Real Time Implementation of Overcome Frequency Jammer

S. Jayadhurga1, S. Malathi2, P. Udayakumaran3
1,2 Final Year Student,3Assistant Professor,Departmet of ECE
MRK Intitute Of Technology, Kattumannarkoil, Tamilnadu

***Abstract*-----Mobile phones play an important role in our day to day life. Inspite of various limitations, it is a part and partial of human life. Hence we can't avoid the usage of mobile phones, thus we have to eliminate its drawbacks to make it more efficient. This paper also deals with the most common drawback of using mobile phones, it is nothing but usage of mobile phones in prohibited areas. A common board or a watch keeper insists the people who get inside the mobile phone prohibited areas like Temples, Conference halls, Hospitals etc., to switch off their mobile phones. It is prohibited in those areas in order to avoid noise pollution, mainly. Though it is insisted some people won't do it and some won't notice it. This is all about this project, to automatically disable the mobile phones in these prohibited areas.**

I. 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, 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 .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). The delivery of such messages is expected to be followed by a sequence of actions on physical infrastructures. Over-due 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. 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. Although there have been significant advances towards jamming characterization and countermeasures 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 level such as packet send/delivery ratio and the number of jammed packets (because existing data services are based on packet-switched networks), or at the network level such as saturated network throughput. However, packet-level and network-level metrics do not directly reflect the latency constraints of message exchange in time-critical applications. 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 .The former refers to those attacks 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.

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 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. 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. We describe preliminaries and the definition of message invalidation ratio. 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. we design and implement the JADE system for the substation network.

II. BLOCK DIAGRAM DESCRIPTION

Restricted Area Section

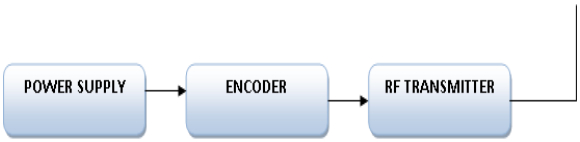

Fig.1.Block diagram for restricted area section

Mobile Section

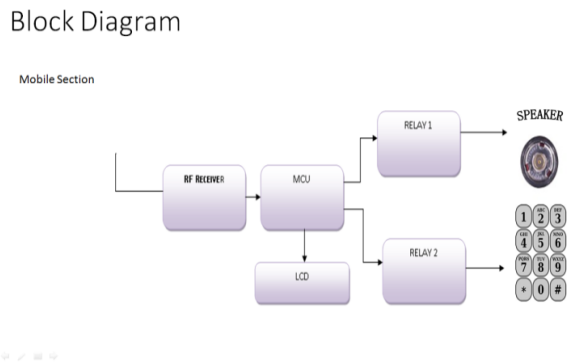

Fig.2.Block diagram for mobile section

III. EXISTING SYSTEM

Muting Mobile ,Voice Mail Converter. In Temples, Restaurants where people get irritated with the noise polluted by the Cell Phone users, where they talk loudly which creates annoyance to others and also due to the ring tones. Frequency jammer technology came under existence which was a temporary solution. Though it eradicated those problems it is not a suitable & good solution.But the main reason why it is not suitable is because of a first and foremost reason. The purpose of using cell phone is affected. Here when we enter the area the mobile phone is set under not reachable state, thus there are chances of missing some important calls. Hospitals and the Airplanes the Electromagnetic waves radiated from the Handsets causes disturbances to those electronic equipments.

IV. PROPESED SYSTEM.

In this we Propose a concept for overcome this, it consists of two devices former the restricted area (Class rooms, hospitals etc..) section once we enter this area the RF signal transfer's from the restricted area to mobile immediately it changes to locking mode. If mobile receives the call, it indicates but speaker and keypad are not working, if you want attend the call exit that place.

- Intelligent system
- Automatic keypad and speaker locking system

It is not affected any emergency call

V. MODELS AND PROBLEM STATEMENT.

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

A. 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). 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.

• Time-critical traffic is used for monitoring, control and protection of electronic devices on physical infrastructures. Such traffic has even more Time-Critical Message Types in IEC 61850 Stringent timing requirements than conventional
delay-sensitive traffic (e.g., video streaming on the Internet). For example, IEC 61850 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 constraints1: 3ms and 10ms.

• Non-time-critical traffic is used for general-purpose exchange of system data, such as logging or file transferring. 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* 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-criticalmessages 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

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.

B. Jamming Models

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

1) Reactive jammers are aware of the target communication systems. They stay quiet when the channel is idle, but start transmitting radio signa to undermine ongoing communication as soon as they sense activity on the wireless channel.

2) 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 Jr(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. For a non-reactive jammer, the jamming interval I is an essential parameter 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 Jnr(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 ; when I is exponentially distributed, the model becomes the memoryless jamming model. Although existing work 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.

C. 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. 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, which can be supported efficiently by IEEE 802.11g/n. In a wireless monitoring network, 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 ad-hoc networks, wireless sensor networks, wireless broadcast networks , and WiFi networks. 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 nonreactive 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. 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 nonreactive jammer is battery-supplied, it may choose a large to conserve energy, which implies that the larger I, the lower the jammer's cost.

D. 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 $r = \mathbf{1}P\{D>\sigma\}$, 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 *Jr(p)* and *Jnr(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.

VI. 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 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.

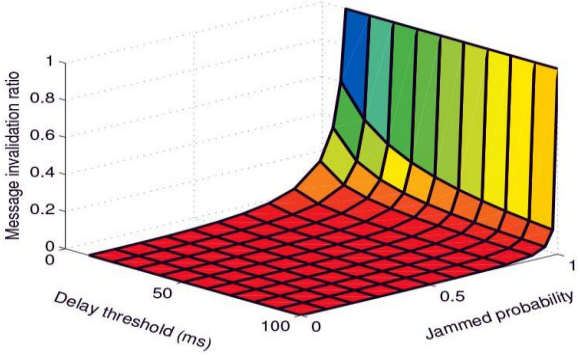

Fig. 3. Upper bound of message invalidation ratio for a time-critical application under reactive jamming.

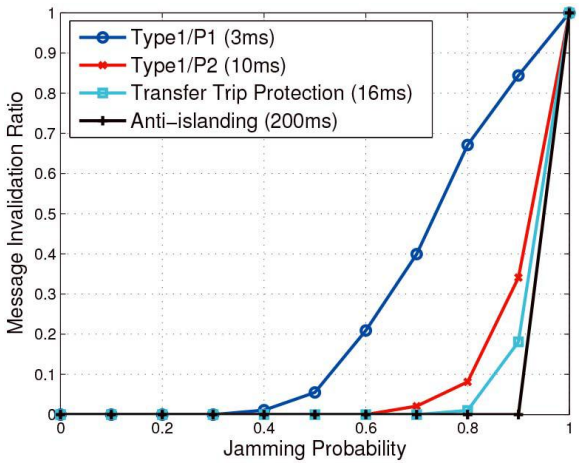

Fig.4.Message invalidation ratios of four different GOOSE applications under reactive jamming

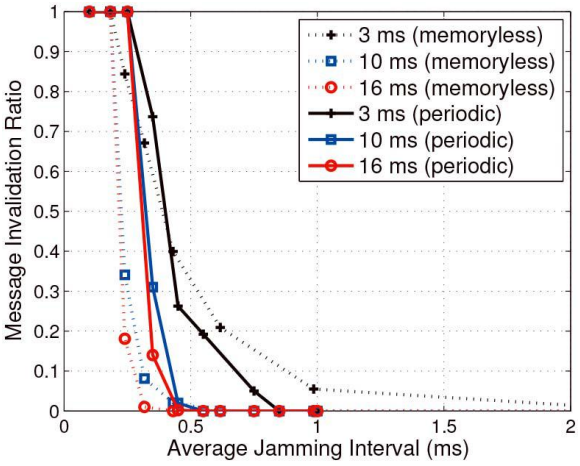

Fig.5.Message invalidation ratios of GOOSE applications under nonreactive jamming

VII. THE JAMMING DETECTOR: JADE

We have modeled the impact of jamming attacks on timecritical 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.

A. 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

Algorithm 1: A single-round detection in JADE
Given: Threshold $p_\star$, 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 $\hat{p} > p_\star$, **print** Jamming Alarm.

VIII. WORKING

In this we Propose a concept for overcome this, it consists of two devices former the restricted area (Class rooms, hospitals etc..) section once we enter this area the RF signal transfer's from the restricted area to mobile immediately it changes to locking mode. If mobile receives the call, it indicates but speaker and keypad are not working, if you want attend the call exit that place. Intelligent system Automatic keypad and speaker locking system It is not affected any emergency call.

IX. CONCLUSION

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*, pp. 1–145, 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. IEEE PES General Meeting*, Calgary, AB, Canada, Jul. 2009.
[3] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," Pacific Northwest National Lab., Richland, WA, USA, Tech. Rep. PNNL-19084, Jan. 2010.
[4] M. Tanaka, D. Umehara, M. Morikura, N. Otsuki, and T. Sugiyama, "New throughput analysis of long-distance IEEE 802.11 wireless communication system for smart grid," in *Proc. IEEE SmartGridComm*, 2011.
[5] NIST Smart Grid Homepage. (2011 Apr. 19). Smart grid panel agrees on standards and guidelines for wireless communication, meter upgrades. *News Release* [Online]. Available: http://www.nist.gov/smartgrid/smartgrid-041911.cfm
[6] *Communication Networks and Systems in Substations*, IEC Standard 61850, 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. IEEE GLOBECOM*, Houston, TX, USA, 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. ACM MobiHoc*, Urbana-Champaign, IL, USA, 2005, pp. 46–57.
[9] L. Sang and A. Arora, "Capabilities of low-power wireless jammers,"in *Proc. IEEE INFOCOM Mini-Conf.*, Rio de Janeiro, Brazil,Apr. 2009.

[10] E. Bayraktaroglu *et al*., "On the performance of IEEE 802.11 underjamming," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, 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. IEEE INFOCOM*, 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. Inf. Forensics Security*, vol. 3, no. 3, pp. 347–358, Sep. 2008.

[13] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jammingresistant key establishment using uncoordinated frequency hopping,"in *Proc. IEEE Symp. Security and Privacy*, Washington, DC,USA, May 2008, pp. 64–78.

[14] M. Strasser, C. Popper, and S. Capkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proc. ACM MobiHoc*, New Orleans, LA, USA, 2009.

[15] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, 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. IEEE INFOCOM*, 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. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010.

[18] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. USENIX Security*, Berkeley, CA, USA, Aug. 2009.

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