Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications

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

Abstract—Recently, wireless networking for emerging cyber-physical systems, in particular the smart grid, has been drawing increasing attention in that it has broad applications for time-critical message delivery among electronic devices on physical infrastructures. However, the shared nature of wireless channels unavoidably exposes the messages in transit to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipments. An important, yet open research question is how to model and detect jamming attacks in such wireless networks, where communication traffic is more time-critical than that in conventional data-service networks, such as cellular and WiFi networks. In this paper, we aim at modeling and detecting jamming attacks against time-critical wireless networks with applications to the smart grid. In contrast to communication networks where packets-oriented metrics, such as packet loss and throughput are used to measure the network performance, we introduce a new metric, message invalidation ratio, to quantify the performance of time-critical applications. Our modeling approach is inspired by the similarity between the behavior of a jammer who attempts to disrupt the delivery of a time-critical message and the behavior of a gambler who intends to win a gambling game. Therefore, by gambling-based modeling and real-time experiments, we find that there exists a phase transition phenomenon for successful time-critical message delivery under a variety of jamming attacks. That is, as the probability that a packet is jammed increases from 0 to 1, the message invalidation ratio first increases slightly, then increases dramatically to 1. Based on analytical and experimental results, we design the Jamming Attack Detection based on Estimation (JADE) scheme to achieve robust jamming detection, and implement JADE in a wireless network for power substations in the smart grid.

Index Terms—Performance modeling, wireless network, time-critical messaging, jamming attack detection, smart grid applications.

1 Introduction

The advancement of today's wireless technologies (e.g., 3G/4G and WiFi) has already brought significant change and benefit to people's life, such as ubiquitous wireless Internet access, mobile messaging and gaming. On the other hand, it also enables a new line of applications for emerging cyber-physical systems, in particular for the smart grid [1], where wireless networks have been proposed for efficient message delivery in electric power infrastructures to facilitate a variety of intelligent mechanisms, such as dynamic energy management, relay protection and demand response [2]–[5].

Differing evidently from conventional communication networks, where throughput is one of the most important performance metrics to indicate how much data can be delivered during a time period, wireless networking for cyber-physical systems aims at offering reliable and timely message delivery between physical devices. In such systems, a large amount of communication traffic is time-critical (e.g., messages in power substations have latency constraints ranging from 3 ms to 500 ms [6]). The delivery of such messages is expected to be followed by a sequence of actions on physical infrastructures. Overdue message delivery may lead to instability of system operations, and even cascading failures. For instance, in the smart grid, a binary result of fault detection on a power feeder can trigger subsequent operations of circuit breakers [7]. If the message containing such a result is missed, or does not arrive on time, the actions on circuit breakers will be delayed, which can cause fault propagation along physical infrastructures and potential damages to power equipments.

As a result, it is of crucial importance to guarantee network availability in terms of message delay performance instead of data throughput performance in such time-critical applications, which is also considered as one of the most challenging issues in cyber-physical systems. However, on the other hand, the shared nature of wireless channels inevitably surrenders information delivery over wireless networks to jamming attacks [8]–[10], which may severely degrade the performance and reliability of these applications by broadcasting radio interference over the shared wireless channel.

Although there have been significant advances towards jamming characterization [8]–[10] and countermeasures [11]–[18] for conventional networks, little attention has been focused on jamming against message delivery in time-critical wireless applications. In particular, conventional performance metrics cannot be readily adapted to measure the jamming impact against time-critical messages. In conventional wireless networks, the impact of jamming attacks is evaluated at the packet

- *Zhuo Lu and Wenye Wang are with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. E-mails: {zlu3, wwang}@ncsu.edu. Cliff Wang is with Army Research Office, Research Triangle Park, NC. Email: cliff.wang@us.army.mil.*

The work was supported by the Army Research Office (ARO) staff research grant W911NF-07-R-0001-05 and the Defense Threat Reduction Agency (DTRA) research grant HDTRA1-08-1-0024. An earlier version of the work was published in IEEE INFOCOM 2011.

level such as packet send/delivery ratio [8] and the number of jammed packets [11] (because existing data services are based on packet-switched networks), or at the network level such as saturated network throughput [10]. However, packet-level and network-level metrics do not directly reflect the latency constraints of message exchange in time-critical applications. For example, 100% packet delivery ratio does not necessarily mean that all messages can be delivered on time to ensure reliable operations in a cyber-physical system.

In addition, lack of the knowledge on how jamming attacks affect such time-critical messaging leads to a gray area in jamming detector design; that is, it is not feasible to design an effective detector to accurately identify attacks with significant impacts on time-critical message delivery. Therefore, towards emerging wireless applications in cyber-physical systems, an open and timely research question is *how to model, analyze, and detect jamming attacks against time-critical message delivery?*

In this paper, we *study the problem of modeling and detecting jamming attacks in time-critical wireless applications*. Specifically, we consider two general classes of jamming attacks widely adopted in the literature: reactive jamming and non-reactive jamming [8]. The former refers to those attacks [8], [13], [17], [18] that stay quiet when the wireless channel is idle, but start transmitting radio signals to undermine ongoing communication as soon as they sense activity on the channel. The latter, however, is not aware of any behavior of legitimate nodes and transmits radio jamming signals with its own strategy.

There are two key observations that drive our modeling of reactive and non-reactive jammers. (i) In a time-critical application, a message becomes invalid as long as the message delay D is greater than its delay threshold σ. Thus, we define a metric, *message invalidation ratio*, to quantify the impact of jamming attacks against the time-critical application. (ii) When a retransmission mechanism is adopted, to successfully disrupt the delivery of a time-critical message, the jammer needs to jam each transmission attempt of this message until the delay D is greater than σ. As a result, such behavior of the jammer is exactly the same as the behavior of *a gambler* who intends to win each play in a game to collect enough fortune to achieve his gambling goal of σ dollars.

Motivated by the two observations, we develop a gambling-based model to derive the message invalidation ratio of the time-critical application under jamming attacks. We validate our analysis and further evaluate the impact of jamming attacks on an experimental power substation network by examining a set of use cases specified by the National Institute of Standards and Technology (NIST). Based on theoretical and experimental results, we design the jamming attack detection based on estimation (JADE) system to achieve efficient and reliable jamming detection for the experimental substation network. Our contributions in this paper are three-fold.

1) We introduce a new metric, message invalidation ratio, to quantify the performance of time-critical applications. Through theoretical and experimental studies, the message invalidation ratios are measured for a number of time-critical smart grid applications under a variety of jamming attacks.
2) For reactive jamming, we find that there exists a phase transition phenomenon of message delivery performance: when jamming probability p (the probability that a physical transmission is jammed) increases, the message invalidation ratio first increases slightly (and is negligible in practice), then increases dramatically to 1. For non-reactive jamming, there exists a similar phenomenon: when the average jamming interval (the time interval between two non-reactive jamming pulses) increases, the message invalidation ratio first has the value of 1, then decreases dramatically to 0.
3) Motivated by the phase transition phenomenon showing that a jammer only leads to negligible performance degradation when its jamming probability p is smaller than the transition point p^*, the proposed JADE method first estimates the jamming probability $\hat{p}$ and then compares $\hat{p}$ with p^* to detect jammers that can cause non-negligible impacts. JADE requires no online profiling/training step that is usually necessary in existing methods [8], [11], [19]. We show via experiments that JADE achieves comparable detection performance with the statistically optimal likelihood ratio (LLR) test. We further show that JADE is more robust than the LLR test in the presence of a time-varying jammer.

The rest of this paper is organized as follows. In Section 2, we describe preliminaries and the definition of message invalidation ratio. In Sections 3 and 4, we model both reactive and non-reactive jamming attacks, derive the message invalidation ratios, and validate our analysis by performing experiments in a power substation network. In Section 5, we design and implement the JADE system for the substation network. Finally, we conclude in Section 6.

2 Models and Problem Statement

In this section, we introduce models for time-critical applications and jamming attacks, then define a metric, message invalidation ratio for later analysis.

2.1 Network and Traffic Models

As of today, the smart grid [1] has become one of the most important cyber-physical systems with a wide range of time-critical applications, we therefore focus on developing models for time-critical wireless networks with applications to the smart grid. Specifically, we consider a single-hop wireless network for a local-area system (e.g., power substation in the smart grid [2]–[4]). The primary goal of such a network is to achieve efficient and reliable communication between local physical devices. There are two types of communication traffic in the network: time-critical and non-time-critical messages.

TABLE 1
Time-critical message types in IEC 61850.

Message Type	Delay Constraint	Purpose
Type 1A/P1	3 ms	GOOSE trip protection
Type 1A/P2	10 ms	GOOSE trip protection
Type 1B/P1	100 ms	automation system interaction
Type 1B/P2	20 ms	automation system interaction

- Time-critical traffic is used for monitoring, control and protection of electronic devices on physical infrastructures. Such traffic has even more stringent timing requirements than conventional delay-sensitive traffic (e.g., video streaming on the Internet). For example, IEC 61850 [6] is a recent communication standard for power substation automation. IEC 61850 defines a variety of message types with specific timing constraints, in which the most time-critical message type, Generic Object Oriented Substation Event (GOOSE), shown in Table 1, has two end-to-end delay constraints[1]: 3ms and 10ms.
- Non-time-critical traffic is used for general-purpose exchange of system data, such as logging or file transferring [6]. Non-time-critical traffic usually does not have delay requirements. For example, IEC 61850 does not explicitly define the delay specification for substation non-critical file transferring, but suggests a timing requirement equal to or greater than 1000 ms.

We will focus on time-critical messages in this paper. An example of transmitting such messages in smart grid applications is *raw data sampling* [6]: in a power substation, an electronic device, called merging unit, keeps sampling the power signal on feeders, sends the sampled data to protection and control devices, which monitor the stream of sampled data and are programmed with incident protection procedures. The messages containing raw data samples are required to be delivered in 3 ms to ensure timely incident management. To transmit such time-critical messages, there are several fundamental requirements: (i) time-critical messages must be processed with the highest priority; (ii) simple protocol processing and low communication overhead are required; (iii) packet queuing or buffering should be avoided.

As a result, IEC 61850 maps the most time-critical GOOSE messages from the application layer directly to the MAC/link layer to reduce processing time and avoid tedious protocol headers. In this regard, since there is no transport layer to guarantee reliability, IEC 61850 defines that the application layer simply retransmits the same GOOSE message multiple times to ensure reliability.

Accordingly, we assume that a time-critical message with end-to-end delay constraint σ is passed from the application layer directly to the MAC layer. There is no flow and congestion control for the transmission. The application layer has a simple processing function that retransmits the same message after the previous transmission fails. The application layer will stop retransmission if the transmission is successful, or the message delay exceeds σ, since the message becomes obsolete or invalid. In addition, we assume that the time-critical network is always unsaturated (i.e., the network bandwidth is greater than the overall traffic load). Otherwise, the timing requirement of a time-critical message may not be guaranteed since the message has to be queued before transmission.

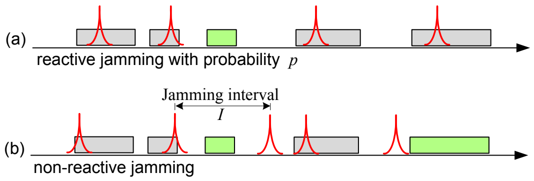

Fig. 1. Reactive jamming versus non-reactive jamming.

2.2 Jamming Models

The broadcast nature of wireless channels inevitably exposes time-critical wireless networks to jamming attacks that may severely degrade the network performance [8]–[10]. The jamming problem in conventional wireless network has been extensively studied regarding jamming strategies [8]–[10], jamming detection [11], [12], [19], and anti-jamming technologies [13]–[18]. According to [8], we summarize jamming attacks into two major types.

1) Reactive jammers, as shown in Fig. 1 (a). Reactive jammers [8], [13], [17], [18] are aware of the target communication systems. They stay quiet when the channel is idle, but start transmitting radio signals (or even meaningful signals [17]) to undermine ongoing communication as soon as they sense activity on the wireless channel.
2) Non-reactive jammers, as shown in Fig. 1 (b). Non-reactive jammers are not aware of any behavior of legitimate nodes and transmit the radio interference over the wireless channel following their own jamming strategies.

Reactive jammers disrupt legitimate transmissions in a more active and versatile manner than non-reactive jammers. When a reactive jammer senses an ongoing packet transmission, it can jam the packet with a controllable probability p. Thus, we model the strategy of a reactive jammer as follows.

Definition 1: The strategy of a reactive jammer is represented by $\mathcal{J}_r(p)$, where $p \in [0,1]$ is the jamming probability, defined as the probability that a physical transmission can be successfully jammed.

Non-reactive jammers have no information of wireless channel activity, and transmit jamming pulse signals following a pre-defined pattern. Typical non-reactive jammers include periodical and random jammers in the literature [8], [10]. For a non-reactive jammer, the

[1] The end-to-end delay is defined as the time interval from the instant that the transmitter's application layer generates a message to the instant that the receiver's application layer successfully receives it.

jamming interval I is an essential parameter [10] to characterize its behavior. If a jammer intends to disrupt more physical transmissions, it can use a very small jamming interval I. To the extreme, the non-reactive jammer with I=0 becomes a continuous jammer. Thus, we use the jamming interval I to model a non-reactive jammer and formally define its strategy as follows.

Definition 2: The strategy of a non-reactive jammer is represented by $\mathcal{J}_{nr}(I)$, where $I \geq 0$ is the jamming interval, defined as the time interval between two adjacent jamming pulses transmitted by the jammer.

The non-reactive jamming model in Definition 2 can represent several widely-used jamming models in the literature. For example, when the jamming interval I is a constant, the model becomes the periodic jamming model [8], [10]; when I is exponentially distributed, the model becomes the memoryless jamming model [10].

Although existing work (e.g. [8], [10]) has shown that a non-reactive jammer is less efficient than a reactive jammer, it is still an easy and simple way to disrupt legitimate traffic in wireless networks. Thus, we consider both reactive and non-reactive jammers in our models.

2.3 Discussion on Assumptions and Models

There have been some works regarding the impact of denial-of-service attacks on delay-sensitive transmission, which are based on congestion control at the transport layer [20], [21]. Our time-critical transmission model at the application-layer features a simple mechanism that keeps retransmitting the same message without any congestion or flow control (which is also standardized in IEC 61850). Such a mechanism is to ensure that a time-critical message can arrive at the destination on time. However, the mechanism may fail to deliver a time-critical message due to high network congestion when all nodes keep transmitting time-critical messages all the time. As a consequence, the assumption of unsaturated traffic load is a precondition for our transmission mechanism to work for time-critical messages. We note that network traffic in power systems has been shown to exhibit unsaturated nature. For example, in a power substation network, the overall load usually ranges from 1.952Mbps to 7.592Mbps [6], which can be supported efficiently by IEEE 802.11g/n [4]. In a wireless monitoring network [22], transformers only need to transmit a message every second to report and update running states. Hence, the assumption of unsaturated network traffic is valid for practical time-critical applications in the smart grid. This is also a major difference between cyber-physical systems and conventional communication networks, in which saturated traffic is usually assumed in performance analysis.

The jamming models used in this paper include reactive jamming and non-reactive jamming, which constitute the majority of jamming attacks widely adopted in existing data communication networks, such as adhoc networks [19], wireless sensor networks [8], wireless broadcast networks [15], [17], and WiFi networks [10]. Our results based on both types of attacks can serve as fundamentals to analysis of more intelligent jamming strategies against time-critical traffic.

It is worth noting that our attack models feature jamming probability p and interval I for reactive and non-reactive jammers, respectively. In practice, an attacker may choose $p{=}1$ (or $I{=}0$) to maximize its impact, such as a reactive jammer always sending radio interference when it senses channel activity [8]. Our modeling, in which p and I vary in wide ranges ($p \in [0, 1]$ and $I \geq 0$), is general to include such extreme cases. In addition, it can also accommodate or indicate the cost of an attacker. If a non-reactive jammer is battery-supplied, it may choose a large I to conserve energy, which implies that the larger I, the lower the jammer's cost.

2.4 Problem Statement

We have modeled the time-critical transmission mechanism and jamming strategies. We then define a performance metric to model the impact of jamming attacks on time-critical traffic.

In conventional networks, legitimate nodes usually request data services from service providers or exchange data among their neighbors. Hence, the throughput is an important performance metric in such networks. However, as stated earlier, the primary goal of time-critical wireless networks is to achieve efficient message delivery for reliable monitoring and control of a variety of physical infrastructures, instead of providing high throughput for clients. Hence, the delay performance of time-critical applications is much more important than the conventional throughput performance. A time-critical message becomes invalid as long as its message delay D is greater than the delay constraint σ. In order to directly reflect how a time-critical message can be delivered on time, we define a performance metric, message invalidation ratio, to evaluate the performance of time-critical applications.

Definition 3: For a time-critical message with delay constraint σ, the message invalidation ratio $r = \mathbf{1}\mathbb{P}\{D > \sigma\}$, where D is the end-to-end message delay.

As we can see, the message invalidation ratio is in fact the tail distribution of the message delay. Thus, for a time-critical application under jamming attacks, the derivation of delay distribution is equivalent to the derivation of message invalidation ratio. With the definition of message invalidation ratio, we formally state our problem of quantifying the impact of jamming attacks against time-critical traffic as follows.

Problem Statement: In a time-critical wireless network, given a time-critical message with end-to-end delay constraint σ, find the message invalidation ratios of the time-critical message under jamming strategies $\mathcal{J}_r(p)$ and $\mathcal{J}_{nr}(I)$, respectively.

In following sections, we first use analytical modeling to derive the message invalidation ratio and perform real-time experiments in a power substation network to validate our analysis. Then, we present the design and experimental results of our jamming detection method.

3 Main Analytical Results

The key question in our study is to answer what is the time-critical message invalidation ratio under both reactive and non-reactive jamming attacks. Accordingly, we separate the question into two parts and investigate the message invalidation ratios with jamming strategies $\mathcal{J}_r(p)$ and $\mathcal{J}_{nr}(I)$, respectively.

3.1 Impact of Reactive Jamming with $\mathcal{J}_r(p)$

We first formulate the reactive jamming problem into a gambling problem, and then derive the message invalidation ratio of time-critical applications under jamming attacks.

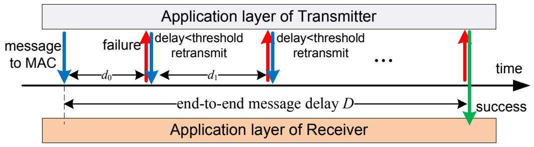
Application layer of Transmitter
message to MAC
failure
delay<threshold retransmit
delay<threshold retransmit
...
time
d_0
d_1
end-to-end message delay D
success
Application layer of Receiver

Fig. 2. Transmission process of time-critical messages at application layer.

Consider a transmitter that needs to send a time-critical message with delay constraint σ, and a jammer with strategy $\mathcal{J}_r(p)$ that attempts to disrupt message delivery in the network. The process for the transmitter to send the time-critical message is illustrated in Fig. 2: The time-critical message is initially generated at the application layer and is passed directly to the MAC layer to transmit. However, the transmission by the MAC layer may not succeed in the presence of the jammer. If transmission failure (e.g., ACK timeout) is reported by the MAC layer, the application layer will retransmit the same message as long as the cumulative message delay does not exceed the threshold σ. Therefore, the end-to-end message delay can be represented as

$$D = \sum_{i=0}^{N} d_i, \tag{1}$$

where N is the number of retransmissions and d_i is the MAC-layer delay during the i-th retransmission.

Note that the number of retransmissions N and the MAC-layer delay d_i are both random variables due to the random backoff mechanism used in wireless MAC protocol (e.g., WiFi and Zigbee). If a message has no delay constraint, the application layer will keep transmitting the same message until it succeeds. In this case, the number of retransmissions N follows the geometric distribution. Then, the end-to-end delay D in (1) becomes a geometric sum and it is not difficult to use asymptotic analysis to derive the distribution of D, similarly to existing work on computing the delay distribution for CSMA/CA networks (e.g., [10], [23]).

However, in our case with a specific delay threshold σ, jamming attacks can only lead to a finite number of retransmissions at the application layer. The number of retransmissions N is in fact a bounded random variable dynamically coupled with the sum of MAC-layer delays $\{d_i\}$, since every time the application layer compares the accumulated message delay with the constraint σ to check whether it should resend a transmission-failed message or drop it. Consequently, it is non-trivial to accurately model and derive the message invalidation ratio of the time-critical application under jamming attacks.

Then, we take a closer look at the process of transmitting a time-critical messages. There are two further observations.

1) Such a process has only two outcomes: the jammer either wins or loses. That is, either the jammer keeps successfully jamming every transmission until the delay is larger than the threshold, or the transmitter successfully delivers the message within the timing constraint.
2) In order to win, the jammer must cumulatively collect the reward, i.e., message delay. Every time he jams a physical transmission, a certain amount of delay contributes to the overall message delay.

Is there any process satisfying the two properties? Yes, it is *gambling*. In other words, if we consider the jammer as a gambler and the delay as money, we can exactly map our problem into a gambling game: a gambler attempts to win a game by consistently winning money to reach his goal. The probabilistic modeling of a gambling game, such as the *gambler's ruin* problem [24], has been well investigated by mathematicians. It has been shown that martingale theory [24], a branch of modern probabilistic measure theory, is an effective tool to solve the *gambler's ruin* problem. Therefore, we are motivated to map our problem into a gambling game and solve it by using martingale theory.

We first construct a game for a gambler shown in Fig 3. The gambler starts with $X_0 = d_0$ dollars. In the n-th play, when event A happens (with probability p_a), the gambler wins d_n dollars; when event A^c happens (with probability 1-p_a), he loses $\frac{p_a}{1-p_a}\mathbb{E}(d_n)$ dollars.[2] His gambling goal is σ dollars. The gambler quits when he either reaches his gambling goal or loses once (i.e., A^c happens).

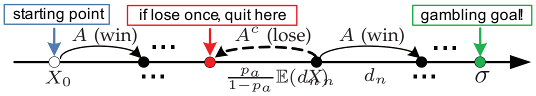

Fig. 3. Setups of our gambling game: the gambler either wins d_n dollars (event A) or loses $\frac{p_a}{1-p_a}\mathbb{E}(d_n)$ dollars (event A^c) in the n-th play. The gambler quits when he either reaches his gambling goal or loses once.

[2] The value of $\frac{p_a}{1-p_a}\mathbb{E}(d_n)$ does not affect the interpretation of our gambling game mapping. It will be shown later that this value is essential to our martingale construction.

Let $\{X_n\}$ be the gambler's money in the n-th play. Specifically, we can write X_n as follows.

$$X_0 = d_0,\ X_n = X_{n-1} + \xi_n, \quad (n \in \mathbb{N}), \tag{2}$$

where $\mathbb{N}$ is the set of positive integers, ξ_n is the reward for the gambler in the n-th play. Since the gambler can either win or lose in the n-th play, the reward ξ_n can be written as

$$\xi_n = d_n \mathbf{1}_A - \frac{p_a}{1-p_a}\mathbb{E}(d_n)\mathbf{1}_{A^c}, \tag{3}$$

where $\mathbf{1}_A$ is the indicator function, has the value 1 if event A happens, and the value 0 otherwise.

Then, we map our scenario of the time-critical transmission into the gambling game: the jammer is the gambler and the delay is money. Each transmission can be regarded as a play. Let event $A = \{\text{the gambler wins money in a play}\} = \{\text{transmission failure at the MAC layer}\}$. The goal of the jammer/gambler is to make the delay/money larger than the threshold σ. To achieve this goal, the jammer/gambler must keep jamming/winning successfully in each transmission/play (i.e., event A always happens). However, once A^c happens, the gambler/jammer loses/fails (i.e., the message is successfully delivered within the delay constraint σ). The message invalidation ratio, which denotes the probability that the cumulative delay is larger than the threshold, is equivalent to the probability that the gambler reaches his goal before he loses.

Note that p_a denotes the transmission failure probability at the MAC layer. Since wireless MAC usually has its own retransmission mechanism due to CSMA/CA (e.g., the default long and short retry limits in IEEE 802.11g are 3 and 7, respectively), event A happens only when every MAC-layer transmission attempt is disrupted by the jammer. Thus, given the number of MAC layer transmission attempts N_{mac}, we obtain $p_a = p^{N_{\text{mac}}}$. Since it has been shown (e.g., [25]) that the collision probability due to legitimate traffic is small if the network is unsaturated, we neglect the impact of legitimate traffic on the MAC-layer transmission failure in our analysis. (We will consider the impact in experiments later).

We have set up the rules for our gambling game. We then use the gambling-based model to derive the message invalidation ratio of time-critical applications under jamming attacks. Before we proceed, we first present the definition of a martingale according to [24].

Definition 4 (Martingale): A process $\{X_n\}$ is called a martingale relative to a filtration $\{\mathcal{F}_n\}$, (A sequence of σ-algebras[3] $\{\mathcal{F}_n\}$ is called a filtration if $\mathcal{F}_n \subset \mathcal{F}_{n+1}$ for any $n \in \mathbb{N}$.) if (i) X_n is $\mathcal{F}_n$-measurable, (ii) $\mathbb{E}|X_n| < \infty$ for any $n \in \mathbb{N}$, (iii) $\mathbb{E}(X_n|\mathcal{F}_{n-1}) = X_{n-1}$ almost surely.

We then show that the gambler's money $\{X_n\}$ is in fact a martingale due to our construction.

Lemma 1: The process $\{X_n\}$ in (2) is a martingale.

Proof: Please refer to the proof in [26]. □

Next, we present our main result of the message invalidation ratio under jamming attacks.

Theorem 1 (Message invalidation ratio for general cases): Given a jamming strategy $\mathcal{J}_r(p)$, the message invalidation ratio r is

$$r = \frac{\mathbb{E}(D_s) - c/(1-p_a)}{\mathbb{E}(D_s) - p_a c/(1-p_a) - \mathbb{E}(D_u)}, \tag{4}$$

where $p_a = p^{N_{\text{mac}}}$, $c = \mathbb{E}(d_i)$ is the mean of the i.i.d. MAC-layer delay d_i, $D_s \le \sigma$ is the end-to-end delay of a successfully delivered message, and $D_u > \sigma$ is the delay of failed message delivery, defined as the interval from the instant that the transmitter starts transmitting a message to the instant that the transmitter stops retransmission due to message invalidation[4].

Proof: Please refer to the proof in [26]. □

Theorem 1 shows that the message invalidation ratio can be analytically represented only by first-order statistics. The result in Theorem 1 is general since it does not make further assumptions on the distribution of the MAC-layer delay. To illustrate intuitive relations between message invalidation ratio r, jamming probability p, and delay threshold σ, we present our complementary analytical result as follows.

Theorem 2 (General upper bound): For the message invalidation ratio r in Theorem 1, it satisfies that

$$r \le \frac{p^{N_{\text{mac}}}c}{(1-p^{N_{\text{mac}}})(\sigma - c) + p^{N_{\text{mac}}}c}.$$

Proof: Please refer to the proof in [26]. □

Remark 1: Theorem 2 provides a general upper bound of message invalidation ratio for time-critical applications. Note that when the jamming probability p is sufficiently small, $(1-p^{N_{\text{mac}}})(\sigma - c) \approx \sigma - c \gg p^{N_{\text{mac}}}c$. We obtain that the upper bound of r in Theorem 2 can be approximated as $p^{N_{\text{mac}}}c/(\sigma - c)$, indicating that the message invalidation ratio decays at least polynomially when p is small and decreasing to 0. Consequently, a small jamming probability p cannot lead to significant impact on the performance of time-critical applications.

Example 1: Fig. 4 numerically illustrates the upper bound of the message invalidation ratio for a time-critical application with 10ms$<\sigma<$100ms, N_{mac}=3, and $c = \mathbb{E}(d_i)$=1ms under the attack of a reactive jammer with $0<p<1$. We observe from Fig. 4 that the message invalidation ratio, as a function of jamming probability p, has a phase transition phenomenon. That is, as p increases, the message invalidation ratio has two distinct increasing phases: a slightly-increasing phase and a dramatically-increasing phase. For example, when σ=10ms, the transition point is approximately at p=0.7 and the corresponding upper bound of message invalidation ratio is r=5%. In other words, the upper bound only increases from 0% slightly to 5% as p goes from 0 to 0.7 and increases from 5% dramatically to 100% as p goes from 0.7 to 1.

[3] Note that σ-algebra is not related to the delay requirement σ.

[4] Note that the reason for $D_u > \sigma$ is that the MAC layer still needs to finish an ongoing transmission even though the application layer is aware that the cumulative delay exceeds the constant σ.

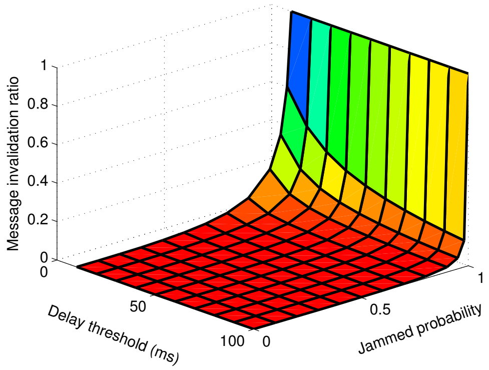

Fig. 4. Upper bound of message invalidation ratio for a time-critical application under reactive jamming.

3.2 Impact of Non-Reactive Jamming with $\mathcal{J}_{nr}(I)$

We next present our main results of the impact of non-reactive jamming on time-critical messages. For a non-reactive jammer with $\mathcal{J}_{nr}(I)$, its jamming interval I can be arbitrarily chosen to adopt various jamming patterns. Since it may be impractical to use one model to include all possible non-reactive jamming patterns, we considered two non-reactive jamming models that are widely-adopted in the literature [8], [10]: memoryless jamming (I is exponentially distributed) and periodic jamming (I is a constant).

By taking advantage of our previous result in Theorem 2, we have the following results for the two widely-used types of non-reactive jamming.

Proposition 1: For a non-reactive jamming strategy $\mathcal{J}_{nr}(I)$, (i) if I is exponentially distributed, the message invalidation ratio r can be upper-bounded by

$$r \leq \frac{c(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}}}{(1-(\sigma-c)(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}})+c(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}}}, \quad (5)$$

where $c = \mathbb{E}(d_i)$, L is the packet length (measured in time). (ii) If I is a constant, the message invalidation ratio r can be approximated as

$$r \approx \begin{cases} 1 & I \leq L \\ (1-\frac{\sigma(I-L)}{IL})\mathbf{1}_{\{2L\leq\sigma<\frac{IL}{I-L}\}}+\frac{L}{I}\mathbf{1}_{\{\sigma<2L\}} & L<I<2L \\ \frac{L}{I}\mathbf{1}_{\{\sigma<2L\}} & I > 2L, \end{cases} \quad (6)$$

where L is the packet length.

Proof: The proof consists of two parts.

(i) As the jamming interval between two adjacent jamming pulses is exponentially distributed, the probability that a jamming signal is generated during the physical transmission of a packet is $1-e^{-L\mathbb{E}(I)}$. Since exponential distribution is memoryless, the jamming probability for each physical transmission is always $1-e^{-L\mathbb{E}(I)}$. Thus, the memoryless jammer with strategy $J_{nr}(I)$ is equivalent to a reactive jammer with strategy $J_r(p)$, where $p = 1-e^{-L\mathbb{E}(I)}$. By using Theorem 2, we obtain

$$\begin{aligned} r &\leq p^{N_{\text{mac}}}c/((1-p^{N_{\text{mac}}})(\sigma-c)+p^{N_{\text{mac}}}c) \\ &\leq \frac{c(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}}}{(1-(\sigma-c)(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}})+c(1-e^{-L\mathbb{E}(I)})^{N_{\text{mac}}}}. \quad (7) \end{aligned}$$

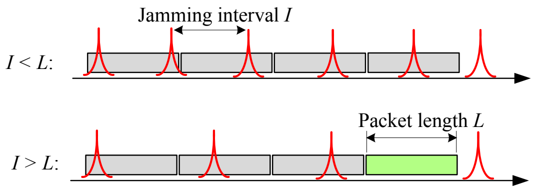

Fig. 5. Periodic jammers with intervals $I \leq L$ and $I > L$.

(ii) When I is a constant, the jammer is a periodic one. It is evident that when the jamming interval $I \leq L$, every physical transmission will be jammed, since there exists at least one jamming pulse during one transmission as shown in Fig. 5. Hence, we have

$$\mathbb{P}(\text{message invalid}|I \leq L) = 1. \quad (8)$$

When $I > L$, define event $B_i = \{$the i-th transmission is jammed$\}$. Consider the first transmission and event B_1, since the transmission and jamming processing are independent, $\mathbb{P}(B_1)$ is equivalent to the probability that there is a jamming pulse over a first transmission interval of L. Thus, $\mathbb{P}(B_1) = L/I$. The message invalidation probability can be represented as

$$\mathbb{P}(\text{message invalid}) = \mathbb{P}\left(\cap_{i=1}^{\sigma/L} B_i\right). \quad (9)$$

When $\sigma < 2L$ and the first transmission fails, even the second transmission succeeds, the message will still become invalid; therefore the message invalidation ratio depends only on the first transmission results. We then have

$$\mathbb{P}(\text{message invalid}|I>L,\sigma<2L) = \mathbb{P}(B_1) = I/L. \quad (10)$$

When $\sigma \geq 2L$ and $I \geq 2L$, the second transmission always succeeds. Then,

$$\mathbb{P}(\text{message invalid}|I \geq 2L, \sigma \geq 2L) = 0. \quad (11)$$

When $\sigma \geq 2L$ and $L < I < 2L$, the transmitter can make approximately σ/L transmission attempts to send the message. The jammer must jam all these transmission in order to disrupt the message delivery. Since the periodic jammer transmits pulses at a constant rate, events $\{B_i\}$ are dependent. We in the following use deduction to obtain the result for this case.

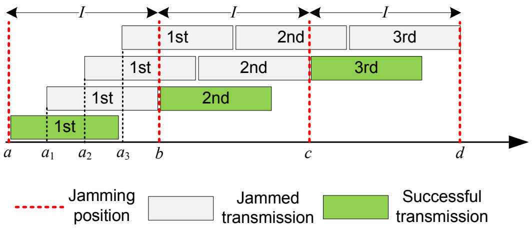

Fig. 6. Periodic jamming with $\sigma \geq 2L$ and $L < I < 2L$.

As shown in Fig. 6, if the first transmission arrives between times a and a_1 ($a_1 = a + (I - L)$), there will be no jamming during the transmission. Then, the first transmission will be jammed if and only if it arrives between times a_1 and b. However this time interval can only guarantee the first transmission to be jammed. If

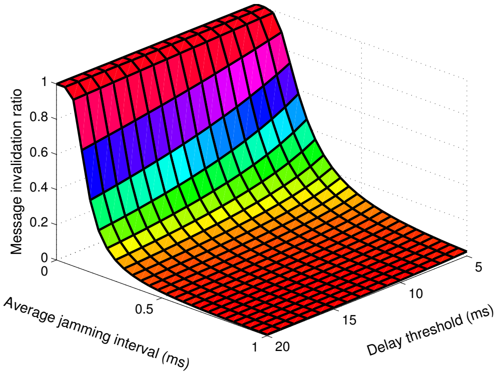

Fig. 7. The message invalidation ratio for a time-critical application under non-reactive memoryless jamming.

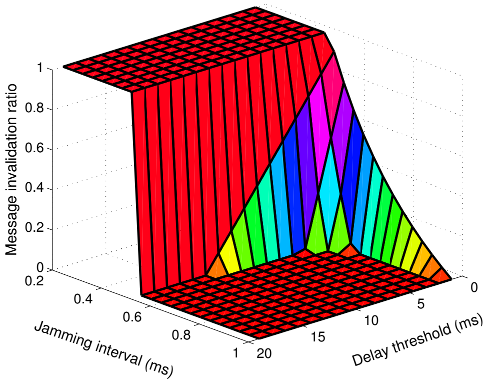

Fig. 8. The message invalidation ratio for a time-critical application under non-reactive periodic jamming.

the first transmission arrives between times a_1 and a_2 ($a_2 = a_1 + (I - L)$), there will be no jamming during the second transmission. Therefore, the first and second transmissions will be both jammed if and only if the first transmission arrives between times a_2 and b.

By using deduction, we obtain that all σ/L transmissions will be jammed if and only if the first transmission arrives between times $a_{\sigma/L}$ and b, where $a_{\sigma/L} = a + \sigma(I - L)/L$ and $b = a + I$. If $a_{\sigma/L} \geq b$, there always exists a transmission, during which there is no jamming pulse. Thus, we have

$$\mathbb{P}(\text{message invalid}|\sigma \geq IL/(I-L), L < I < 2L) = 0. \quad (12)$$

Otherwise, the message invalidation ratio is

$$\begin{aligned}&\mathbb{P}(\text{message invalid}|\sigma \geq IL/(I-L), L < I < 2L)\\&= \mathbb{P}(\text{first transmission arrives at } [a_{\frac{\sigma}{L}}, b])\\&= (I - \sigma(I-L)/L)/I = 1 - \sigma(I-L)/(IL). \quad (13)\end{aligned}$$

Combining (8), (10), (11), (12) and (13) yields the results of the impact of periodic jamming. □

Example 2 (Memoryless Jamming): Fig. 7 numerically illustrates the upper bound of the message invalidation ratio for a time-critical application with 5ms$<\sigma<$20ms, N_{mac}=3, L=0.5ms, and $c = \mathbb{E}(d_i)$=2ms under the attack of a memoryless jammer with 0ms$<\mathbb{E}(I)<$0.04ms. Different from Fig. 4, Fig. 7 shows that the message invalidation ratio consists of three decreasing phases: as the average jamming interval $\mathbb{E}(I)$ increases from 0, the message invalidation first remains 1, then dramatically decreases, and finally approaches 0.

Example 3 (Periodic Jamming): Fig. 8 illustrates the message invalidation ratio for a time-critical application with 1ms$<\sigma<$20ms and L=0.5ms under the attack of a periodic jammer with 0ms$<I<$1ms. Similar to Fig. 7, Fig. 8 shows that the message invalidation ratio also consists of three decreasing phases: as the jamming interval I increases from 0, the message invalidation first remains 1, then sharply decreases, and finally approaches 0.

Figs. 7 and 8 show that for non-reactive jamming, there always exists two critical values I_1 and I_2: If $\mathbb{E}(I) < I_1$, non-reactive jammers can almost disrupt all time-critical transmissions. If $\mathbb{E}(I) > I_2$, non-reactive jammers only cause negligible effect on time-critical transmission. Due to randomness, a memoryless jammer's message invalidation ratio transition region from 1 to 0 is much smoother than a periodic jammer.

Remark 2: Our analytical results show that for reactive jamming with $\mathcal{J}_r(p)$, there exists a phase transition phenomenon: the message invalidation ratio first has a slightly increasing phase and then dramatically increases to 1, as the jamming probability p increases from 0 to 1. For non-reactive jamming with $\mathcal{J}_{nr}(I)$, the message invalidation ratio first has the value of 1, then has a dramatically decreasing phase and finally approaches 0 as the jamming interval I increases from 0 to infinity.

4 Experimental Study

We have so far derived analytical results for a time-critical application under both reactive and non-reactive jamming attacks. Next, we perform extensive experiments to further investigate the jamming impact on time-critical wireless networks. As aforementioned, there are a few existing works [2], [22], [27], [28] that have shown the advantage and efficiency of wireless networks for the smart grid based on off-the-shelf wireless products (e.g., WiFi and CDMA). In this section, we use real-time experiments to show quantitatively to what extent jamming attacks can cause damages to a practical wireless network for smart grid applications.

4.1 Experimental Setups

4.1.1 GOOSE Applications

As IEC 61850 [6] is a recent smart grid communication standard for power substations, we choose IEC 61850 as our power communication protocol. Since GOOSE messages in IEC 61850 have very strict timing requirements, we use different GOOSE applications to evaluate the impact of jamming attacks on a wireless network. Specifically, we consider two protocol-defined GOOSE applications: Types 1A/P1 and 1A/P2 with constraints of 3ms and 10ms [6], respectively. We also consider two GOOSE applications for transfer trip protection and anti-islanding with delay constraints of 8-16ms and 150-300ms [2], respectively.

4.1.2 Implementation

We set up a WiFi-based wireless power network to evaluate the GOOSE performance under jamming attacks. Since GOOSE is mapped from the application layer directly to the MAC layer, we implement a GOOSE messaging module in the Linux kernel. Detailed setups are as follows. (i) Protocol: GOOSE over WiFi. (ii) IEEE 802.11g (ad-hoc mode) at 2.462 GHz. As GOOSE requires the highest priority, we use Madwifi to set min and max contention windows to be 4 and 8, respectively. We also set the retry limit to be 3. (iii) We use USRP N210 to set up three types of jammers: reactive, memoryless, and periodic jammers. For reactive jamming, we use C++ code to directly control USRP to sense and transmit. The fastest reactive time is observed around 600μs to 800μs (Less reactive time can be achieved by modifying FPGA [29]). The default jamming duration is set to be 22μ as given in [10]. We also calibrate the duration from 20μs to 150μs in experiments. (iv) We make WiFi run at 9Mbps instead of lower speed to make it more vulnerable to jamming. (v) In order to let the reactive jammer have time to react, null data is appended to each packet to make it long enough (800-1300 bytes) in experiments.

4.1.3 Performance Metric

We use the message invalidation ratio to measure the jamming impact. We transmit 1000 GOOSE messages for every GOOSE application in each experiment, We then measure the delay of each GOOSE message, compare the delay with the threshold and compute the message invalidation ratio.

4.2 A Two-Node-and-One-Jammer Scenario

Our first experiment is to evaluate a simple communication scenario that commonly exists in power systems: an electronic device observes an event (e.g., an abnormal status) and transmits a GOOSE message to inform the other of this event. The goal of this experiment is to show how a jammer can affect time-critical GOOSE transmissions between a single transmitter-receiver pair.

We show in Fig. 9 the impact of a reactive jammer on the message invalidation ratios of different GOOSE applications with delay limits of 3ms, 10ms, 16ms, and 200ms, respectively. It can be seen from Fig. 9 that every GOOSE application exhibits a phase transition phenomenon: when the jamming probability p is small, the message invalidation ratio is 0; and as p increases, the message invalidation ratio becomes non-zero and increases dramatically to 1. For example, in Fig. 9, when p goes from 0 to 0.6, the Type-1A/P2 (10ms limit) message invalidation ratio always remains zero, which implies that a small jamming probability p cannot lead to significant performance degradation. Fig. 9 also shows that less delay-sensitive GOOSE applications are not extremely vulnerable to reactive jamming attacks. For example, for the anti-islanding application, the message invalidation ratio is 0.1% at $p = 0.9$.

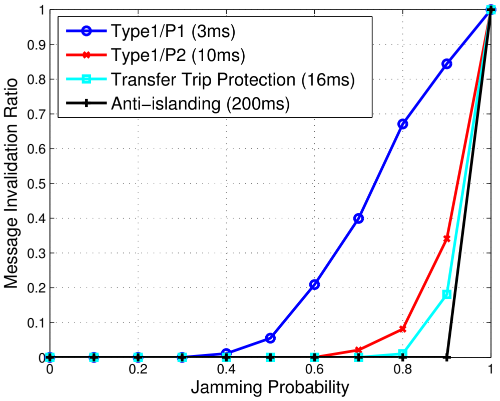

Fig. 9. The message invalidation ratios of four different GOOSE applications under reactive jamming.

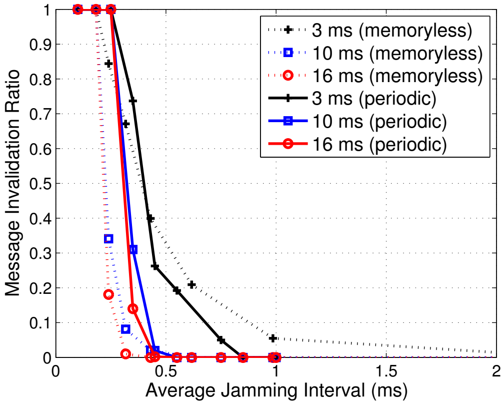

Fig. 10. The message invalidation ratios of GOOSE applications under non-reactive jamming.

We then show in Fig. 10 the impact of non-reactive jammers, including memoryless and periodic jammers, on GOOSE applications with the same setups used in Fig. 9. We can see from Fig. 10 that the message invalidation ratio decreases with the increasing of the (mean) jamming interval. The decreasing of the message invalidation consists of a slightly-decreasing phase (remaining 1), a sharply-decreasing phase (from 1 to 0), and another slightly-decreasing phase (approaching 0).

Fig. 10 also shows that, similarly to reactive jamming in Fig. 9, the phase transition phenomena become more evident as the delay threshold increases from 3ms to 16ms. This indicates that if a message has a sufficiently large delay threshold, the jamming interval has to be chosen smaller than the transmission time of one packet in order to disrupt the transmission of a message; otherwise, there always exists a packet whose transmission interval falls between two subsequent jamming pulses and then the message will be delivered successfully.

Note that the network throughput degradation due to jamming attacks has been well-studied for WiFi networks [10]. Comparing our experimental results with those in [10], we can find that a jammer that results in severe throughput degradation does not necessarily lead to a large message invalidation ratio. For example, when $p = 0.9$ for a reactive jammer, the throughput is degraded by 88% in our experiments, but the message invalidation ratio is 0.1% for the anti-islanding application in Fig. 9. Thus, the message invalidation ratio is an application-oriented performance metric and is more appropriate than the saturated throughput to quantify the performance of time-critical applications.

4.3 A Small-Scale Network Scenario

We now consider a WiFi-based power network scenario [30]: a transformer bay in a Type D2-1 power substation has two breaker intelligent electronic devices (IEDs), two protection-and-control (P&C) IEDs, and one merging-unit (MU) IED. All breaker IEDs and P&C IEDs periodically send updated meter values to a station server at a fixed rate of 20Hz. The MU IED periodically sends raw data messages to P&C IEDs at a rate of 920Hz, 2400Hz, or 4800Hz. (All setups are from [30].) Note that all traffic rates are measured at the application layer. We do not control the message transmission mechanism below the application layer. In fact, since we use the 802.11 MAC layer, the real traffic on the wireless channel may not be strictly periodic due to scheduling, backoff, and jamming. Our goal is to not only investigate the impact of jamming attacks but also evaluate the effect of legitimate traffic on GOOSE messaging in a small-scale power network over WiFi access.

TABLE 2
Message invalidation ratio versus reactive jamming probability p and transmission rate of the MU IED.

Type-1A/P1 GOOSE with 3ms limit						
p :	0	0.2	0.4	0.6	0.8	1
920 Hz:	0	0.006	0.044	0.275	0.694	1
2400 Hz:	0	0.008	0.051	0.281	0.701	1
4800 Hz:	0	0.008	0.052	0.289	0.737	1
Type-1A/P2 GOOSE with 10ms limit						
p :	0	0.2	0.4	0.6	0.8	1
920 Hz:	0	0	0	0.002	0.049	1
2400 Hz:	0	0	0	0.003	0.050	1
4800 Hz:	0	0	0	0.003	0.052	1

We first evaluate the impact of a reactive jammer. Table 2 shows the message invalidation ratios of Type-1A/P1 (3ms limit) and Type-1A/P2 (10ms limit) GOOSE messages transmitted from a breaker IED to a P&C IED. Note that the WiFi-based network is always unsaturated even when the transmission rate of the MU IED is 4800Hz. We can see from Table 2 that unsaturated traffic load has nearly negligible effect on the message invalidation ratio. For example, when the jamming probability p is fixed to be 0.8, the message invalidation ratio of Type-1A/P2 (10ms limit) GOOSE messages increases from 4.9% to 5.2% as the MU IED transmission rate goes from 920Hz to 4800Hz.

We next investigate the impact of non-reactive jammers on the same network. Table 3 shows the impact of a periodic jammer on Type-1A/P2 (10ms limit) GOOSE messages transmitted from a breaker IED to a P&C IED. We observe from Table 3 that for the periodic jammer, increasing unsaturated traffic load also has negligible effect on the message invalidation ratio. For example, when the jamming interval I=0.2ms, the message invalidation only increases by less than 1% as the raw data sampling rate goes from 920Hz to 4800Hz.

TABLE 3
Message invalidation ratio versus periodic jamming interval I and transmission rate of the MU IED.

I (ms):	0	0.1	0.2	0.3	0.4	0.5
920 Hz:	1	1	0.121	0	0	0
2400 Hz:	1	1	0.124	0	0	0
4800 Hz:	1	1	0.130	0	0	0

For our experiential results in Tables 2 and 3, we conclude that the increasing of unsaturated traffic load can only slightly degrade the performance of time-critical transmissions. It is also noted from Tables 2 and 3 that legitimate traffic does not affect the phase transition phenomenon of the message invalidation ratio. As a result, from the perspective of network performance evaluation, channel collision due to legitimate traffic can be regarded as a form of reactive jamming with very small jamming probability p, which has been shown to cause negligible impacts on time-critical transmission in both theoretical modeling and real-time experiments.

5 The Jamming Detector: JADE

We have modeled the impact of jamming attacks on time-critical applications and validated our analysis by performing experiments in a power network. Our analytical and experimental results provide a prerequisite to the design of jamming detectors for wireless smart grid applications. In this section, we implement a jamming detection system, JADE (Jamming Attack Detection based on Estimation) to achieve both efficiency and reliability in wireless applications in a power substation.

5.1 Design and Implementation

Due to the importance of power networks, a jamming detector should yield a reliable output within a short decision time to notify network operators of potential threats. Existing methods in general require an online profiling step, which periodically estimates parameters [8], [11] or infers statistical models [12], [19] from measured data, to provide empirical knowledge for jamming detection. For example, a sequential jamming detector proposed in [11] needs to estimate the transmission failure probabilities in both non-jamming and jamming cases before performing jamming detection. However, such profiling-based methods face several practical issues for time-critical systems: (i) the profiling phase inevitably increases the detection time; (ii) it is unclear in practice how much reliability the profiling phase can provide for later jamming detection.

As we can see, existing profiling-based detectors may not be directly used in practical power systems. Thus, we are motivated to design a new jamming detection system, JADE, to achieve reliability for jamming detection in power systems as well as to shorten the decision time, compared with existing profiling-based methods. The intuition of JADE is as follows.

First, the online profiling based methods are used in ad-hoc or sensor networks where network parameters for a node (e.g., number of nodes, background traffic) are usually considered unknown. Therefore, online profiling is essential for jamming detection to accommodate changes of network setups and topologies. However, nodes in a power network are usually static and have nearly predictable traffic (e.g., the raw data sampling rate and meter update rate of IEDs). Thus, on-line profiling is not necessary, and off-line profiling should be sufficient for jamming detection in a power network. In other words, the profiling can be done during the network initialization or maintenance period, thereby shortening the decision time by eliminating (or significantly reducing the frequency of) the online profiling process.

Second, the goal of both reactive and non-reactive jammers is to disrupt the message delivery by jamming packets. Thus, for any jammer, despite its jamming behavior, there always exists a jamming-induced probability, denoting the probability that a packet will be disrupted by jamming. In this regard, every jammer can be considered as a reactive jammer with certain jamming probability p. As we observed previously, the phase transition phenomenon for the reactive jamming case indicates that when the jamming probability p is sufficiently small, the jamming impact is nearly negligible. This means that in order to detect the presence of a harmful jammer, a detection system only needs to estimate the jamming probability $\hat{p}$, and then to compare the estimation with a critical jamming probability p^*, with which a jammer can cause non-negligible impact on power networks. If $\hat{p}$ is small, whether it is induced by channel collision, fading, or even jamming, it cannot lead to significant performance degradation. Otherwise, the detection system should raise an alarm.

Accordingly, we implement the JADE system at a MU IED that periodically transmits raw data samples at the rate of 920Hz [2]. JADE observes the transmission result of each data sample and estimates the jamming probability $\hat{p}$ by

$$\hat{p} = \frac{1}{N} \sum_{i=1}^{N} \mathbf{1}_{F_i}, \tag{14}$$

where N is the number of observations, and F_i denotes the event that the i-th transmission fails.

After the estimation in (14), JADE raises a jamming alarm if $\hat{p} > p^*$. Detailed setups of JADE are shown in Algorithm 1. The threshold p^* can be chosen via offline profiling (i.e., via either theoretical analysis or experiments). In particular, as aforementioned, nodes in a power network are usually static and have nearly predictable network traffic for monitoring and control. In other words, network setups including the number of nodes, network topology, traffic rates and timing requirements are all known to the network operator. In this regard, the threshold p^* can be chosen after the message invalidation ratio, as a function of jamming probability p, is computed. The choice of p^* can be further verified and adjusted by experiments during network setup and maintenance periods.

Algorithm 1 : A single-round detection in JADE

```
Given: Threshold $p^*$, Number of needed samples $N$.
Initialization: $n \leftarrow 0, \hat{p} \leftarrow 0$.
repeat
  Transmit a packet and $n \leftarrow n + 1$.
  if transmission failure then
    $\hat{p} \leftarrow ((n-1) * \hat{p} + 1)/n$
  else
    $\hat{p} \leftarrow (n-1) * \hat{p}/n$
  end if
until $n$ is equal to $N$
If $\hat{p} > p^*$, print Jamming Alarm.
```

Note that when JADE transmits a message, it will use a time counter to measure the time when the ACK returns. If the ACK never returns and the counter reaches the timeout, JADE will conclude the transmission fails.

5.2 Performance Analysis

In this subsection, we present the theoretical performance analysis of the JADE detection system. We use two conventional metrics: detection and false alarm probabilities to measure the performance of JADE. Specifically, we have the following results.

Theorem 3: (i) If there is a jammer with jamming probability p, the JADE system with detection threshold p^* has a detection probability of

$$P_D = \mathbb{P}(\hat{p} > p^*) \approx Q\left(\frac{p^* - p}{p(1-p)N}\right), \tag{15}$$

where $Q(\cdot)$ is the Q-function, written as $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$. (ii) If there is no jamming and wireless fading leads to a transmission failure probability of p_0, the JADE system with detection threshold p^* has a false alarm probability of

$$P_F = \mathbb{P}(\hat{p} > p^*) \approx Q\left(\frac{p^* - p_0}{p_0(1-p_0)N}\right), \tag{16}$$

where $Q(\cdot)$ is the Q-function.

Proof: (i) The estimation of p is written as $\hat{p} = \frac{1}{N}\sum_{i=1}^{N} \mathbf{1}_{F_i}$, where $\mathbf{1}_{F_i}$ follows the bernoulli distribution

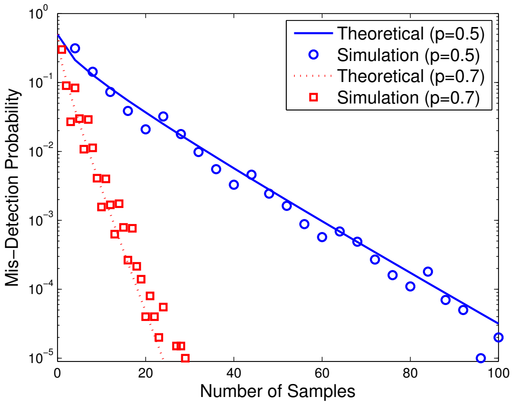

Fig. 11. Theoretical mis-detection probability $(1 - P_{\scriptscriptstyle D})$ versus simulated mis-detection probability. The threshold p^* is set to be 0.3. The jammer has two probabilities: $p = 0.5$ and $p = 0.7$.

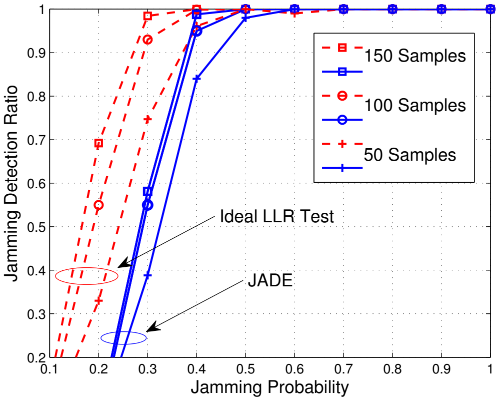

Fig. 12. Jamming detection ratios of both JADE and the likelihood ratio test in the presence of a jammer with different jamming probabilities.

with parameter p. We have $\mathbb{E}(\mathbf{1}_{F_i}) = p$ and $\text{Var}(\mathbf{1}_{F_i}) = p(1-p)$.

Define a new sequence $\{Z_N\}$ to be $Z_N = \frac{\hat{p}-p}{\sqrt{p(1-p)/N}}$. Then, $\hat{p} = p + Z_N\sqrt{p(1-p)/N}$.

From the central limit theorem, as $N \to \infty$, Z_N converges in distribution to a normally distributed random variable with zero mean and variance 1; i.e., $Z_N \sim \mathcal{N}(0,1)$. Accordingly,

$$\hat{p} \sim \mathcal{N}\left(p, p(1-p)/N\right) \quad \text{as } N \to \infty. \tag{17}$$

Thus, the detection probability, the probability that $\hat{p} > p^*$, can be denoted as

$$P_{\scriptscriptstyle D} = \mathbb{P}(\hat{p} > p^*) \approx Q\left((p^* - p)\sqrt{N}/\sqrt{p(1-p)}\right), \tag{18}$$

where $Q(\cdot)$ is the Q-function.

(ii) Similarly to (i), the estimation $\hat{p}$ can be approximated as a Gaussian random variable:

$$\hat{p} \sim \mathcal{N}\left(p_0, p_0(1-p_0)/N\right) \quad \text{as } N \to \infty. \tag{19}$$

Thus, the false-alarm probability, the probability that $\hat{p} > p^*$, can be denoted as

$$P_{\scriptscriptstyle D} = \mathbb{P}(\hat{p} > p^*) \approx Q\left(\frac{(p^* - p_0)\sqrt{N}}{\sqrt{p_0(1-p_0)}}\right). \tag{20}$$

□

Fig. 11 shows the theoretical results of the mis-detection probability $(1-P_D)$ in comparison with simulation results. It is noted from Fig. 11 that the detection performance of JADE improves as the number of samples N increases. Further, when the jammer becomes aggressive, i.e., p becomes large, JADE can achieve better detection performance. For example, when the number of samples N is 20, p increases from 0.5 to 0.7, the mis-detection probability of JADE decreases from 0.02 to 0.00004. Hence, JADE achieves accurate jamming detection for aggressive jammers.

5.3 Experimental Results

We then use the experimental power network in Section 4.3 to assess the performance of JADE. As the lowest bound of GOOSE delay is 3ms, we choose the corresponding critical jamming probability (detection threshold) p^*=0.3 from experimental results in Fig. 9. We also implement the statistically optimal likelihood ratio (LLR) test in our experiments for performance comparison. (A sequential version of the LLR test is used in [11].) The LLR test first requires a profiling step to estimate the packet jammed probability. During our experiments, we assume that the LLR test knows the information perfectly; i.e., we set exactly the same jamming probability in the LLR test as that used by the jammer. Thus, we refer to this detector as the ideal LLR test. Given the raw data transmission rate of 920 Hz, we set N=50, 100 and 150 samples such that the corresponding decision time for detection is 54 ms, 109 ms and 163 ms, respectively.

We also note that

5.3.1 *Reactive Jamming*

We first consider the detection performance of JADE on reactive jamming. Fig. 12 shows the jamming detection ratios (i.e. the probability that a detector issues an alarm when there indeed exists jamming) of both JADE and the ideal LLR test. We can see that the ideal LLR test outperforms JADE significantly when the jamming probability $p < 0.3$. This is because JADE does not target jamming attacks with jamming probability $p < p^* = 0.3$. Since the phase transition phenomenon has shown that less aggressive jammers cannot dramatically affect the performance of time-critical traffic, a jammer with jamming probability $p < 0.3$ that attempts to evade the JADE detection will fail to cause noticeable message invalidation ratios. It is further observed from Fig. 12 that when the jamming probability is greater than 0.3, the ideal LLR test and JADE achieve comparable performance especially when the number of samples N is

TABLE 4
Detection Ratios of both JADE and Likelihood Ratio Test in the presence of a time-varying jammer.

Number of Samples:	50	100	150	200
JADE:	98.6%	99.1%	100%	100%
LLR Test:	91.3%	92.1%	92.5%	91.6%

TABLE 5
Jamming detection ratios of JADE for periodic jamming with different jamming intervals.

Interval (ms):	0.4	0.5	0.6	0.7	0.8	0.9
100 Samples:	100%	100%	84.5%	0%	0%	0%
150 Samples:	100%	100%	97.4%	0%	0%	0%
200 Samples:	100%	100%	100%	0%	0%	0%

large. For example, when N=150 and p=0.4, the detection ratios of JADE and the ideal LLR test are 98.4% and 99.1%, respectively. Thus, JADE is able to detect harmful jamming attacks with nearly optimal performance.

It is well known that the performance of the LLR test could be degraded by model mismatch due to imperfect estimation or insufficient profiling. To compare the robustness of JADE with that of the LLR test, we design a sophisticated jammer that keeps changing its jamming probability randomly and uniformly within $[0.4, 0.9]$. In this case, the LLR test first estimates the jamming probability and then performs jamming detection based on the estimation output. Table 4 shows the detection ratios of both JADE and the LLR test for N=50, 100, 150, and 200. We can see that JADE is more robust than the LLR test to detect such a time-varying jammer. Because of the model mismatch problem, we observe from Table 4 that increasing the number of samples cannot improve the performance of the LLR test.

5.3.2 Non-Reactive Jamming

We then consider the detection performance of JADE on non-reactive jamming. We use the same network setups as in previous experiments for reactive jamming. The threshold of JADE is set to be $p^* = 0.3$. Table 5 shows the detection performance of JADE on a periodic jammer for different numbers of data samples. We observe that JADE detection performance exhibits a sharp phase transition when the jamming interval I goes from 0.6ms to 0.7ms, indicating that JADE yields very accurate detection for aggressive periodic jammers (small jamming intervals) yet has very poor performance for mild periodic jammers. However, as shown in Fig. 10, when the periodic jamming with jamming interval larger than 0.7, the message invalidation ratio is smaller than 0.1, implying that though such a jammer is likely to evade the detection of JADE, it cannot cause severe performance degradation of time-critical applications. Thus, JADE is able to provide accurate detection for both reactive and non-reactive jamming attacks that can cause significant impact on wireless time-critical applications.

5.4 Discussions

Our experimental results showed that JADE achieves efficient and robust jamming detection for aggressive and harmful jammers, at the cost of low detection ratio for less-aggressive jammers. We note that JADE is an application-oriented detector that can be applied directly to practical wireless power systems. It is worth noting that during our experiments, we also used the false alarm probability to evaluate the performance of both JADE and the LLR test. We found that neither JADE nor the LLR test issues a jamming alarm when there exists no jamming, since the wireless network is unsaturated and transmission failure rarely happens.

Note that jamming detection is the first step to defend against jamming attacks. Anti-jamming systems must be designed and deployed for time-critical applications. For example, forward error correction (FEC) coding is able to combat jamming signals with duration of several bits that is within the FEC ability; using undisclosed secret keys in spread spectrum is very effective against jammers that have no knowledge to the keys; and some advanced spread spectrum schemes (e.g., [17], [31]) can eliminate the requirement of the secret keys. In addition, smart jamming strategies (e.g. attacking 802.11 rate adaption [32]) have been proposed recently to affect the network performance severely. As a result, our future work includes designing anti-jamming schemes against basic and sophisticated attacking strategies (e.g., rate-adaption attacks [32]) in time-critical applications.

It is also worth noting that in our theoretical modeling, a jammer always uses a constant jamming probability p. However, in practice, the jammer may choose a dynamic jamming probability p to extend its strategy. For example, it may increase p in each retransmission. How such a dynamic strategy affects time-critical wireless applications requires more theoretical investigation, which will be one of our future work.

6 Conclusions

In this paper, we provided an in-depth study on the impact of jamming attacks against time-critical smart grid applications by theoretical modeling and system experiments. We introduced a metric, message invalidation ratio, to quantify the impact of jamming attacks. We showed via both analytical analysis and real-time experiments that there exist phase transition phenomena in time-critical applications under a variety of jamming attacks. Based on our analysis and experiments, we designed the JADE system to achieve efficient and robust jamming detection for power networks.

References

[1] Office of the National Coordinator for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," *NIST Special Publication 1108*, 2009.

[2] 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. of IEEE PES General Meeting (PES '09)*, July 2009.

[3] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," in *Tech. Report, Pacific Northwest National Laboratory*, Jan. 2010.

[4] Wi-Fi Alliance, "WiFi for the smart grid: Mature, interoperable, security-protected technology for advanced utility management communications," Sept. 2009.

[5] NIST Smart Grid Homepage, "Smart grid panel agrees on standards and guidelines for wireless communication, meter upgrades," *News Release*, Apr. 19 2011.

[6] IEC Standard, "IEC 61850: Communication networks and systems in substations," 2003.

[7] X. Lu, Z. Lu, W. Wang, and J. Ma, "On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP," in *Proc. of IEEE Globecom' 11*, Dec. 2011.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of ACM MobiHoc '05*, 2005, pp. 46–57.

[9] L. Sang and A. Arora, "Capabilities of low-power wireless jammers," in *Proc. of IEEE INFOCOM '09 mini-conference*, Apr. 2009.

[10] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *Proc. of IEEE INFOCOM '08*, Apr. 2008, pp. 1265–1273.

[11] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. of IEEE INFOCOM '07*, May 2007, pp. 1307–1315.

[12] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," *IEEE Trans. Info. Forensics and Security*, vol. 3, pp. 347–358, Sept. 2008.

[13] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. of IEEE Symposium on Security and Privacy*, May 2008, pp. 64–78.

[14] M. Strasser, C. Popper, and S. Capkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proc. of ACM MobiHoc '09*, 2009.

[15] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. of IEEE INFOCOM '08*, Apr. 2008.

[16] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. of IEEE INFOCOM '07*, May 2007, pp. 2526–2530.

[17] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. of IEEE INFOCOM '10*, Mar. 2010.

[18] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. of USENIX Security Symposium (Security '09)*, Aug. 2009.

[19] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," in *Proc. of IEEE ICC '09*, Jun. 2009.

[20] A. Shevtekar and N. Ansari, "Do low rate dos attacks affect QoS sensitive VoIP traffic?" in *Proc. of IEEE ICC' 06*, June 2006.

[21] E. Casini, A. van der Zanden, R. Goode, and R. Berto-Monleon, "IP QoS with military precedence level for the NATO information infrastructure," in *Proc. of IEEE MILCOM' 11*, Nov. 2011.

[22] F. Cleveland, "Uses of wireless communications to enhance power system reliability," in *Proc. of IEEE PES General Meeting (PES '07)*, June 2007.

[23] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions," *IEEE Trans. Networking*, vol. 15, pp. 159–172, Feb. 2007.

[24] W. David, *Probability with Martingales*. Cambridge University, 1991.

[25] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE Trans. Networking*, vol. 16, no. 4, pp. 791–802, Aug. 2008.

[26] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. of IEEE INFOCOM' 11*, Apr. 2011.

[27] S. Emrich, "Dispelling the myths associated with spread spectrum radio technology in electric power SCADA networks," in *Proc. of IEEE PES General Meeting (PES '07)*, June 2007.

[28] H. J. Zhou, C. X. Guo, and J. Qin, "Efficient application of GPRS and CDMA networks in SCADA system," in *Proc. of IEEE PES General Meeting (PES '10)*, July 2010.

[29] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactive jamming in wireless networks: how realistic is the threat?" in *Proc. of ACM WiSec' 11*, 2011.

[30] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. Power Delivery*, vol. 22, no. 3, July 2007.

[31] A. Cassola, T. Jin, G. Noubir, and B. Thapa, "Efficient spread spectrum communication without preshared secrets," *IEEE Trans. Mobile Computing*, vol. 12, Aug. 2013.

[32] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of ieee 802.11 rate adaptation algorithms against smart jamming," in *Proc. of ACM WiSec' 11*, 2011.

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

Wenye Wang received the M.S.E.E. degree and Ph.D. degree in computer engineering from the Georgia Institute of Technology, Atlanta, in 1999 and 2002, respectively. She is an Associate Professor with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC. Her research interests include mobile and secure computing, modeling and analysis of wireless networks, network topology, and architecture design. Dr. Wang 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 recipient of the NSF CAREER Award 2006. She is the co-recipient of the 2006 IEEE GLOBECOM Best Student Paper Award - Communication Networks and the 2004 IEEE Conference on Computer Communications and Networks (ICCCN) Best Student Paper Award.

Cliff Wang graduated from North Carolina State University with a PhD degree in computer engineering 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 associate faculty member of computer science in the College of Engineering at North Carolina State University. Dr. Wang has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently information security.