JADE: Detection of Jamming Attacks in Wireless Ad Hoc Networks

J. Patankar[Guide], Rohini Katore, Shivani Tadpelliwar, Vaishnavi Singreddiwar, Shweta Toradmal

Abstract-*Time-critical wireless applications in emerging network systems, such as e-healthcare and smart grids, have been drawing increasing attention in both industry and academia. The broadcast nature of wireless channels unavoidably exposes such applications to jamming attacks. However, existing methods to characterize and detect jamming attacks cannot be applied directly to time-critical networks, whose communication traffic model differs from conventional models. In this paper, we aim at modelling and detecting jamming attacks against time-critical traffic. We introduce a new metric, message invalidation ratio ,to quantify the performance of time-critical applications. A key insight that leads to our modelling is that the behaviour of a jammer who attempts to disrupt the delivery of a time-critical message can be exactly mapped to the behaviour of a gambler who tends to win a gambling game. We show via the gambling-based modelling and real-time experiments that there in general exists a phase transition phenomenon for a time-critical application under jamming attacks: as the probability that a packet is jammed increases from 0 to 1, the message invalidation ratio first increases slightly (even negligibly), then increases dramatically to1. Based on analytical and experimental results, we further design and implement the JADE (Jamming Attack Detection based on Estimation) system to achieve efficient and robust jamming detection for time-critical wireless networks.*

I. INTRODUCTION

1.1 Overview

Emerging time-critical wireless systems, such as wireless e-healthcare and wireless power networks, provide a new paradigm of modern wireless networks, whose primary goal is to achieve efficient and reliable message delivery for monitoring and control purposes, instead of providing data services for clients. Hence, a large amount of communication traffic is time-critical in such networks. For example, data messages in power substations are required to be delivered with specific latency constraints, ranging from 3 milliseconds (ms) to 1 second. Due to their significance to human beings e.g. e-healthcare and societies e.g. power grids; it is of crucial importance to guarantee network availability for such time-critical wireless networks. However, on the other hand, the shared nature of wireless channels inevitably exposes wireless networks to jamming attacks that may severely degrade the performance of these time-critical networks. Although great progress has been made towards jamming characterization and countermeasure for conventional networks, little attention has been focused on time-critical wireless networks. Indeed, time-critical networks pose challenging issues to existing Research on jamming attacks. In conventional networks, the jamming impact is evaluated at packet level e.g. packet send/delivery ratio, the number of jammed packets or network level e.g. saturated network throughput However, packet-level or network-level metrics do not directly reflect the latency constraints of time-critical applications. Hence, conventional performance metrics cannot be readily adapted to measure the jamming impact on time-critical applications. Further, lack of the knowledge how jamming attacks affect time-critical traffic leads to a gray area in the design of jamming detection in time-critical networks: it becomes impractical to achieve efficient jamming detection since detectors are not able to accurately identify jamming attacks, which can cause potentially severe performance degradation of time critical applications. Therefore, towards time-critical wireless applications, a fundamental question remains unsolved: How to model, analyze, and detect jamming attacks against time critical traffic?

1.2 Brief Description:

In this paper, we study the problem of modelling 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], that stay quiet when the wireless channel is idle, but start transmitting radio signals to undermine on-going communication as soon as they sense activity on the channel. The latter, however, is not aware of any behaviour of legitimate nodes and transmits radio jamming signals with its own strategy. There are two key observations that drive our modelling 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 behaviour of the jammer is exactly the same as the behaviour 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 ˆp and then compares ˆp 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]. 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.

1.3 Problem Definition

To implement a model,the time-critical transmission mechanism and jamming strategies which defines a performance metric to model the impact of jamming attacks on time-critical traffic.

We have modelled 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.

II. MODULE DESCRIPTION

1. Cluster configuration

In this module, each node registers the details such as Node IP address, port number, and distance. Node details are stored and maintained in sever database. After that node enters the ip address and port number to activate themselves in the network. Clusters are capable of performing multiple complex instructions by distributing workload across all connects servers. Clustering improves the system availability to users, its aggregate performance, and overall tolerance to faults and component failures. A failed sever is automatically shut down and its users are switched instantly to the other servers.

2. Estimate Message Invalidation Ratio

Message Invalidation Ratio is mainly used to quantify the performance of the time critical application in the presence of Reactive as well as Non-Reactive jammer. Consider a transmitter that needs to send a time critical message with delay constraint σ, and a jammer with strategy *Jr(p)* that attempts to disrupt message delivery in the network. 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 б.

3. Detect the Jammer : JADE

The implement a jamming detection system, JADE (Jamming Attack Detection based on Estimation) to achieve both efficiency and reliability in wireless application. A jamming detector should yield a reliable output within a short decision time to notify network operators of potential threats. Exiting methods in general require periodically estimates parameter or infers statistical models from measured data, to provide empirical knowledge for jamming detection. A sequential jamming detector proposed in needs to estimate the transmission failure probabilities in both non-jamming and jamming cases before performing jamming detection. It faces several issues for time critical system.
(i)The profiling phase inevitably increases the detection time.
(ii) it is unclear in practice how much reliability.

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..

4. Anti-jamming

Received Signal Strength Indicator (RSSI) value, generally in telecommunications, signal strength refers to the magnitude of the electric field at a reference point that is at a significant distance from the transmitting node to receiving location. It may also be referred to as received signal level or field strength. By using this strategy, RSSI value is computed based on Packet Delivery Ratio (PDR).Jammer sends more signals than the trusted node. With the help of this, frequency of the signals is increases. There is a special interval of RSSI value, which is below the normal signal strength, meaning that the link is weak. In that case, the algorithm will return a normal state, (because of low PDR value). Otherwise it detects that jammer tries to slowdown the time critical message transmission speed. Hence this way Anti jamming system works.the privacy-preserving public cloud data auditing system, which met all above requirements. To support efficient handling of multiple auditing tasks, they further explored the technique of bilinear aggregate signature to extend the main result into a multi-user setting, where TPA could perform multiple auditing tasks simultaneously. Extensive security and performance analysis showed the proposed schemes were provably secure and highly efficient.

III. RELATED WORK

1. Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution (2009).

Description:

Mobile ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security sensitive operations are still the main applications of ad hoc networks. One main challenge in design of these networks is their vulnerability to Denial-of-Service (DoS) attacks. In this paper, we consider a particular class of DoS attacks called Jamming. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets. We propose in this study a new method of detection of such attack by the measurement of error distribution.

2.Jamming resistant Broadcast Communication without Shared Keys(2009).

Description:

Jamming-resistant broadcast communication is crucial for safety-critical applications such as emergency alert broadcasts or the dissemination of navigation signals in adversarial settings. These applications share the need for guaranteed authenticity and availability of messages which are broadcasted by base stations to a large and unknown number of (potentially untrusted) receivers. Common techniques to counter jamming attacks such as Direct-Sequence Spread Spectrum (DSSS) and Frequency Hopping are based on secrets that need to be shared between the sender and the receivers before the start of the communication. However, broadcast anti-jamming communication that relies on either secret pairwise or group keys is likely to be subject to scalability and key-setup problems or provides weak jamming resistance, respectively. In this work, we therefore propose a solution called Uncoordinated DSSS (UDSSS) that enables spread-spectrum anti-jamming broadcast communication without the requirement of shared secrets. It is applicable to broadcast scenarios in which receivers hold an authentic public key of the sender but do not share a secret key with it. UDSSS can handle an unlimited amount of receivers while being secure against malicious receivers. We analyze the security and latency of UDSSS and complete our work with an experimental evaluation on a prototype implementation.

3. Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks (2008).

Description:

Carrier-sensing multiple-access with collision avoidance (CSMA/CA)-based networks, such as those using the IEEE 802.11 distributed coordination function protocol, have experienced widespread deployment due to their ease of implementation. The terminals accessing these networks are not owned or controlled by the network operators (such as in the case of cellular networks) and, thus, terminals may not abide by the protocol rules in order to gain unfair access to the network (selfish misbehavior), or simply to disturb the network operations (denial-of-service attack). This paper presents a robust nonparametric detection mechanism for the CSMA/CA media-access control layer denial- of-service attacks that does not require any modification to the existing protocols. This technique, based on the –truncated sequential Kolmogorov–Smirnov statistics, monitors the successful transmissions and the collisions of the terminals in the network, and determines how "explainable" the collisions are given for such observations. We show that the distribution of the explain ability of the collisions is very sensitive to changes in the network, even with a changing number of competing terminals, making it an excellent candidate to serve as a jamming attack indicator. Ns-2 simulation results show that the proposed method has a very short detection latency and high detection accuracy.

4. Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks (2007).

Description:

We consider a scenario where a sophisticated jammer jams an area in a single-channel wireless sensor network. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region. The jammer is detected at a monitor node by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network computes channel access probability in an effort to minimize the jamming detection plus notification time. In order for the jammer to optimize its benefit, it needs to know the network channel access probability and number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. We study the idealized case of perfect knowledge by both the jammer and the network about the strategy of one another, and the case where the jammer or the network lacks this knowledge. The latter is captured by formulating and solving optimization problems, the solutions of which constitute best responses of the attacker or the network to the worst-case strategy of each other. We also take into account potential energy constraints of the jammer and the network. We extend the problem to the case of multiple observers and adaptable jamming transmission range and propose a intuitive heuristic jamming strategy for that case.

Existing System

Recently, use of timing channels has been proposed in the wireless domain to support low rate, energy efficient communications as well as covert and resilient communications.

In existing system methodologies to detect jamming attacks are illustrated; it is also shown that it is possible to identify which kind of jamming attack is on-going by looking at the signal strength and other relevant network parameters, such as bit and packet errors.
Several solutions against reactive jamming have been proposed that exploit different techniques, such as frequency hopping, power control and unjammed bits.

Proposed System

1. We develop a gambling based model to derive the message invalidation ratio of the time-critical application under jamming attacks.
2. We set up real-time experiments to validate our analysis and further evaluate the impact of jamming attacks on an experimental power substation network. Based on our theoretical and experimental results.
3. We design and implement the JADE system (Jamming Attack Detection based on Estimation) to achieve efficient and reliable jamming detection for power networks.

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

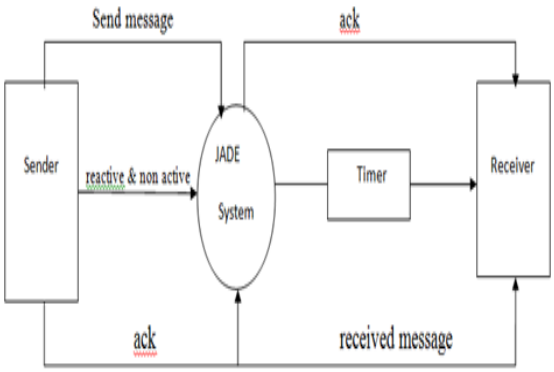
The idea matrix is as follows :

IDEA MATRIX

I	D	E	A
INCREASE : effectiveness and efficiency for secure data encoding and data decoding.	**DRIVE:** How to detect attacks in wsn	**EDUCATE :** identify the challenges of secure data transmission in sensor networks	**ACCELERATE :** low energy and bandwidth consumption, efficient storage and secure transmission.
IMPROVE: High data trustworthiness of sensor data.	**DELIVER:** Efficient techniques for data decoding and verification at the base station.	**EVALUATE :** Incorporate data binding	**ASSOCIATE:** Only authorized parties i.e. BS can process and check integrity for data
IGNORE : packet forgery attacks	**DECREASE :** Packet loss attacks.	**ELIMINATE :** Unauthorized parties to check integrity for data.	**AVOID :** Delivery of false packet, packet loss

IV. PROPOSED WORK

System Architecture:



The sender sends a message to JADE (Jamming Attack Detection based on Estimation) system and get an acknowledge to system. The timer can give a maximum time otherwise it will turn off. The receiver receives the message and it gives back to an acknowledgment. JADE (Jamming Attack Detection based on Estimation) test can also perform for detect the maximum times of jamming

V. ALGORITHM AND MATHEMATICAL MODEL

Algorithm:

1. Protocol we used (wire-less).
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.
2. Algorithms are used to count jamming ratio.
We use the message invalidation ratio to measure the jamming impact.
3. Algorithm for detecting jamming point
Jamming Attack Detection based on Estimation (JADE) scheme for robust jamming detection.
4. Algorithm is used to solve the jamming

```
do
   While (PolicyEndureTime)
          do
             While (CommunicationPeriod)

                 Nodes Communicate;
              end while

            GetPDR();
           DetermineNodeState();
           UpdateTransmitionProbabilities()
            ChooseStrategy(Policy, State);
            SendNotification();

     end while;
        DeterminePolicy();
end;
```

5. Details, Description and working of JADE method.

It is very importance to detect the jamming attacks in power networks. The system should yield a reliable output within a short decision time to notify network operators of potential threats.

Description (intuition) of JADE is as follows:

First, the online profiling based methods are used in adhoc 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.

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, by 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 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 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.

Working/Implementation:

We implement the JADE system at a MUIED that periodically transmits raw data samples at the rate of 920Hz. JADE observes the transmission result of each data sample and estimates the jamming probability p` by

$$P` = \frac{1}{N}\sum_{i=1}^{N} 1_{F_i}$$

Where N is the number of observations jamming attacks in the network, and Fi denotes the event that the i-th transmission fails.

After the estimation in, the JADE raises a jamming alarm if p` > p∗.

The following algorithm shows the design of JADE of single observation of jamming in network:

Input: Threshold p∗, Number of needed samples N.

Initialization: n ← 0, p` ← 0.

repeat

Transmit a packet and n ← n + 1.

if transmission failure

p` ← ((n − 1) ∗p` + 1)/n

else

p` ← (n − 1) ∗p`/n

end

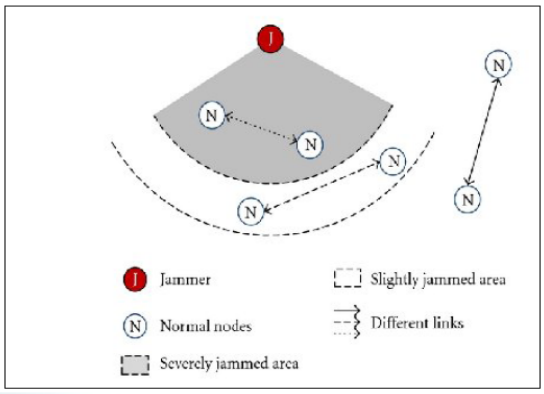
if until n is equal to N

If `p > p∗, displays Jamming Alarm/message.

The threshold p∗ can be chosen via offline profiling i.e. via either theoretical analysis or experiments.

We assume 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.

Reference Diagram shows the jamming scenario:



VI .CONCLUSION

In this paper, we provided an in-depth study on the impact of jamming attacks against time-critical smart grid applications by theoretical modelling 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.

FUTURE ENHANCEMENTS

Therefore in this paper, we aim to delivery data on message securely in wireless application by avoiding the attacker which attack the data while in transmit. In Broadcast communication, it is vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions i.e. attack takes place. The open nature of

the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

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 IEC61850 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 IEEE802.11 wireless communication system for smart grid," in Proc.IEEE Smart Grid Comm, 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 Standard61850, 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 Mobi Hoc, 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. Bayraktarogluet al., "On the performance of IEEE 802.11 under jamming," 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, "Jamming resistant 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 uncoordinatedFHSS anti-jamming communication," in Proc. ACM MobiHoc, NewOrleans, LA, USA, 2009.

[15] J. T. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wirelessbroadcast networks," in Proc. IEEE INFOCOM, Phoenix, AZ,USA, Apr. 2008.

[16] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channelhopping to increase 802.11 resilience to jamming attacks," inProc. IEEE INFOCOM, May 2007, pp. 2526–2530.

[17] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differentialDSSS: Jamming-resistant wireless broadcast communication," inProc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010.

[18] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcastcommunication without shared keys," in Proc. USENIXSecurity, Berkeley, CA, USA, Aug. 2009.

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

[20] A. Shevtekar and N. Ansari, "Do low rate dos attacks affect QoSsensitive VoIP traffic?" in Proc. IEEE ICC, Istanbul, Turkey, Jun.2006.

[21] E. Casini, A. van der Zanden, R. Goode, and R. Berto-Monleon,"IP QoS with military precedence level for the NATO informationinfrastructure," in Proc. IEEE MILCOM, Baltimore, MD, USA,Nov. 2011.

[22] F. Cleveland, "Uses of wireless communications to enhance powersystem reliability," in Proc. IEEE PES General Meeting, Tampa, FL,USA, Jun. 2007.

[23] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributedcoordination function in nonsaturated heterogeneousconditions," IEEE Trans. Netw., vol. 15, no. 1, pp. 159–172, Feb.2007.

[24] W. David, Probability with Martingales. Cambridge, U.K.:Cambridge University, 1991.

[25] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial ofservice attacks on ad hoc networks," IEEE Trans. Netw., 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-criticaltraffic," in Proc. IEEE INFOCOM, Shanghai, China, Apr. 2011.

[27] S. Emrich, "Dispelling the myths associated with spread spectrumradio technology in electric power SCADA networks," in Proc.IEEE PES General Meeting, Shanghai, China, Jun. 2007.

[28] H. J. Zhou, C. X. Guo, and J. Qin, "Efficient application of GPRSand CDMA networks in SCADA system," in Proc. IEEE PESGeneral Meeting, Minneapolis, MN, USA, Jul. 2010.

[29] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactivejamming in wireless networks: How realistic is the threat?" inProc. ACM WiSec, Hamburg, Germany, 2011