Bob's transmission, when the data packet is transmitted with secrecy rate $\mathcal{R}/k$, is

$$P_{\text{B}_q-\text{G}}^{n} = 1 - \prod_{\ell=1}^{k} \Pr\left\{R_{\text{B}_q-\text{G}}^{\ell,t_n} \geq \frac{\mathcal{R}}{k}\right\} \tag{28}$$

where $\prod_{\ell=1}^{k} \Pr\left\{R_{\text{B}_q-\text{G}}^{\ell,t_n} \geq \frac{\mathcal{R}}{k}\right\}$ is the probability that the k transmissions are decoded at George correctly.

By using this encoding scheme, the secrecy outage probability of the ℓ-th block (from the k blocks of a data packet) is

$$P_{n,\text{sec}}^{\ell} = P_{n,\text{sec}}^{\text{block}} = \Pr\left\{\min\left\{R_{n-\text{B}_q,\text{sec}}^{\ell,t_n}, R_{\text{B}_q-\text{G},\text{sec}}^{\ell,t_n}\right\} < \frac{\mathcal{R}}{k}\right\} \tag{29}$$

which is the probability that Eve can decode partially (or completely) the n-th Alice transmitted information from either the first hop or the second hop. It is noteworthy that the probability in (29) is independent of time since the channels are i.i.d. If $k - m$ blocks of a packet experience a secrecy outage, which occurs with probability $\left(P_{n,\text{sec}}^{\text{block}}\right)^{k-m}$, Eve can decode a fraction $\frac{k-m}{k}$ of the n-th Alice's packet. The fraction of unsecured data from the n-th Alice to George is

$$P_{n,\text{sec}} = \sum_{m=0}^{k} \frac{k-m}{k} \mathcal{C}_{k-m}^{k} \left(P_{n,\text{sec}}^{\text{block}}\right)^{k-m} \left(1 - P_{n,\text{sec}}^{\text{block}}\right)^{m} \tag{30}$$

where $\mathcal{C}_{k-m}^{k}$ denotes k choose $k - m$.

VI. SIMULATION RESULTS

We consider DSM in a service area with $M = 200$ consumers. The energy-consumption of each consumer is random and follows a normal distribution [9], [33], [34] with mean of 3 kWh and standard deviation of 1.5. The maximum energy-consumption of each consumer is 10 kWh. The smart meter in each consumer measures and determines energy demand. The service area is divided into subareas and a NAN gateway is deployed for each of these subareas. There is one DAU in the service area.

The MDMS collects and computes the aggregated energy demand of a service area and buys its energy supply in

the unit-commitment stage at the beginning of each time period. Then, if the energy supply is not sufficient, additional energy is bought in the economic-dispatch stage. If the energy demand for any consumer is not received, the MDMS uses $x = 1.1$ times the mean value of the energy-consumption of that consumer as an estimated energy demand. The energy prices in the unit-commitment and economic-dispatch stages (i.e., forward and option prices) are $p_{uc} = 7$ and $p_{ed} = 10$ cents/kWh, respectively. We assume that $\theta_{\mathrm{A}} = \theta_{\mathrm{B}} = \theta$.

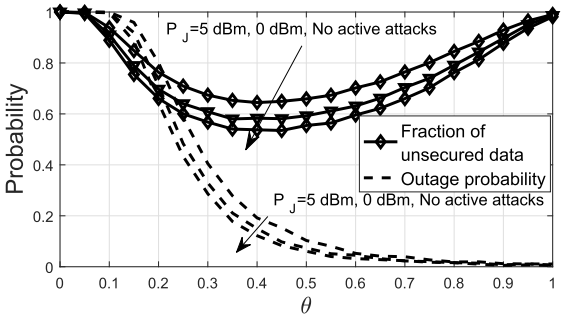

FIGURE 4. Impact of θ and P_{J} on the system's security and reliability.

In Fig. 4, we show the impact of the power ratio θ and the active attacker jamming power, P_{J}, on both the system's security, measured as the fraction of the bits decoded at Eve per hour, and its reliability, measured by the outage probability of the transmissions from an Alice to George. As shown in Fig. 4, there is an optimal θ where the security is maximized (i.e., the fraction of decoded bits at Eve is minimized). In addition, allocating all of Alice's transmit power to data transmission (i.e., setting $\theta = 1$) is beneficial in terms of reliability but security is sacrificed. In addition, the figure shows the reduction of both the security and reliability by increasing the active attacks powers. This is expected since the jamming power decreases both the link rates and the secrecy rates of the legitimate system.

Fig. 5 demonstrates the impact of the parameter $\mathcal{R}$ and the proposed encoding schemes at the legitimate transmitters. The proposed encoding scheme, where the data is encoded over the k available communication time slots to secure the transmissions and decrease the outage probability, performs much better than sending the same data packet over the k communication time slots. This is because in the latter scheme the transmission rate per communication time slot is high which increases both the secrecy and link outage probabilities. Moreover, if the eavesdropper was able to decode one of the k transmissions, the whole packet will be known at Eve. On the other hand, the former scheme prevents the possibility of decoding all the packets at Eve and the transmission rate is much lower than the latter scheme (i.e., lower with a factor of k) as explained in Section V-C. Fig. 5 also quantifies the reliability and the security losses when increasing $\mathcal{R}$.

Fig. 6 shows the impact of the power ratio θ and the active attacker jamming power level, P_{J}, on the total cost paid

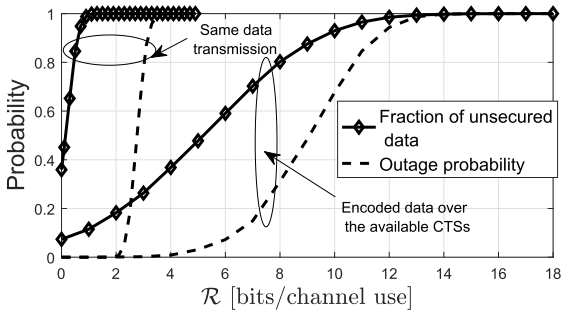

FIGURE 5. Impact of $\mathcal{R}$ and the encoding schemes at Alices on the system's security and reliability. In the figure's legend, CTS refers to communication time slot.

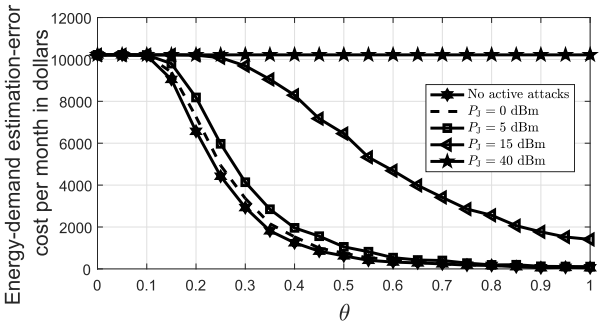

FIGURE 6. Impact of θ and P_{J} on cost of energy-demand estimation-error cost.

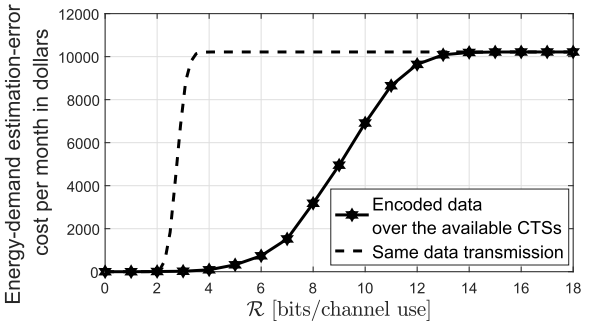

FIGURE 7. Impact of $\mathcal{R}$ and the proposed encoding schemes at Alices on energy-demand estimation-error cost.

by the utility per month due to energy-demand estimation errors. As shown in the figure, setting $\theta = 1$, as explained in Fig. 4, achieves the lowest cost and the highest system's reliability, but at the expense of lower security. In addition, the figure quantifies the increase of the cost payments due to active jamming attacks. At very high jamming power levels, the cost will be fixed for all θ at its maximum value since the outage probability is 1.

Fig. 7 demonstrates the impact of the parameter $\mathcal{R}$ and the proposed encoding schemes at the legitimate transmitters on the cost due to energy-demand estimation errors. The proposed encoding scheme results in a much lower cost than the case of sending the same data packet over the k communication time slots. Moreover, increasing $\mathcal{R}$ incurs a monetary loss which ranges from zero at very low $\mathcal{R}$ and saturates at the

significant value of \$10, 220 at high $\mathcal{R}$. The case of high $\mathcal{R}$ and the saturation in the figure is due to the fact that the outage probability will be 1 at high $\mathcal{R}$ which means that the utility (or MDMS) will not know the exact energy requirements of the $M = 200$ consumers.

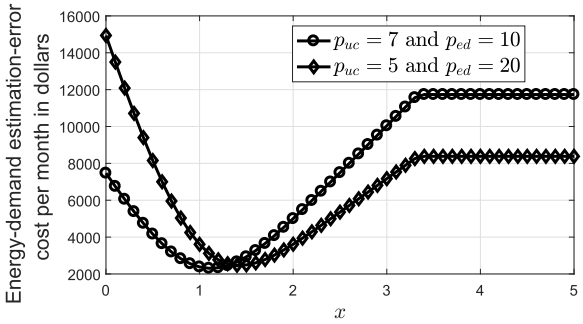

FIGURE 8. Impact of the parameter x on the energy-demand estimation-error cost.

The impact of the parameter x on the energy-demand estimation error is shown in Fig. 8. The parameter x is used to weight the mean of a consumer's average energy demand to get an estimate for the consumers' energy demands when there are wireless link outages. Interestingly, there is an optimal value of x that minimizes the energy-demand estimation-error cost and results in a lower monetary loss to the utility. This value depends on the average system's parameters (such as the energy-demand distributions of consumers, the means and variances of the distributions, the maximum energy-demand at consumers, and the outage probability of the wireless link). For the assumed system's parameters, the optimal value of x is 1.1 for $p_{uc} = 7$ cents/kWh and $p_{ed} = 10$ cents/kWh. Note that the cost difference between the case of $x = 1.1$ and $x = 1$ is negligible. Hence, instead of searching for the exact x that results in the minimum monetary loss, the utility (or the MDMS) can simply assume $x = 1$ which means that the energy-demand estimation of a consumer is its average obtained from the historical energy demands records of the consumers stored in the utility's database. Note that the optimal value of x moves away from $x = 1$ when the difference between the p_{ed} and p_{uc} is relatively high. For example, as shown in Fig. 8, when $p_{uc} = 5$ cents/kWh and $p_{ed} = 20$ cents/kWh, the optimal value of x is $x^\star = 1.5$. However, typically, the difference between p_{ed} and p_{uc} is not high, and hence, assuming $x = 1$ is reasonable. Finally, the saturation in the curves is due to the fact that the estimated energy E_n for consumer n cannot exceed the maximum energy demand of a consumer which is assumed to be $\text{Max}_n = 10$ kWh in our numerical results. Hence, increasing x (which results in an energy-demand estimation of $E_n = \mu x$) does not change the estimated energy demand at the utility or the energy-demand estimation-error cost.

VII. CONCLUSIONS AND FUTURE WORK

We presented a PHY reliability and security tradeoff analysis of the wireless communications system that enables DSM in the SG. Passive and active attacks effects were incorporated in this tradeoff analysis and their impacts on both the system's reliability and security were quantified. To improve the system's security, we proposed an AN-aided scheme and we showed that enhancing the security of the legitimate transmissions will decrease the reliability of the DMS functionality. The reason is that to secure the transmissions, a fraction of the transmit power will be assigned to AN transmissions instead of using all the transmit power for reliable data exchange with the gateways. To further secure the wireless communication system supporting the DMS and enhance its reliability, we proposed a new encoding scheme at the transmitting nodes where the energy demand information is securely encoded over the communication time slots in a given hour. Our numerical results quantified the negative impact of the wireless channel outages on the DSM reliability and the energy-demand estimation error monetary loss measured in dollars. Moreover, we quantified the gain of our proposed encoding scheme in terms of improving the DSM's security and reducing the monetary loss to the utility. In addition, we showed that our proposed AN-aided secure scheme reduces the secrecy outage probability of the wireless communications system supporting DSM and protects it against passive eavesdropping.

Future research includes an investigation of the case of multiple antennas at all nodes and proposing new AN-aided schemes based on this new degree of freedom to enhance the system's security against both eavesdropping and active attacks. In addition, a redundant design can be investigated where multiple gateways (Bobs) can be utilized in each subarea to enhance the reliability of wireless transmissions from the consumers to Bobs and from Bobs to George.

REFERENCES

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

[2] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2012.

[3] S. Dharmaraja, V. Jindal, and U. Varshney, "Reliability and survivability analysis for UMTS networks: An analytical approach," *IEEE Trans. Netw. Service Manage.*, vol. 5, no. 3, pp. 132–142, Sep. 2008.

[4] G. Egeland and P. E. Engelstad, "The availability and reliability of wireless multi-hop networks with stochastic link failures," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1132–1146, Sep. 2009.

[5] O. M. Al-Kofahi and A. E. Kamal, "Survivability strategies in multihop wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 71–80, Oct. 2010.

[6] A. G. Bruce, "Reliability analysis of electric utility SCADA systems," in *Proc. IEEE Int. Conf. Power Ind. Comput. Appl.*, May/Jun. 1997, pp. 200–205.

[7] Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.

[8] Y. Wang, W. Li, and J. Lu, "Reliability analysis of wide-area measurement system," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1483–1491, Jul. 2010.

[9] D. Niyato, P. Wang, and E. Hossain, "Reliability analysis and redundancy design of smart grid wireless communications system for demand side management," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 38–46, Jun. 2012.

[10] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[11] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[12] H. Su, M. Qiu, and H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 62–68, Aug. 2012.
[13] D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, "An enhanced public key infrastructure to secure smart grid wireless communication networks," *IEEE Netw.*, vol. 28, no. 1, pp. 10–16, Jan. 2014.
[14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[15] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*. New York, NY, USA: Springer, 2010, pp. 1–18.
[16] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel Gaussian wiretap channel," in *Proc. Global Telecommun. Conf. (Globecom)*, 2008, pp. 1–5.
[17] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.
[18] M. Kobayashi, M. Debbah, and S. Shamai (Shitz), "Secured communication over frequency-selective fading channels: A practical vandermonde precoding," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, p. 386547, Aug. 2009.
[19] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[20] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2009, pp. 2437–2440.
[21] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.
[22] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Enhancing the PHY-layer security of MIMO buffer-aided relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 400–403, Aug. 2016.
[23] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.
[24] T. Akitaya, S. Asano, and T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 807–812.
[25] A. El Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/document/7543526
[26] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. Int. Workshop Hybrid Syst., Comput. Control*, 2009, pp. 31–45.
[27] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.
[28] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Proc. ISRCS*, 2013, pp. 54–59.
[29] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proc. IEEE CDC*, Dec. 2013, pp. 5444–5449.
[30] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2011.
[31] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. IEEE CDC*, Dec. 2010, pp. 1096–1101.
[32] H. S. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proc. IEEE CDC*, Dec. 2012, pp. 2551–2556.
[33] B. Moradzadeh and K. Tomsovic, "Two-stage residential energy management considering network operational constraints," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 2339–2346, Dec. 2013.
[34] P. Samadi, H. Mohsenian-Rad, V. W. S. Wong, and R. Schober, "Utilizing renewable energy resources by adopting DSM techniques and storage facilities," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4221–4226.
[35] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

AHMED EL SHAFIE (M'10) received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, and the M.Sc. degree in communication and information technology from Nile University in 2014. He is currently pursuing the Ph.D. degree with The University of Texas at Dallas, USA. He received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer 2015, the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer 2016, and the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer 2016.

DUSIT NIYATO (M'09–SM'15–F'17) received the B.Eng. degree from the King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently an Associate Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the area of energy harvesting for wireless communication, Internet of Things, and sensor networks.

RIDHA HAMILA (SM'03) received the M.Sc., Licentiate of Technology (Hons.), and Doctor of Technology degrees from the Department of Information Technology, Tampere University of Technology (TUT), Tampere, Finland, in 1996, 1999, and 2002, respectively. From 1994 to 2002, he held various research and teaching positions at the Department of Information Technology, TUT. From 2002 to 2003, he was a System Specialist with the Nokia research Center and Nokia Networks, Helsinki. From 2004 to 2009, he was with the Etisalat University College, Emirates Telecommunications Corporation, UAE. He is currently an Associate Professor with the Department of Electrical Engineering, Qatar University, Qatar. He is also an Adjunct Professor with the Department of Communications Engineering, TUT. He has been involved in several past and current industrial projects Qtel, QNRF, Finnish Academy projects, TEKES, Nokia, EU research, and education programs. He supervised a large number of under/graduate students and post-doctoral fellows. His current research interests include mobile and broadband wireless communication systems, cellular and satellites-based positioning technologies and synchronization and DSP algorithms for flexible radio transceivers. In these areas, he has authored over 120 journal and conference papers most of them in the peer-reviewed IEEE publications, filed two patents, and wrote numerous confidential industrial research reports.

NAOFAL AL-DHAHIR (F'07) received the Ph.D. degree in electrical engineering from Stanford University. From 1994 to 2003, he was a Principal Member of the Technical Staff, GE Research and AT&T Shannon Laboratory. He is currently an Erik Jonsson Distinguished Professor with The University of Texas at Dallas. He is a Co-Inventor of 41 issued U.S. patents and a Co-Author of over 325 papers with over 8700 citations. He was a co-recipient of the four IEEE best paper awards, including the 2006 IEEE Donald G. Fink Award. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS.