Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming

Zhuo Lu, *Student Member, IEEE*, Wenye Wang, *Senior Member, IEEE*, and Cliff Wang, *Senior Member, IEEE*

Abstract—Smart grid is a cyber-physical system that integrates power infrastructures with information technologies. To facilitate efficient information exchange, wireless networks have been proposed to be widely used in the smart grid. However, the jamming attack that constantly broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. Hence, spread spectrum systems, which provide jamming resilience via multiple frequency and code channels, must be adapted to the smart grid for secure wireless communications, while at the same time providing latency guarantee for control messages. An open question is how to minimize message delay for timely smart grid communication under any potential jamming attack. To address this issue, we provide a paradigm shift from the *case-by-case* methodology, which is widely used in existing works to investigate well-adopted attack models, to the *worst-case* methodology, which offers delay performance guarantee for smart grid applications under any attack. We first define a generic jamming process that characterizes a wide range of existing attack models. Then, we show that in all strategies under the generic process, the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of traffic can in fact improve the worst-case delay performance. As a result, we demonstrate a lightweight yet promising system, transmitting adaptive camouflage traffic (TACT), to combat jamming attacks. TACT minimizes the message delay by generating extra traffic called *camouflage* to balance the network load at the optimum. Experiments show that TACT can decrease the probability that a message is not delivered on time in order of magnitude.

Index Terms—Smart grid, wireless applications, performance modeling, worst-case analysis, message delay, jamming attacks

1 Introduction

Smart grid is an emerging cyber-physical system that incorporates networked control mechanisms (e.g., advanced metering and demand response) into conventional power infrastructures [1]. To facilitate information delivery for such mechanisms, wireless networks that provide flexible and untethered network access have been proposed and designed for a variety of smart grid applications [2], [3], [4], [5], such as substation automation [2], [4] and home metering [5]. As a result, wireless networks have become an essential integration to the communication infrastructure for the smart grid.

However, the use of wireless networks introduces potential security vulnerabilities due to the shared nature of wireless channels. Indeed, it has been pointed out in [1], [6] that the jamming attack, which uses radio interference to disrupt wireless communications [7], [8], [9], can result in network performance degradation and even denial-of-service in power applications, thereby being a primary security threat to prevent the deployment of wireless networks for the smart grid. How to defend against jamming attacks is of critical importance to secure wireless communications in the smart grid.

There have been extensive works on designing spread spectrum based communication schemes, which provide jamming resilience to conventional wireless networks by using multiple orthogonal frequency [8], [10] or code [9], [11] channels. Interesting enough, most efforts adopt a case-by-case (or model-by-model) methodology to investigate how a message can be sent to its destination. In other words, based on commonly-adopted jamming attack models (e.g., periodic, memoryless, and reactive models [12]), existing works focus on designing anti-jamming communication schemes for message delivery in conventional wireless networks.

However, the NIST has recently imposed a strong requirement for smart grid security: *power system operations must be able to continue during any security attack or compromise (as much as possible)* [1]. This means that the widely-used case-by-case methodology cannot be readily adapted to wireless smart grid applications, because it is not able to guarantee reliable communication under any potential jamming attack. To provide such a guarantee, securing wireless smart grid applications requires a paradigm shift from the case-by-case methodology to a new *worst-case* methodology that offers performance assurance under any attack scenario. On the other hand, it has been shown that the message delay performance can be substantially worsen and even violate the timing requirement of control applications under inappropriate security design. For example, in an experimental substation network [13], if a RSA-based scheme is

- *Z. Lu and W. Wang are with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606. E-mail: {zlu3, wwang}@ncsu.edu.*
- *C. Wang is with Computer Sciences, Army Research Office, Research Triangle Park, NC. E-mail: cliff.wang@us.army.mil.*

Manuscript received 14 May 2013; revised 24 Mar. 2014; accepted 3 Apr. 2014. Date of publication 10 Apr. 2014; date of current version 16 Jan. 2015. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TDSC.2014.2316795

used for authenticating *trip protection* messages, 40 percent messages cannot be delivered and verified under the timing requirement of 3 ms. This show that in addition to the necessity of using the worst-case methodology, security design for the smart grid should also attempt to minimize the message delay such that it always meets the timing requirement. As a result, in this paper, we aim at solving a fundamental yet open question for wireless smart grid applications: *how to minimize the message delay under worst-case jamming attacks*. The answer to this question cannot only help us design network strategies against worst-case jamming attacks in wireless smart grid applications, but also offer general guidance into jamming defense strategies in cyber-physical systems.

In this paper, we address this issue by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for smart grid applications. We consider two general jamming-resilient communication modes for smart grid applications: coordinated and uncoordinated modes [8], [9], [10]. In coordinated mode, the sender and receiver share a common secret or key (e.g., code-frequency channel assignment), which is unknown to attackers. Accordingly, an attacker has to choose its own strategy to disrupt the communication between the transmitter and receiver. Coordinated communication is a conventional model in spread spectrum systems. However, the transmitter and receiver may not share a common secret initially (e.g., a node joins a network and attempts to establish a secret with others). Uncoordinated communication is therefore used to help establish such an initial key. In uncoordinated communication, the sender and receiver randomly choose a frequency-code channel to transmit and receive, respectively. A message can be delivered from the sender to the receiver only if they both reside at the same channel, and at the same time the jammer does not disrupt the transmission on the channel.

As power applications are time-critical with strict timing requirements (e.g., 3 and 10 ms in substation trip protection [14]), message delivery becomes invalid as long as its delay D is greater than the delay threshold σ. Therefore, different from existing metrics (e.g., throughput or packet delivery ratio [7]) to evaluate the jamming impact in conventional wireless networks, we use the message invalidation probability $\mathbb{P}(D > \sigma)$, which directly reflects timing requirements of power applications, to measure the jamming impact in the smart grid. Our goal is to minimize $\mathbb{P}(D > \sigma)$ under the worst-case jamming attack. To this end, we first define a generic jamming process that includes a wide range of existing jamming models. Then, we use both theoretical analysis and experimental study to derive $\mathbb{P}(D > \sigma)$ and accordingly design a solution to minimize $\mathbb{P}(D > \sigma)$ under jamming attacks. We highlight our major findings as follows:

1) We propose to study the worst-case performance under a generic (rather than specific) jamming process. We show, through mathematical derivations, that the worst-case performance in terms of message invalidation probability exhibits a U-shaped[1] response to aggregated network traffic load. In order words, the message invalidation probability is a first-decreasing, then-increasing function of network traffic load.
2) Based on this U-shape effect, we propose a transmitting adaptive camouflage traffic (TACT) system that uses "camouflage traffic" to achieve the optimal aggregated network traffic load to minimize the message invalidation ratio.

The underlying explanation behind the U-shape phenomenon and the TACT anti-jamming strategy is that using camouflage traffic (i.e., redundant traffic transmitted by TACT) is the over-provision of bandwidth in a smart grid network, where time-critical traffic rate is smaller than the network bandwidth. By sending more such camouflage traffic (mixed with smart grid control traffic) to the network, we can force a jammer to "waste" enough jamming capability on the camouflage traffic (because the jammer has no way to tell the camouflage traffic from the real smart grid traffic), so that the jammer cannot find the real traffic quickly enough. Therefore, the message invalidation ratio decreases when we send camouflage traffic into the network under jamming. However, if the rate of sending camouflage traffic keeps increasing and approaches the network bandwidth, more network collisions will happen in the network, thereby degrading the network performance (i.e., increasing the message invalidation ratio). As a result, there exists an optimal rate to send camouflage traffic and TACT is used to adaptively find this rate.

Because our strategy is based on the worst-case methodology, the U-shape property and the global minimum of the message invalidation probability are independent with a particular jamming strategy, thus offering performance guarantee for a wireless smart grid application under jamming attacks.

The rest of this paper is organized as follows. In Section 2, we introduce preliminaries and models. In Sections 3, 4, and 5, we derive the theoretical results, design the method of TACT, then implement TACT in our experimental smart grid system, Green Hub, respectively. Finally, we conclude in Section 6.

2 Models and Problem Formulation

In this section, we first introduce backgrounds on wireless networks for the smart grid, then present network and jamming models, finally formulate the problem.

2.1 Backgrounds: Smart Grid over Wireless

Wireless networks are in general used for local-area smart grid applications, such as substation automation and distributed energy management [2], [3]. The wireless network for a local-area power system consists of a number of intelligent electronic devices (IEDs) and the gateway node. IEDs are devices installed on infrastructures to fulfill power management procedures by communicating with each other. The gateway is connected to the smart grid backbone network. Local-area messages can be forwarded via the gateway to outside networks.

Due to the broadcast nature of wireless channels, wireless networks for the smart grid are inevitably exposed to

1. Mathematically, a function is said to be U-shaped if it is first-decreasing, then-increasing.

jamming attacks, which transmit radio interference to prevent legitimate messages from being received [7], [8], [9]. It has already been pointed out that jamming attacks, by disrupting communication between power equipments, can possibly result in grid operation instability or even regional blackout [15]. Therefore, wireless networks for the smart grid must have the ability to combat jamming attacks. There are two widely-used spread spectrum techniques [8], [9], [11], [16] to defend against jamming attacks in the literature. (i) Frequency hopping spread spectrum (FHSS): the sender and receiver switch a frequency channel among a pool of candidate channels from time to time. The jammer can only jam a transmission when it is on the same channel. (ii) Direct sequence spread spectrum (DSSS): the sender multiplies the original data with a pseudo-noise (PN) sequence (called a code channel). The receiver uses a correlator with the same PN sequence to recover the original message. It is difficult for a jammer to disrupt the communication unless it knows the PN sequence used by the channel.

Both FHSS and DSSS have been proposed and used for power applications [3], [15], [17], [18]. For example, a DSSS based system is demonstrated in [17] for local substation automation. Since FHSS and DSSS provide jamming resilience by using multiple orthogonal frequency and code channels, a trivial solution for decreasing the message delay is to increase the number of frequency or code channels. Then, a jammer will have a lower chance to transmit jamming signals on the same channel used by a transmit-receive pair. However, it is quite undesirable in practice because of the large cost of network spectrum resources. Therefore, we attempt to minimize the message delay in a wireless network with fixed numbers of frequency and code channels.

2.2 Network Model

We consider a wireless local-area network $\mathcal{N}(m, N_f, N_c)$, where m is the number of nodes (including IEDs and the gateway) in the network, N_f and N_c are the numbers of frequency and code channels, respectively. There are two major types of traffic flows in the network: 1) Local traffic, which is generated from one node to another for local monitoring or protection; 2) Outside traffic, which is between a node and an outside node via the smart grid backbone network.

For a message going outside, it will be delivered first from an IED to the gateway via the local-area network (local delivery), then to the destination network via the smart grid backbone network. If there exists a jammer, it can affect the delay performance of both local and outside traffic types. For outside traffic, the delay component for the first local delivery can dominate in the overall end-to-end delay, since the smart grid backbone network is always of high bandwidth. Therefore, we focus on the message delay of local traffic in the network.

It is worth noting that in the smart grid, a large amount of network traffic features a constant traffic model for continuous monitoring and control of power equipments [3], [14], [19]. In addition, nodes can have distinct network traffic loads for different applications. For example, merging-unit IEDs in a substation can send data of sampled power signal quality at various rates of 960-4,800 messages/, dependent on configuration [19]. Thus, we assume that there are heterogeneous traffic loads in network $\mathcal{N}(m, N_f, N_c)$; i.e., node i has a constant traffic load of λ_i messages/s ($i \in \{1, 2, \ldots, m\}$) in the network.

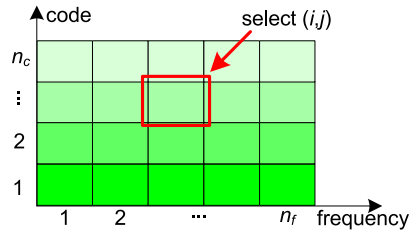


Fig. 1. N_f frequency and N_c code channels available.

2.3 Communication and Interference Models

2.3.1 Protocol Processing

In the smart grid, to ensure in-time monitoring and control of power devices, a large amount of communication messages have stringent timing requirements. For example, substation applications have 3-500 ms delay constraints for message delivery [14]. We refer to such messages as *time-critical* messages. The nature of time-critical messages indicates that they should be immediately transmitted and avoid being buffered. For example, time-critical messaging in substation communications [14] features a simple transmission mechanism at the application layer: bypass TCP and retransmit the same message multiple times to ensure timely delivery and reliability. Thus, we also adopt such a mechanism at the application layer of each node.

When a message is passed from the application layer to the MAC layer, traditionally, CSMA/CA is used to sense the channel activity before sending the message. However, CSMA/CA is primarily designed for one-channel networks, and may not be efficient in spread spectrum systems. In network $\mathcal{N}(m, N_f, N_c)$, the wireless channel is separated into N_f frequency and N_c code channels. Such channels can be considered orthogonal to each other [20]. Even if there are multiple wireless transmissions over the same frequency channel, they will be successfully decoded at receivers as long as they use distinct code channels. CSMA/CA, which defers a transmission after sensing activity on a frequency channel, may unintentionally degrade the delay performance.

Thus, we assume that when the MAC layer receives a message from upper layers, it will directly transmit the message on a frequency-code channel pair, denoted as the (i, j)th channel shown in Fig. 1. Since the application layer will retransmit the message multiple times, the MAC layer will assign a distinct frequency-code channel to each retransmission.

To correctly decode the message, the receiver must reside on the same frequency-code channel used by the sender. However, the receiver may or may not have the information of the sender's channel assignment, which leads to distinct communication modes between the sender and receiver. In what follows, we will consider extensively-used models in the literature.

2.3.2 Secret Communications and Key Establishment

As mentioned previously, two communicators may or may not share a common secret channel assignment (the key) with each other. If they do share a key, receiver can synchronize with the sender's frequency-code channel switching, which is called *coordinated communication mode*. In this mode, we assume that for a sender-receiver pair, each channel assignment is uniformly distributed over all $N_f N_c$ selections such that the chance of potential channel collision among legitimate nodes is minimized.

Coordinated communication happens only when two communicators share a secret unknown to others. However, they initially may not have such a secret. In fact, it is commonly adopted (e.g., [8], [10], [11]) that they share no secret key before they attempt to communicate. Then, how to establish a key before they use it to communicate coordinatedly? To solve the question, a wide-adopted solution (e.g., [8], [10], [11]) is *uncoordinated communication mode*, which is shown as follows.

First, assume that the two communicators can always verify each other's authenticity (e.g., their public keys are open to everyone). Every packet transmitted by the sender is digitally signed by the sender's private key. Then, the receiver can use the sender's public key to verify if a packet is indeed sent by the real sender.

Second, the sender keeps sending the key information to a randomly selected frequency/code channel. The information is encrypted (e.g., using the receiver's public key) such that it is only decodable to the real receiver. At the same time, the receiver randomly chooses a channel to listen on. When the sender and receiver reside on the same channel, the key information can be successfully delivered, thereby finishing the key establishment.

After the key establishment, the sender and receiver have shared a common secret key, so they can use the key to communicate. We can see that although uncoordinated communication looks less efficient, it is still essential to achieve coordinated communication. As a result, both uncoordinated and coordinated modes are vital for securing jamming-resilient communications.

Since channel selection is random in the uncoordinated mode, we adopt the uniform selection strategy [21], in which both sender and receiver uniformly choose channels to transmit and receive, respectively.

2.3.3 Interference Model

In coordinated mode, the sender and receiver have the common knowledge of the secret channel assignment, and can synchronize with each other. The transmission on a channel fails only when it is disrupted by jamming or other transmissions at the same channel. Thus, we assume that for coordinated communication, the message delivery on the (i,j)th channel fails when at least one of the following two events holds: 1) at least a portion ρ ($0 < \rho < 1$) of the transmission is disrupted by jamming on the (i,j)th channel; 2) at least a portion ρ of the transmission collides with other legitimate traffic on the (i,j)th channel.

For uncoordinated mode, message delivery failure can be caused by not only jamming or other transmissions on the same channel, but also the channel selection mismatch between the sender and receiver. Therefore, we assume that the message delivery with duration T_L on the (i,j)th channel fails if at least one of the following holds: 1) at least a portion ρ of the transmission is disrupted by jamming on the (i,j)th channel; 2) at least a portion ρ of the transmission collides with other legitimate traffic on the (i,j)th channel; 3) During the message transmission, the receiver resides on the (i,j)th channel for a time duration smaller than $(1-\rho)T_L$.

Note that the value of ρ varies in practice, depending on error correction coding. For example, the standard (255,223) Reed-Solomon code is used in the transmission, it is capable of correcting up to 16 bit errors among every 223 information bits [9], resulting in $\rho \approx 7.1$ percent.

2.4 Generic Jamming Model

The objective of a jammer is to broadcast interference to disrupt messages as many as possible in network $\mathcal{N}(m, N_f, N_c)$. As the network has multiple channels, the jammer can adopt a wide range of strategies. In the literature, there are two major jamming types in terms of jamming behavior: non-reactive and reactive models [7], [8], [9], [10], [11]. Non-reactive jammers transmit radio interference by following their own strategies. Reactive jammers transmit interference only when they sense any activity on a wireless channel. In addition, a jammer can either target a single frequency-code channel or have the ability to attack multiple channels at the same time. In this paper, we assume that the jammer has the knowledge of the pool of candidate channels used in the network, and attempt to choose the best strategy to attack one or some of the channels and lead the worst-case attack. In order to adopt varying strategies the jammer can use, we define a generic process to accommodate various jamming behaviors and models in the literature.

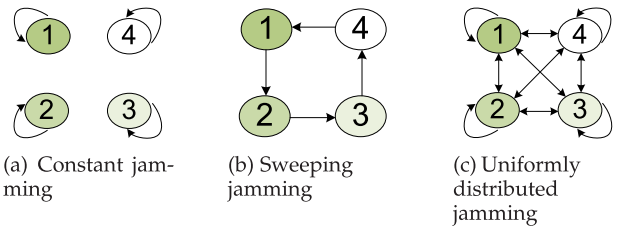
Definition 1 (Generic Jamming Process). *A jamming attack can be represented as a Markov-renewal process*

$$((\mathcal{F},\mathcal{C}),X) = \{(\mathcal{F}_k,\mathcal{C}_k), X_k | k = 1,2,\ldots\},$$

where X_k is the renewal interval representing the jamming duration at the kth state, denoted by $(\mathcal{F}_k,\mathcal{C}_k) = \{(F_{k,i}, C_{k,i})\}_{i\in[1,s]}$, the set of frequency and code channels targeted by the jammer, $(F_{k,i}, C_{k,i})$ is a particular frequency and code channel, and s is the number of channels the jammer can attack simultaneously. The embedded transition matrices associated with states $(\mathcal{F}_k,\mathcal{C}_k)$ are denoted as $\mathbf{Q}_f$ and $\mathbf{Q}_c$, respectively. When the jamming is non-reactive, $((\mathcal{F},\mathcal{C}),X)$ is assumed to be a continuous Markov process. When the jamming is reactive, $X_k = \tau + S_k \mathbf{1}_A$,[2] where τ is the constant channel sensing time, S_k is the duration of the jamming signal, A denotes the event that at least one channel in set $(\mathcal{F}_k,\mathcal{C}_k)$ is sensed busy.

Remark 1. The generic jamming process can characterize both non-reactive and reactive jamming behaviors. In addition, it also models jammers that can attack $s \geq 1$ frequency-codechannels at the same time. Thus, the generic model defined in Definition 1 can represent a

2. $\mathbf{1}_A$ denotes the indicator function, which has the value 1 for A and the value 0 for A^c.



(a) Constant jamming (b) Sweeping jamming (c) Uniformly distributed jamming

Fig. 2. Jamming strategies due to state transitions.

wide range of existing jamming models and strategies in the literature. For example, consider a simple network with four frequency channels in the presence of a jammer that can attack only one frequency channel at the same time. If the jammer's transition matrix $\mathbf{Q}_f$ is the 4×4 identity matrix with state transitions shown in Fig. 2a, every state is an absorbing state and the process represents continuous jamming on a particular channel [7]. Similarly, Figs. 2b and 2c represent sweeping jamming [22] and uniformly-distributed jamming, respectively.

As we can see in the Markov-renewal model, $\{X_k\}$ and $\{(\mathcal{F}_k, \mathcal{C}_k)\}$ can directly reflect when a certain set of channels is affected by the jamming attack, and matrices $\mathbf{Q}_f$ and $\mathbf{Q}_c$ can model what the jamming strategy is.

2.5 Problem Formulation

The primary goal of smart grid communication is to achieve timely monitoring and control for power control applications. Therefore, the delay performance is of critical importance in the smart grid. A time-critical message becomes invalid as long as its message delay D is greater than its delay constraint σ. As a result, we focus on how to minimize the message invalidation probability $\mathbb{P}(D > \sigma)$ in network $\mathcal{N}(m, N_f, N_c)$ under the generic jamming process $((\mathcal{F}, \mathcal{C}), X)$.

It is worth noting that there are two opposites in the network: the network operator always attempts to minimize the message delay; in contrast, the jammer always intends to maximize the message delay. The lowest bound of the message delay is always achieved when there exists no jammer or a naive jammer. As the NIST requires smart grid operations must continue under any potential attack, we adopt a worst-case methodology to study the problem of minimizing message delay in the smart grid under jamming attacks:

1. In wireless local-area network $\mathcal{N}(m, N_f, N_c)$, for a time-critical application with delay threshold σ, what is the worst-case delay performance $\mathbb{P}(D > \sigma)$ under the generic jamming process $((\mathcal{F}, \mathcal{C}), X)$.
2. Given the worst-case scenario in Step 1, how to minimize $\mathbb{P}(D > \sigma)$.

There has been existing work addressing denial-of-service attacks on multimedia traffic (e.g., [23], [24]). We note that the differences between smart grid traffic and multimedia traffic are: 1) smart grid traffic is more time-critical (e.g., 3 ms requirement in GOOSE compared with around 100 ms requirement for multimedia), 2) time-critical traffic is periodical, unsaturated (i.e., the traffic load smaller than the network bandwidth) in the smart grid, and multimedia traffic is usually saturated and requires adequate congestion control. As a result, the smart grid traffic features a simpler retransmission mechanism without congestion control. In addition, we will show that we can take advantage of the unsaturated nature of smart grid traffic to design countermeasures.

Next, we use theoretical analysis to show the worst-case delay performance under jamming attacks.

3 Theoretical Analysis

In this section, we theoretically analyze the worst-case delay performance for wireless smart grid applications under the generic jamming model. We first consider the worst case in coordinated communication, then the worst case in uncoordinated communication. Finally, we propose a method to minimize the worst-case delay for both coordinated and uncoordinated modes.

3.1 Jamming against Coordinated Mode

Our goal is to find the jamming attack that maximizes $\mathbb{P}(D > \sigma)$ such that we can identify the worst-case attack targeting wireless smart grid applications. As our generic jamming process characterizes both non-reactive and reactive jammers, we provide analytical results of their impacts on $\mathbb{P}(D > \sigma)$, respectively.

Lemma 1 (Non-Reactive Jamming). *In wireless local-area network $\mathcal{N}(m, N_f, N_c)$ in the presence of a non-reactive jamming process $\{(\mathcal{F}, \mathcal{C}), X\}$ with ability to attack s channels simultaneously, the message delay D_k of a time-critical application at node k satisfies*

$$\mathbb{P}(D_k > \sigma) \leq \left(1 - \left(1 - \frac{1}{N_f N_c}\right)^{2T_L(1-\rho)\gamma_k} \left(1 - \frac{(1-\rho)s}{\rho N_f N_c}\right)\right)^{\sigma/T_L}, \quad (1)$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1, j\neq k}^{m} \lambda_j$, and λ_j is the traffic rate at node j.

Proof. Without loss of generality, assume that node 1 transmits a message with delay threshold σ and duration T_L. The application layer can transmit the message at most $\lfloor \sigma/T_L \rfloor$ times (for the sake of simplicity, we in the following assume that σ/T_L is an integer, i.e., $\lfloor \sigma/T_L \rfloor = \sigma/T_L$, which does not affect the derivation of our main results). Among all σ/T_L transmission attempts, the ith one uses the (u_i, v_i)th channel ($1 \leq i \leq \sigma/T_L$).

The message invalidation probability $\mathbb{P}(D_1 > \sigma)$ is equal to the probability that all σ/T_L transmission attempts are disrupted by either collision or jamming, i.e.,

$$\mathbb{P}(D_1 > \sigma) = \mathbb{P}\Big(\cap_{i=1}^{\sigma/T_L}(J_i \cup C_i)\Big), \quad (2)$$

where C_i and J_i denote the events that the ith transmission is disrupted by collision and jamming, respectively.

First, we derive the collision probability $\mathbb{P}(C_i)$. Suppose that node 1's ith transmission starts at time 0, a collision that can successfully disrupt node 1's transmission will happen if another node makes a transmission attempt during period $[(\rho - 1)T_L, (1 - \rho)T_L]$ and at the

same time uses the same channel. Since all nodes have constant traffic rates, there are $2(1-\rho)T_L\sum_{j=2}^{m}\lambda_j$ transmissions at other nodes that can possibly disrupt node 1's transmission. As the frequency-code channel for each transmission in the network is uniformly assigned among all N_fN_c selections, the collision probability is equal to the probability that there is at least one other transmission colliding with node 1's ith transmission, which can be written as

$$\mathbb{P}(C_i) = 1 - \left(1 - 1/(N_fN_c)\right)^{2(1-\rho)T_L\gamma_1}, \tag{3}$$

where $\gamma_1 = \sum_{j=2}^{m}\lambda_j$.

Then, we compute the jamming probability $\mathbb{P}(J_i)$. The jamming process $\{(\mathcal{F},\mathcal{C}), X\}$ has renewal intervals $\{X_l\}$. Let N_i represent how many times the jammer makes a state transition, and we have $N_i = sup_{n\in\mathbb{N}}\{\sum_{l=1}^{n} X_l < (1-\rho)T_L\}, \mathbb{N} = \{0,1,2,\ldots\}$, where $X_1,\ldots,X_{N_i}$ are jamming intervals during the ith transmission. In order to disrupt the ith transmission (i.e., J_i holds), the sum of jamming intervals on the (i,j)th channel must be larger than the threshold ρT_L. Letting B_l be the event that the lth interval with length X_l hits the (u_i,v_i)'th channel (i.e., $B_l = \{u_i \in F_l, v_i \in C_l\}$), we obtain

$$\begin{aligned}\mathbb{P}(J_i|u_i,v_i) &= \mathbb{P}\left(\sum_{l=1}^{N_i} X_l\mathbf{1}_{B_l} \geq \rho T_L\right) \leq \mathbb{E}\left(\sum_{l=1}^{N_i} X_l\mathbf{1}_{B_l}\right)/(\rho T_L)\\ &= \mathbb{E}(N_i)\mathbb{E}(X_l)\mathbb{P}(B_l)/(\rho T_L),\end{aligned} \tag{4}$$

where the last equality and inequality follows from Wald's equation and Markov's inequality respectively, $\mathbb{E}(N_i) = (1-\rho)T_L/\mathbb{E}(X_l)$ and $\mathbb{P}(B_l)$ denotes the probability that the jamming hits the (u_i,v_i)th channel. Since (u_i,v_i) is uniformly assigned, it follows from (4) that

$$\begin{aligned}\mathbb{P}(J_i) &\leq \sum_{p=1}^{N_f}\sum_{q=1}^{N_c}\mathbb{E}(N_i)\mathbb{E}(X_l)\mathbb{P}(B_l)/(\rho T_L)/(N_fN_c)\\ &\leq \frac{(1-\rho)T_L}{\mathbb{E}(X_l)}\mathbb{E}(X_l)\frac{s}{N_fN_c}\frac{1}{\rho T_L} = \frac{(1-\rho)s}{\rho N_fN_c}.\end{aligned} \tag{5}$$

Finally, combining (2), (3) and (5) finishes the proof. □

Next, we present our results on reactive jamming.

Lemma 2 (Reactive Jamming). *In wireless local-area network $\mathcal{N}(m,N_f,N_c)$ in the presence of a reactive jammer $\{(\mathcal{F},\mathcal{C}),X\}$ that has sensing time τ and can attack s channels simultaneously, for a time-critical application at node k, its message delivery delay D_k satisfies*

$$\mathbb{P}(D_k > \sigma) \leq \left(1 - \left(1 - \frac{1}{N_fN_c}\right)^{2T_L(1-\rho)\gamma_k}\left(1 - \frac{sT_L}{\frac{\tau N_fN_c}{1-\rho} + \rho T_L^2\gamma_k}\right)\right)^{\sigma/T_L}, \tag{6}$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1,j\neq k}^{m}\lambda_j$, and λ_j is the traffic rate at node j.

Proof. Similar to the proof for Lemma 1, assume that node 1 transmits a message with delay threshold σ. The transmission resides at the (u_i,v_i)th channel for the ith attempt. To find $\mathbb{P}(D_1 > \sigma)$, we first need to compute both collision and jamming probabilities, $\mathbb{P}(C_i)$ and $\mathbb{P}(J_i)$. As $\mathbb{P}(C_i)$ is given in (3), we in the following compute $\mathbb{P}(J_i)$.

For the sake of simplicity, assume that the ith transmission starts at time 0. Define a renewal process $N_i(t) = \sup_{n\in\mathbb{N}}\{\sum_{l=1}^{n} X_l < t\}, \mathbb{N} = \{0,1,2,\ldots\}$. Then X_1, $X_2,\ldots,X_{N_i(t)}$ are renewal intervals during period $[0,t]$. Different from non-reactive jamming, reactive jamming has renewal intervals $X_l = \tau + S_l\mathbf{1}_A$, where A denotes the event that a channel is sensed with activity, and S_l is the jamming duration. To maximize its damage to the network, the reactive jammer should always set the jamming duration S_l to be ρT_L. This means that when the jammer senses a transmission, it always chooses the minimum effective jamming duration to disrupt the transmission such that it can immediately move on to sense and jam other channels. Thus, we choose $S_l = \rho T_L$.

In order to successfully disrupt the ith transmission (e.g., J_i holds), the reactive jammer must switch to the (u_i,v_i)th channel at least once during $[0,(1-\rho)T_L-\tau]$. Let event $B_l = \{u_i \in \mathcal{F}_l\, v_i \in \mathcal{C}_l\}$. Then, $\mathbb{P}(J_i|u_i,v_i) = \mathbb{P}(\sum_{l=1}^{N_i((1-\rho)T_L-\tau)}\mathbf{1}_{B_l} \geq 1)$. Using similar procedures in (4) and (5), we have

$$\mathbb{P}(J_i) \leq \mathbb{E}(N_i((1-\rho)T_L-\tau)s/(N_fN_c). \tag{7}$$

To obtain $\mathbb{E}(N_i((1-\rho)T_L-\tau)$, we first have from the elementary renewal theorem

$$\lim_{t\to\infty}\mathbb{E}(N_i(t))/t = 1/\mathbb{E}(X_l), \tag{8}$$

where $\mathbb{E}(X_l) = \tau + \rho T_L\mathbb{P}(A)$, $\mathbb{P}(A)$ is the probability that a channel is sensed busy and $\mathbb{P}(A) = 1-(1-1/(N_fN_c))^{(1-\rho)T_L\gamma_1}$. Then, it is reasonable to assume that sensing time $\tau \ll T_L$ and renewal interval $\mathbb{E}(X_l) \ll T_L$ since power networks always have unsaturated traffic loads [3], [14] for timely monitoring and control. Thus, from (8), $\mathbb{E}(N_i((1-\rho)T_L-\tau)$ can be approximated as

$$\begin{aligned}\mathbb{E}(N_i((1-\rho)T_L-\tau)) &\approx \frac{(1-\rho)T_L-\tau}{\mathbb{E}(X_l)} \approx \frac{(1-\rho)T_L}{\mathbb{E}(X_l)}\\ &= \frac{(1-\rho)T_L}{\tau + \rho T_L - \rho T_L\left(1-\frac{1}{N_fN_c}\right)^{(1-\rho)T_L\gamma_1}} \approx \frac{(1-\rho)T_L}{\tau + \frac{\rho(1-\rho)T_L^2\gamma_1}{N_fN_c}}.\end{aligned} \tag{9}$$

The last approximation follows from the fact that $(1-x)^a \approx 1-ax$ for small x. From (7) and (9), we obtain

$$\mathbb{P}(J_i) \leq \frac{(1-\rho)sT_L}{\tau N_fN_c + \rho(1-\rho)T_L^2\gamma_1}. \tag{10}$$

Combining (2), (3) and (10) completes the proof. □

Based on Lemmas 1 and 2, we then show that reactive jamming in general leads to the worst-case delay performance, thereby maximizing the damage to the network.

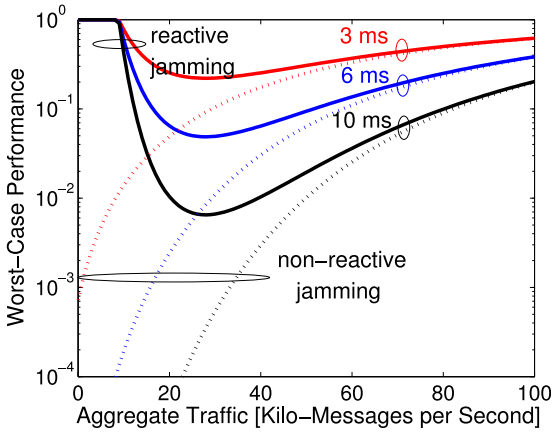


Fig. 3. Coordinated communication: worst-case delay performance $\mathbb{P}(D_k > \sigma)$ versus aggregate traffic γ_k at node k for time-critical applications with delay thresholds of 3-9 ms. ($N_f = N_c = 10$, $T_L = 1$ ms, $\rho = 0.1$, and $\tau = 1$ μs.)

Theorem 1 (Worst-case delay in coordinated mode). *For wireless local-area network $\mathcal{N}(m, N_f, N_c)$ under coordinated communication, the worst-case delay performance at node k is induced by reactive jamming with sensing time τ sufficiently small. Specifically, the message delay D_k satisfies*

$$\mathbb{P}(D_k > \sigma) \leq \left(1 - \left(1 - \frac{1}{N_f N_c}\right)^{2T_L(1-\rho)\gamma_k} \left(1 - \frac{sT_L}{\frac{\tau N_f N_c}{1-\rho} + \rho T_L^2 \gamma_k}\right)\right)^{\sigma/T_L}, \tag{11}$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1, j\neq k}^{m} \lambda_j$, and λ_j is the traffic rate at node j.

Proof. Comparing (1) with (6), it suffices to show

$$\frac{(1-\rho)sT_L}{\tau N_f N_c + \rho(1-\rho)T_L^2\gamma_k} \geq \frac{s}{\rho N_f N_c}, \tag{12}$$

which is equivalent to

$$\tau \leq \rho T_L - \rho(1-\rho)T_L^2\gamma_k/(N_f N_c). \tag{13}$$

In order for (13) to hold for τ sufficiently small, it suffices to show that the right-hand side of (13) is larger than 0, i.e., $\rho T_L - \rho(1-\rho)T_L^2\gamma_k/(N_f N_c) > 0$. Let $\hat{\gamma}$ be the overall message rate in the network and B be the maximum bit rate supported by each sub-channel. Then, a single message includes $T_L B$ bits, and the overall network traffic rate (in terms of bits/s) can be written as $\hat{r} = T_L B\hat{\gamma}$, which is smaller than the overall channel bandwidth $N_f N_c B$. In other words, we have $\hat{r} = T_L B\hat{\gamma} \leq N_f N_c B$, i.e., $T_L\hat{\gamma} \leq N_f N_c$. Since it always holds that $\gamma_k \leq \hat{\gamma}$, we have $T_L\gamma_k \leq N_f N_c$ and

$$\rho T_L - (\rho(1-\rho)T_L^2\gamma_k)/(N_f N_c) \geq \rho T_L - \rho(1-\rho)T_L > 0, \tag{14}$$

which finishes the proof. □

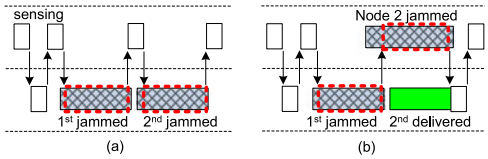


Fig. 4. Message delivery under reactive jamming.

Remark 2. Theorem 1 shows that reactive jamming with sensing time τ sufficiently small will induce the worst-case performance. Theoretically, we can always assume that τ is arbitrarily small and consider reactive jamming as the worst case. Will reactive jamming do so in practice? The essence of the question is how small τ can be for a practical jammer. Taking a closer look at (13), we find that the right-hand side can be approximated as ρT_L when the pool of channel selections is large (i.e., $N_f N_c$ is large), which is true for an effective anti-jamming system. This indicates that reactive jamming is more harmful than non-reactive jamming when τ is smaller than the minimum jamming duration ρT_L. It has been shown that τ can be designed very small, depending on implementation; while ρT_L should be kept relatively large to effectively disrupt a transmission. For example, a software-defined radio based jammer [25] needs 20 μs to sense an 802.15.4 transmission and send jamming signals for at least 26 μs to disrupt the transmission. Such a sensing time can be further shorten with a hardware implementation instead of a software implementation, which demonstrates that τ is indeed smaller than ρT_L in practice. Therefore, it is reasonable to consider reactive jamming as the worst case both theoretically and practically.

Fig. 3 shows an example of the worst-case message invalidation probabilities induced by both non-reactive (1) and reactive jamming (6) for time-critical applications at node k. We can see that reactive jamming always leads to worse delay performance than non-reactive jamming, and that the delay performance at node k also depends on the aggregate traffic load γ_k. An interesting observation from Fig. 3 is that in the reactive-jamming case, the message invalidation probability is not minimized at $\gamma_k^* = 0$. Instead, it is minimized at a fairly large value $\gamma_k^* \approx 38$ kilo-messages/s.

Fig. 3 illustrates that, interestingly, the worst-case delay (caused by reactive jamming) is in fact a U-shaped (first-decreasing then-increasing) function of traffic load γ_k. This is due to the sensing and reacting nature of reactive jamming. Consider a simple example: Fig. 4a shows two transmissions of a message by node 1 with two-channel frequency-hopping. If there is no other traffic, by scanning the two channels alternately, a reactive jammer can always sense and jam both transmissions. If node 2 is also transmitting as shown in Fig. 4b, the jammer can also sense and attempt to disrupt node 2's transmission. Then, there is a chance that node 1's message can be delivered during the time that the jammer is jamming node 2's transmission. Thus, fairly increasing network traffic load can in fact improve the delay performance under reactive jamming. On the other hand, the over-increase of traffic will surely decrease the performance since transmissions have a high probability to collide with each other. Hence,

there should be an optimal traffic load such that the worst-case message delay can be minimized.

In the following, we show theoretically that there exists a traffic load γ_k^* to minimize the worst-case message invalidation probability for node k in the network.

Theorem 2 (Optimal load in coordinated mode). *In wireless network $\mathcal{N}(m, N_f, N_c)$, node k's worse-case message invalidation probability (11) in coordinated communication is minimized at*

$$\gamma_k^* = \frac{1}{\rho(1-\rho)T_L^2}\left(\frac{c_1c_2 - \sqrt{c_1^2c_2^2 - 4c_1c_2\rho T_L}}{2c_1} - \tau N_f N_c\right),$$

where $c_1 = 2\ln(1-1/(N_fN_c))$ and $c_2 = (1-\rho)T_L$.

Proof. It is equivalent to show that γ_k^* maximizes the following function:

$$f(\gamma_k) = \left(1 - \frac{1}{N_fN_c}\right)^{2T_L(1-\rho)\gamma_k}\left(1 - \frac{(1-\rho)T_L}{\tau N_fN_c + \rho(1-\rho)T_L^2\gamma_k}\right). \tag{15}$$

Letting $\nabla_{\gamma_k^*} f(\gamma_k^*) = 0$ results in a quadratic equation

$$c_1w^2 - c_1c_2w + c_2\rho T_L = 0, \tag{16}$$

where $c_1 = 2\ln(1-1/(N_fN_c))$, $c_2 = (1-\rho)T_L$, and

$$w = \tau N_fN_c + \rho(1-\rho)T_L^2\gamma_k^*. \tag{17}$$

Solving equation (16) for w yields

$$w = \left(c_1c_2 - \sqrt{c_1^2c_2^2 - 4c_1c_2\rho T_L}\right)/(2c_1). \tag{18}$$

Combining (17) with (18) completes the proof. □

Remark 3. Theorem 2 shows that there indeed exists a unique traffic load γ_k^* for node k to minimize its worst-case delay, and that γ_k^* is independent of the delay threshold σ, which can be also observed in Fig. 3. Thus, the delay of messages with different delay thresholds can be all minimized at the same optimal traffic load.

3.2 Jamming against Uncoordinated Mode

So far, we have derived the theoretical results of the worst-case jamming impact on coordinated communication, which is used for IED communication in normal operations in the smart grid. We show that, interestingly, there indeed exists a unique traffic load for a node to minimize its worst-case delay. In the following, we present the theoretical results on uncoordinated communication, which can be used for key establishment between IEDs. Similar to Section 3.1, our goal is to find out the worst case performance, $\mathbb{P}(D > \sigma)$, for uncoordinated communication under both non-reactive and reactive jamming attacks.

Theorem 3 (Worst case delay in uncoordinated mode). *For wireless local-area network $\mathcal{N}(m, N_f, N_c)$ under uncoordinated communication, the worst-case delay performance at node k is induced by the reactive jamming with sensing time τ sufficiently small. Specifically, the message delay D_k satisfies $\mathbb{P}(D_k > \sigma)$*

$$\leq \left(1 - \frac{(N_fN_c-1)^{2T_L(1-\rho)\gamma_k}}{(N_fN_c)^{2T_L(1-\rho)\gamma_k+1}}\left(1 - \frac{sT_L}{\frac{\tau N_fN_c}{1-\rho} + \rho T_L^2\gamma_k}\right)\right)^{\sigma/T_L}, \tag{19}$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1, j\neq k}^{m}\lambda_j$, and λ_j is the traffic rate at node j.

Proof. Without loss if generality, assume that node 1 attempts to transmit a message with duration T_L to node 2 using the uncoordinated mode, in which nodes 1 and 2 uniformly choose a frequency-code channel to transmit and receive, respectively. They switch channels from time to time. For the sake of simplicity, the time is partitioned into time slots with length T_L. The sender and receiver switch their channels at the beginning of each time slot. Assume that for the ith delivery attempt ($1 \leq i \leq \sigma/T_L$), nodes 1 and 2 reside at the (u_i, v_i)th channel and the (d_i, e_i)th channel, respectively.

The message invalidation probability is written as

$$\mathbb{P}(D_1 > \sigma) = \mathbb{P}\Big(\cap_{i=1}^{\sigma/T_L}(C_i \cup J_i \cup M_i)\Big), \tag{20}$$

where C_i and J_i denote the events that the ith transmission is disrupted by collision and jamming, respectively; and M_i denotes the event that there is a channel mismatch between the sender and receiver, i.e., $M_i = \{u_i \neq d_i\} \cup \{v_i \neq e_i\}$.

To find $\mathbb{P}(D_1 > \sigma)$, we need to compute the collision probability $P(C_i)$, jamming probability $P(J_i)$, and the mismatch probability $P(M_i)$, respectively. Since we have already obtained $P(C_i)$ in (3), as well as $P(J_i)$ in (5) and (10) under non-reactive and reactive jamming attacks, we in the following derive $P(M_i)$, which is the probability that node 1 does not reside at the same channel as node 2, i.e., either $u_i \neq d_i$ or $v_i \neq e_i$. We have

$$\mathbb{P}(M_i) = \mathbb{P}(\{u_i \neq d_i\} \cup \{v_i \neq e_i\}) = 1 - 1/(N_fN_c). \tag{21}$$

With (20), (21), (3), (5) and (10), using similar procedures in Theorem 1, we get $\mathbb{P}(D > \sigma)$ satisfies (19). □

Fig. 5 shows an example of the worst-case message invalidation probabilities for a time-critical application in both coordinated and uncoordinated modes. It is observed that similar to coordinated communication, the worst-case message invalidation probability in uncoordinated communication exhibits U-shaped curves in Fig. 5, indicating that the delay performance in uncoordinated communication also depends on the aggregate traffic load γ_k, and can be minimized by optimizing γ_k. However, the delay performance in uncoordinated communication is substantially worse than that in coordinated communication. This is due to the opportunistic nature of uncoordinated communication: the sender and receiver have to randomly select channels to transmit and receive, respectively. Fig. 5 implies that in general, uncoordinated communication should not be used for time-critical message delivery.

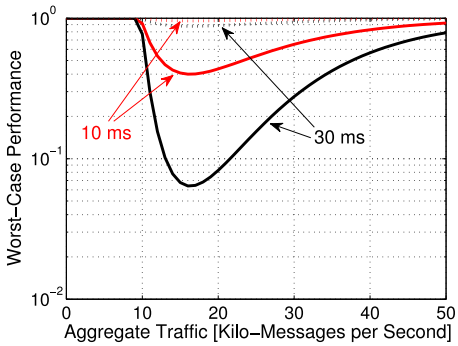


Fig. 5. Uncoordinated communication: worst-case $\mathbb{P}(D_k > \sigma)$ versus γ_k with delay thresholds of 10 and 30 ms. (N_f=10, N_c=2, T_L=1 ms, ρ=0.1, and $\tau = 1$ μs.)

Another observation in Fig. 5 is that the message invalidation probability is always minimized at the same traffic load regardless of communication modes. For example, we can see that the probabilities for all four cases in Fig. 5 are all minimized at $\gamma_k \approx 19$ kilo-messages/s. This shows that if we have the same setups in a wireless network, there exists one optimal traffic load for a node to minimize its message invalidation probability in both coordinated and uncoordinated communications, which is formally proved in the following.

Theorem 4 (Optimal load in uncoordinated mode). *In a network with setups stated in Theorem 2, the optimal load γ_k^* in coordinated mode also minimizes the message invalidation probability in uncoordinated mode.*

Proof. For uncoordinated communication, in order to minimize (19) (as a function of γ_k), it is equivalent to find the value of γ_k to maximize function

$$g(\gamma_k) = \frac{(N_f N_c - 1)^{T_L(1-\rho)\gamma_k}}{(N_f N_c)^{T_L(1-\rho)\gamma_k + 1}} \left(1 - \frac{(1-\rho)sT_L}{\tau N_f N_c + \rho(1-\rho)T_L^2 \gamma_k}\right) = f(\gamma_k)/(N_f N_c), \tag{22}$$

where $f(\gamma_k)$ is given in (15), which is the objective function in the coordinated mode. Hence, finding γ_k^* that maximizes $g(\gamma_k)$ is equivalent to finding γ_k^* that maximizes $f(\gamma_k)$. Therefore, γ_k^* also minimizes the message invalidation probabilities in uncoordinated mode. □

Remark 4. Despite the evident performance difference between coordinated and uncoordinated communications, Theorem 4 illustrates that their delay performance can be optimized at the same time by choosing one optimum traffic load in the network. In the smart grid, a node's traffic load is usually static and quite unsaturated for real-time power management. For example, wireless monitoring for substation transformers only needs to transmit a message every second [2]. This indicates that in general, we should intentionally increase a certain amount of redundant traffic to obtain the optimal traffic load. Then, legitimate messages can have a chance to be successfully delivered during the period that jamming attacks attempt to disrupt redundant traffic. We name such traffic as *camouflage traffic* since it serves as camouflage to "hide" legitimate traffic from attacks.

4 TACT System

We have shown that for both coordinated and uncoordinated communications in wireless smart grid applications, the delay performance is sensitive to the network traffic load under jamming attacks. As a result, generating camouflage traffic is promising to improve the worst-case delay performance. In this section, we present our adaptive method that generates camouflage traffic to minimize the message delivery delay in wireless networks for smart grid applications.

4.1 Motivation and Method Design

Our objective is to design a feasible method to minimize the worst case delay performance for practical wireless smart grid applications under jamming attacks. We first describe the general idea of our method, which can be used for both coordinated and uncoordinated communication modes. Notice that Theorem 2 shows that the optimal load γ_k^* is a function of message transmission time T_L, which depends on message length L. If all nodes' messages have the same length, the optimal load for every node will be the same, i.e., $\gamma_1^* = \gamma_2^* = \cdots = \gamma_m^*$. However, in the smart grid, a node has different message types with distinct lengths. For example, monitoring and control messages in substations can have lengths of 98 and 16 bytes [19], respectively. Thus, it is impossible to use one optimal load to minimize the delay for all message types. A reasonable choice is to generate camouflage traffic at the optimal point to minimize the delay for the most time-critical messages, since such messages are of the most importance and generally used for protection procedures [14], [19]. Therefore, to obtain the optimal traffic load γ_k^*, T_L is chosen to be the transmission time of the most time-critical messages. Then, we have $\gamma_1^* = \gamma_2^* = \cdots = \gamma_m^*$.

It is also worthy of mention that the optimal traffic load γ_k^* is a function of the jammer's sensing time τ. As τ varies in practice, it is difficult to pre-configure network setups to generate camouflage traffic at the optimal load. An appropriate strategy is to adaptively generate traffic at each node into the network such that the overall network traffic load can be balanced around the optimum. Thus, we design the TACT method (transmitting adaptive camouflage traffic). The intuition behind TACT is two-fold. 1) TACT should avoid node coordination. Admittedly, node coordination can further help improve the delay performance. However, it introduces an additional security issue of coordination message delivery under jamming. Thus, TACT should be of distributed nature, inducing the minimum complexity and node coordination. 2) Since the worst-case message delay is minimized at a positive traffic load, TACT should always attempt to increase the traffic load. If the performance is degraded after the increase, it can reduce the load.

Accordingly, we propose to implement the TACT method at every node in a wireless network for the smart grid. As shown in Algorithm 1, TACT measures the delivery results of probing messages to adjust the amount of camouflage messages in the network. Each camouflage message is transmitted on a randomly selected frequency/code channel. When TACT is deployed, there are three major traffic types in the network: i) *routine traffic* for power

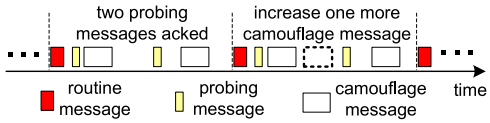


Fig. 6. How TACT balances the network traffic.

monitoring and control, which cannot be changed as it is coupled with setups of power devices, ii) *probing traffic* for performance measurement, its message transmission time equals to T_L, iii) *camouflage traffic* to balance the overall network traffic load. Fig. 6 shows an example of traffic dynamics caused by TACT: in the first observation period, two probing messages are both ACKed, meaning that current traffic load is not harmful. Then, TACT sends one more camouflage message in the next observation period. The traffic load will keep being increased until it reaches the optimum, and finally fluctuate around the optimum.

Algorithm 1 : TACT at Each Node.

Given: L,$L_{\min}$,$L_{\max}$,Δ_{inc},Δ_{dec}. **Init:** $M_{\text{prev}}=0$,$L=L_{\min}$
repeat
  Transmit probing messages in observation period.
  Measure the number of ACKs, M_{now}.
  if Performance not degraded ($M_{\text{now}} \geq M_{\text{prev}}$) **then**
    Increase the traffic load: $L \leftarrow \min(L+\Delta_{\text{inc}}, L_{\max})$.
  else
    Decrease the traffic load: $L \leftarrow \max(L-\Delta_{\text{dec}}, L_{\min})$.
  end if
  Record history: $M_{\text{prev}} \leftarrow M_{\text{now}}$.
until TACT is disabled.

4.2 Uniform Optimum

When TACT is deployed at node k, it starts to increase node k's traffic load λ_k. However, increasing λ_k cannot improve node k's own delay performance since $\mathbb{P}(D_k > \sigma)$ is not a function of λ_k but a function of $\gamma_k = \sum_{j=1,j\neq k}^{m} \lambda_j$. By transmitting more traffic into the network, node k in fact improves the network traffic loads γ_i $(i \neq k)$ observed at other nodes. At the same time, node k is expecting others to do the same to help itself. Thus, the efficiency of TACT relies on such homogenous behavior in all nodes, which however cannot be guaranteed when nodes have evidently heterogenous traffic rates. Consider an extreme case: there are two nodes (nodes 1 and 2) with routine traffic rates of 1 and 1,000 messages/s, respectively. The optimal loads $\gamma_1^* = \gamma_2^* = 1{,}000$ under a reactive jammer. Initially, $\gamma_1 = \sum_{j=1,j\neq 1}^{2} \lambda_j = 1{,}000$ and $\gamma_2 = \sum_{j=1,j\neq 2}^{2} \lambda_j = 1$. When TACT starts, node 2 is far from the optimum and keeps increasing its traffic load. In contrast, node 1 immediately reaches the optimum and never generates more traffic to help node 2.

Therefore, in order to ensure uniform optimum over all nodes, a solution is to mandate every node have the same minimum traffic load, regardless of their different routine traffic rates. This can be achieved by assigning different minimum camouflage traffic loads $L_{\min}$ (as given in Algorithm 1) to different nodes. Specifically, let node k's minimum camouflage traffic load $L_{\min}(k) = \max_{1\leq i\leq m}\alpha_i - \alpha_k$, where α_i denotes the (fixed) routine traffic load at node i. Thus, the minimum overall traffic load must be transmitted by every node is uniformly equal to $\max_{1\leq i\leq m}\alpha_i$. In the previous example, we can assign $L_{\min} = 999$ and 0 to nodes 1 and 2, respectively. Then, both nodes can have the optimal traffic load when TACT starts. If the optimal load is 1,500 messages/s, both nodes will increase their camouflage traffic loads until reaching the optimum. In the next section, we use experiments to show the effectiveness of TACT.

4.3 TACT in Coordinated and Uncoordinated Modes

So far, we have presented the fundamentals of TACT to minimize the worst-case message delay under jamming attacks. Although we have shown that uncoordinated w communication is not appropriate for time-critical applications, it is still essential to establish the secret key for coordinated communication. As a result, both communication modes are indispensable to fully secure communications for time-critical applications in the smart grid. Specifically, uncoordinated mode is used for key establishment and update. After the secret key is established or updated, the two communicators can use coordinated mode to exchange information based on the secret key. Hence, to substantially improve the performance of a wireless smart grid application with jamming resilience, TACT should be adapted to both coordinated and uncoordinated communications. This means that TACT must be enabled as long as a node is active, regardless of the mode on which it operates. Accordingly, we summarize the complete jamming-resilient communication scheme with TACT in Algorithm 2.

Algorithm 2 : Communication Scheme with TACT.

Initialization: Enable TACT.
repeat
  Mode $\leftarrow$ Uncoordinated mode.
  Obtain key K and period T_K from gateway.
  Mode $\leftarrow$ Coordinated mode.
  Use K for a period of T_K.
until The node leaves the network.

In Algorithm 2, all the keys of a node is obtained from the gateway via uncoordinated communication. If two nodes want to communicate with each other, they also need to request the key for such communication from the gateway. Hence, the gateway can be considered as a key management center in the network. It is worthy of note that in Algorithm 2, every node operates on either uncoordinated or coordinated mode. The gateway, however, is required to operate on both modes simultaneously. Unlike IEDs that are embedded computers on power infrastructures, the gateway is usually a computer server equipped with powerful computing and communication abilities [5]; thus, it is reasonable to assume that the gateway is capable of operating on both modes.

4.4 Discussion on Improving TACT

In Algorithm 2, we can see that when an IED joins the network, it starts to adaptively transmit camouflage traffic until it observes performance degradation at a certain load, then remains approximately at the load. This inevitably leads to a fair amount of redundant traffic and a waste of energy used to transmit such traffic even when there is no attack.

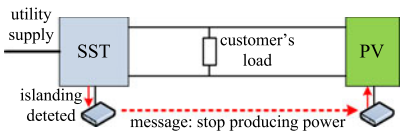


Fig. 7. Anti-islanding procedure in Green Hub.

Although we know that in this case, the delay is still upper bounded by the guaranteed performance given in Theorem 1, it is quite desirable to avoid such traffic in normal system operations. To this end, we can deploy a reactive jamming detector [26] in each IED, TACT is triggered and starts to transmit camouflage traffic only when an attack is detected.

It is worth noting that the distributed nature of TACT requires the minimum node coordination, in which each node sends camouflage traffic on randomly selected channels. Such traffic may collide with legitimate one; thus, node coordination may further improve the efficiency of TACT, which can be achieved by letting the gateway node assign carefully-designed transmission patterns for camouflage traffic at each node.

5 Smart Grid Anti-Islanding: Secure Key Establishment and Communication

We have found that there exists an optimal traffic load to minimize the worst-case message delay, and carefully designed the distributed TACT method to achieve the optimal load. In this section, we aim at implementing a practical TACT based system to optimize the delay performance of an important smart grid application, anti-islanding, under jamming attacks in our experimental micro smart grid, Green Hub.

5.1 Anti-Islanding for a Micro Smart Grid

Our goal is to use real-world experiments to show the effectiveness of TACT to improve the delay performance of a wireless application in the smart grid under jamming attacks. In the following, we first introduce the smart grid system used in the experiments. North Carolina State University has established a micro smart grid, Green Hub, to test key smart grid components, such as solid-state transformer (SST), wireless networking, and dynamic spectrum access [27] for the smart grid. Green Hub includes two solar-array based photovoltaic (PV) systems as distributed energy resources.

An important protection procedure for distributed energy resources is anti-islanding. In power engineering, islanding [28] refers to the condition in which distributed energy resources continue power supply even though the electric utility is disconnected. Unintentional islanding can cause many problems, such as damaging customers' loads and harming distributed energy resources [28]. Thus, anti-islanding procedures must be deployed in power systems to prevent any unintentional islanding.

Fig. 7 shows an anti-island procedure in Green Hub: when the utility supply is disconnected, the SST detects the islanding and sends an anti-islanding message to the PV system to make the system stop generating power. The delay threshold of such a message is 150-300 ms [3].

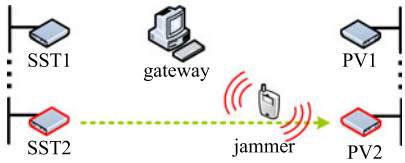


Fig. 8. Attack scenario in the anti-islanding network.

5.2 System Setups

Network setup. There have been several wireless testing networks for anti-islanding in the power engineering community [3], [28]. In this work, we use universal software radio peripheral (USRP) devices with GNU Radio to set up a frequency-hopping based wireless network to provide jamming resilience for the anti-islanding application. Green Hub has two PV-SST pairs for anti-islanding protection. Each device is connected to an IED for communication. Thus, the network consists of four IEDs and a gateway for centralized management. Each IED's routine traffic is one message of status update to the gateway every second. Both IEDs and the gateways use USRPs to communicate with each other.

Spread spectrum systems. The network uses eight frequency hopping channels at the 2.4 GHz band, each of which uses BPSK modulation and has a bandwidth of 125 KHz, resulting in a total network bandwidth of 1 MHz. The length of an anti-islanding message is 400 bytes, thereby leading to a transmission time of $(400^{*}8)/125 = 25.6$ ms. The delay threshold is set to be 150 ms. The application layer at each IED transmits one message four times. Thus, the secret key shared by each transmit-receive pair is a frequency-hopping pattern with four hops. For TACT, the lengths of probing and camouflage messages are set to be 400 and 1,000 bytes, respectively. Note that we choose long camouflage messages to increase the chance that a reactive jammer senses and jams such messages.

Jamming attacks. We also set up a USRP-based jammer with operational bandwidth of 125 KHz. When it is non-reactive, it keeps broadcasting jamming pulses, each of which is sent on a randomly selected channel. When it is reactive, it uses an energy detector to scan all eight hopping channels one by one, and jams any on-going transmission as long as it senses energy activity. The jamming pulse duration is set to be 1 ms.

Attack scenario. The attack scenario is illustrated in Fig. 8: all IEDs (SST1, PV1, SST2, and PV2) inform the gateway of their status every second. If SST1 or SST2 detects an islanding, it will send to its counterpart an anti-islanding message. The jammer targets SST2 and attempts to disrupt SST2's messages to PV2.

5.3 Experimental Results

When the network is set up, all IEDs first communicate uncoordinatedly with the gateway to obtain their secret keys of channel assignments, then use the keys to communicate in a coordinated manner. As a result, we first consider the uncoordinated case; i.e., we first evaluate how TACT can improve the delay performance of key establishment, and then move on to the coordinated case.

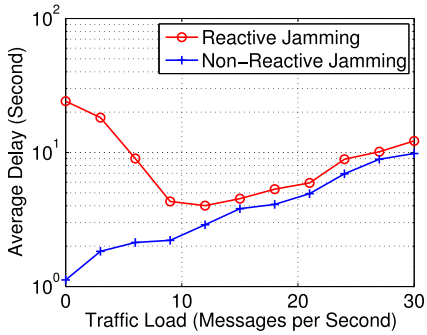


Fig. 9. Uncoordinated: Average key establishment delay versus per-node network traffic load.

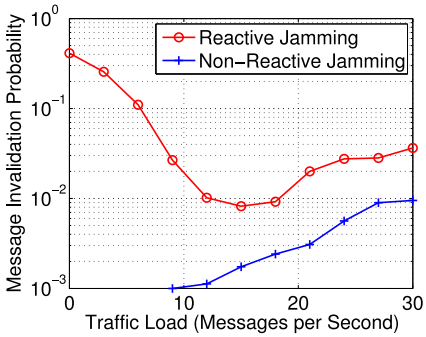


Fig. 10. Coordinated: Message invalidation probability versus traffic load.

5.3.1 Key Establishment

We consider key establishment based on uncoordinated communication: every node keeps sending key requests to the gateway on uniformly selected frequency channels. At the same time, the gateway uniformly chooses a frequency channel to receive. A message is delivered only when a node and the gateway reside on the same channel. We define the delay of the key establishment for a node is the time duration from the instant that the node sends the first key request to the instant that the node receives the reply from the gateway.

Fig. 9 illustrates the mean delay of key establishment as a function of the network traffic load under both non-reactive jamming and reactive jamming. We can observe from Fig. 9 that reactive jamming always induces larger key establishment delay than non-reactive jamming for uncoordinate communication, which indicates that we should always consider the reactive jamming as the worst-case scenario for uncoordinate communication. Note that Fig. 9 exhibits a U-shaped curve for the delay performance under reactive jamming, showing that under reactive jamming, there always exists a traffic load to minimize the average key establishment delay. As a result, TACT that is primarily designed to counter-attack reactive jamming by achieving the optimal traffic load, should be useful to substantially decrease the key establishment delay in the wireless anti-islanding scenario.

Next, we enable TACT at every node and evaluate the effectiveness of TACT on uncoordinated communication under reactive jamming. During experiments, we set the following TACT parameters: $L_{\min} = 0$, $L_{\max} = 30$, $\Delta_{\text{inc}} = 2$, $\Delta_{\text{dec}} = 2$, and ten probing messages are sent every second. Table 1 illustrates the average key establishment delay under three scenarios: i) frequency hopping under reactive jamming (TACT is off), ii) frequency hopping with camouflage traffic (TACT is on), iii) baseline performance (no jamming, no TACT). It is observed from Table 1 that uncoordinated communication based key establishment incurs fairly large delay even for the baseline (no-jamming case) performance that have the average delay of 814 ms. This is due to the opportunistic nature of uncoordinated communication. Under reactive jamming, we can see that the key establishment delay increases to 24.2 s. However, when TACT is enabled, the delay decreases dramatically to 5.61 s, as shown in Table 1. Therefore, TACT is very effective to improve the delay performance for key establishment in the smart grid.

TABLE 1
Average Delay in Uncoordinated Communication

Setups:	TACT off	TACT on	Baseline
Delay :	24.2 s	5.61 s	0.814 s

5.3.2 Jamming-Resilient Communication

Next, we consider the coordinated mode after the key is established. We evaluate the impact of both reactive and non-reactive jammers on the anti-island application. We generate camouflage messages at rates of 0-30 messages/s. Fig. 10 shows that the message invalidation probability as a function of the camouflage traffic rate of each IED. We can see from Fig. 10 that reactive jamming always leads to worse performance than non-reactive jamming, indicating that reactive jamming should be considered as the worst-case scenario. Thus, in the following, we will only consider reactive jamming. Fig. 10 also shows that the message invalidation probability induced by reactive jamming is a U-shaped function of the traffic load. We can see that the message invalidation probability decreases from 41.2 to 0.82 percent as the camouflage traffic load goes from 0 to 15 messages/s.

Then, we consider the delay performance with different delay thresholds of 150, 190, and 230 ms under reactive jamming. If the delay threshold becomes larger, we can transmit the same message more times to ensure more reliability. Thus, the transmissions have five, six, and seven hops (transmission attempts) for messages with delay thresholds of 150, 190, and 230 ms, respectively. Fig. 11

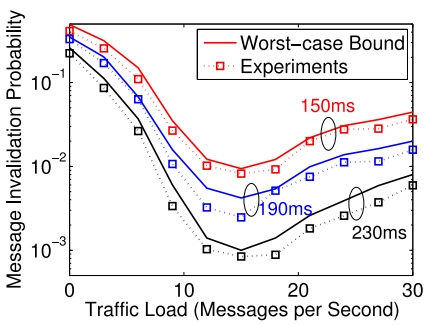


Fig. 11. Coordinated: Message invalidation probability with different delay thresholds.

TABLE 2
Message Invalidation in Coordinated Communication

Setups:	TACT off	TACT on	Baseline
Delay :	41.2%	0.9076%	0.0532%

TABLE 3
Message Invalidation versus Number of Hopping Channels

Number of Channels (N_f):	6	8	10	12
TACT off:	92.3%	68.1%	41.2%	10.1%
TACT on:	15.1%	6.01%	0.831%	0.212%

shows that the message invalidation probabilities for different delay thresholds. In addition, we also compare the worst-case bounds in Theorem 2 with the experimental results, as shown in Fig. 11. Although we can see that that there exists a small and non-uniform gap between the worst-case bound and the experimental measurement for each delay threshold, the performance trends shown by the experimental results do match the theoretical predication and the U-shape phenomena, which indicates that the worst-case bound in Theorem 2 is tight to predict realistic jamming impacts.

Next, we evaluate the effectiveness of TACT against reactive jamming in coordinated communication. We use the same setups in Table 1. Table 2 illustrates message invalidation probabilities in three scenarios: i) frequency hopping under reactive jamming (TACT is off), ii) frequency hopping with camouflage traffic (TACT is on), iii) baseline performance (no jamming, no TACT). It is observed from Table 2 that TACT decreases the message invalidation probability from 41.2 to 0.9076 percent. Although TACT does not achieve the minimum probability of 0.82 percent shown in Fig. 10, it still improves the delay performance in order of magnitude under reactive jamming. Note that the baseline performance in Table 2 shows a positive message invalidation probability. This is because error correction is not used in our experiments in order to reduce the GNU Radio processing delay.

Table 3 shows the message invalidation probability as a function of the number of frequency-hopping channels N_f under reactive jamming. It is known that increasing N_f can reduce the message delay for spread spectrum communication, as more spectrum resources are used. Table 3 illustrates that when N_f goes from 6 to 12, the message invalidation probability in the frequency-hopping-only (no TACT) scenario decreases from 92.3 to 10.1 percent; while TACT can further reduce the probability from 10.1 to 0.21 percent. As a result, TACT is a promising mechanism that offers a new dimension to improve the delay performance for smart grid communication.

5.4 Discussions

In our experiments, both IEDs and jammer have low operational bandwidth of 125 KHz, which is due to the limit processing capability of the USRP-to-PC architecture. Thus, our goal is not to design a commercial anti-islanding system, but to demonstrate a proof-of-concept application of TACT in the smart grid.

We observed that TACT achieved nearly-optimal performance. It is challenging to design an adaptive method that always works at the optimal load. However, the concept of transmitting camouflage traffic can lead to more TACT-like methods to further improve the delay performance for wireless smart grid applications.

Currently, both legitimate and camouflage traffic is blind to all legitimate receivers and attackers, which is the simplest setup for the attackers to have no ability to identity legitimate traffic from camouflage traffic, which on the other hand causes collisions between legitimate and camouflage traffic transmissions. We will explore smart ways to avoid such collisions in the future work.

We also emphasize that our methodology in this paper is to optimize the worst-case performance to offer performance guarantee for smart grid applications. Therefore, our worst-case optimization does not necessarily means a uniformly optimal solution to all cases. This indicates that when a jammer constantly changes its jamming behavior, our countermeasure may not keep providing optimal solutions against each behavior. However, despite the jammer's varying strategies, its induced performance is always bounded by the worst case. Therefore, as long as we design our countermeasures based on the worst case, we can always provide performance guarantee under any attack behavior, which is our goal and also essential for smart grid applications.

6 Conclusion

In this paper, we provided a comprehensive study on minimizing the message delay for smart grid applications under jamming attacks. By defining a generic jamming process, we showed that the worst-case message delay is a U-shaped function of network traffic load. We designed a distributed method, TACT, to generate camouflage traffic to balance the network load at the optimal point. We showed that TACT is a promising method to significantly improve the delay performance in the smart grid under jamming attacks.

Acknowledgments

The work was supported by Army Research Office (ARO) staff research grant W911NF-07-R-0001-05 and National science Foundation (NSF) Career Award CNS-0546289. Part of the work was presented in IEEE INFOCOM '12.

References

[1] *Guidelines for Smart Grid Cyber Security*, NIST IR-7628, NIST Smart Grid Cyber Security Working Group, vol. 1-3, Aug. 2010.
[2] F. Cleveland, "Uses of wireless communications to enhance power system reliability," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, p. 1.
[3] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, 2009, pp. 1–8.
[4] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," in Tech. Rep., Richland, WA, USA, Pacific Northwest Nat. Laboratory, Jan. 2010, PNNL-19084.
[5] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, pp. 3604–3629, 2011.
[6] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems - current status and future trends," in *Proc. Power Systems Conf. Expo.*, 2009, pp. 1–9.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.
[8] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE Symp. Security Privacy*, May 2008, pp. 64–78.
[9] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. IEEE IEEE Conf. Comput. Commun.*, Mar. 2010, pp. 1–9.
[10] M. Strasser, C. Popper, and S. Capkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proc. ACM Int. Symp. Mobile Ad Hoc Network. Comput.*, 2009, pp. 207–218.
[11] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. 18th USENIX Security Symp.*, Aug. 2009, pp. 231–248.
[12] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *Proc. IEEE IEEE Conf. Comput. Commun.*, Apr. 2008, pp. 1265–1273.
[13] X. Lu, W. Wang, and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems," *Int. J. Distributed Sensor Netw.*, vol. 2012, p. 13, Apr. 2012.
[14] *IEC 61850: Communication Networks and Systems in Substations*, IEC Standard, 2003.
[15] H. Li, L. Lai, and R. C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Proc. 45th Annu. Conf. Inf. Sci. Syst.*, Mar. 2011, pp. 1–6.
[16] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. IEEE Conf. Comput. Commun.*, 2008, pp. 1211–1219.
[17] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in *Proc. IEEE Power Eng. Soc. Summer Meet.*, June 2007, pp. 1–8.
[18] J. Gardner, "Spread spectrum communications for SCADA systems," *Pipeline and Gas J.*, vol. 238, Feb. 2011, pp. 1–6.
[19] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1482–1489, Jul. 2007.
[20] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[21] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 703–715, Jun. 2010.
[22] S. G. Glisic, A. Mammela, V.-P. Kaasila, and M. D. Pajkovic, "Rejection of frequency sweeping signal in DS spread spectrum systems using complex adaptive filters," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 136–145, Jan. 1995.
[23] B. Zhao, C. Chi, W. Gao, S. Zhu, and G. Cao, "A chain reaction DoS attack on 3G networks: Analysis and defenses," in *Proc. IEEE Conf. Comput. Commun.*, 2009, pp. 2455–2463.
[24] M. Brinkmeier, G. Schafer, and T. Strufe, "Optimally DoS resistant P2P topologies for live multimedia streaming," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 6, pp. 831–844, Jun. 2009.
[25] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Security*, 2011, pp. 47–52.
[26] M. Strasser, B. Danev, and S. Capkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sensor Netw.*, vol. 7, no. 2, pp. 16:1–16:29, 2010.
[27] L. Sun and W. Wang, "On distribution and limits of information dissemination latency and speed in mobile cognitive radio networks," in *Proc. IEEE Conf. Comput. Commun.*, 2011, pp. 246–250.
[28] W. El-Khattam, T. S. Sidhu, and R. Seethapathy, "Evaluation of two anti-islanding schemes for a radial distribution system equipped with self-excited induction generator wind turbines," *IEEE Trans. Energy Convers.*, vol. 25, no. 1, pp. 107–117, Mar. 2010.

Zhuo Lu received the PhD degree from the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC, in 2013. He is currently a research scientist at Intelligent Automation Inc, Rockville MD. His research interests include network and mobile security, cyber-physical system security. He is a student member of the IEEE.

Wenye Wang received the MSEE and PhD degrees from the Georgia Institute of Technology, in 1999 and 2002, respectively. She is a professor with the Department of Electrical and Computer Engineering, North Carolina State University. Her research interests include cyber-physical systems, mobile and cloud computing, and cyber security. She received the National science Foundation (NSF) CAREER Award 2006 and the corecipient of the 2006 IEEE GLOBECOM Best Student Paper Award and the 2004 IEEE ICCCN Best Student Paper Award. She has been a member of the Association for Computing Machinery (ACM) since 1998, and a member of the Eta Kappa Nu and Gamma Beta Phi honorary societies since 2001. She is a senior member of the IEEE.

Cliff Wang graduated with the PhD degree in computer engineering from North Carolina State University in 1996. He is currently the division chief for the Army Research Office's computer sciences program and manages a large portfolio of advanced information assurance research projects. He is also appointed as an adjunct faculty member of computer science in the College of Engineering at North Carolina State University. He has been carrying out research in the area of computer vision, medical imaging, high-speed networks, and most recently information security. He is a senior member of the IEEE.