Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Jammer Detection System

Swati Baban Kobal, Sucheta Rajendra More, Shraddha Tanaji Kumbhar, Jyoti Shravan Sonawne
Prof. Anuja Zade
anujazade@gmail.com
Jspm's Rajashri Shahu Collage of Engineering,Tathwade,Pune.
kobal.swati@gmail.com, shraddhakumbhar094@gmail.com, sonawane.jyoti26@gmail.com, more.sucheta29@gmail.com

***Abstract* --** Time-critical wireless applications in rising network devices, like e-healthcare and sensible grids, have recently been drawing increasing attention in each trade and establishment. the published nature of wireless channels inevitably reveals such applications to taking part in attacks. however existing methods to characterize and find out jam attacks can't be used on to time-critical systems, whose communication traffic unit differs from standard versions. Here, we tend to aim modeling and finding jam attacks against time-critical traffic. we tend to introduce a brand new metric, message dissolution magnitude relation, to quantify the performance of time-critical applications. A key insight that causes our modeling is sometimes that the behavior of a transmitter United Nations agency efforts to disrupt the delivery of a time-critical conception are often specifically planned to the behavior of a gambler United Nations agency looks to win a recreation game. we tend to show through the gambling-based modeling and time period experiments that presently there on the entire exists a stage transition development for a time-critical application beneath taking part in attacks: because the chance that packet is crammed will increase from zero to one, the message dissolution magnitude relation initial will increase somewhat (even negligibly), then raises significantly to a minimum of one. supported artificial and experimental results, all folks additional style and apply the JADE (Jamming Assault Detection counting on Estimation) program to realize economical and sturdy jam detection meant for time-critical wireless networks.

Keywords: JADE (Jamming Attack Diagnosis based on Estimation), LLR (Likelihood ratio), Performance modeling, wireless network, time-critical messages, jamming attack detection, good grid applications.

I. INTRODUCTION

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.

II. RELATED WORK

1. Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution(2009).
Authors: Ali Hamieh, Jalel Ben-Othman.
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).
Authors: Christina P¨opper, ETH Zurich Mario Strasser, Srdjan Cˇ apkun.
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. Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping (2008).
Authors: Mario Strasser, Christina P¨opper, Srdjan Cˇ apkun, Mario Cˇ agalj
Description: We consider the following problem: how can two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of a communication jammer? An inherent challenge in solving this problem is that known anti-jamming techniques (e.g., frequency hopping or direct-sequence spread spectrum) which should support device communication during the key establishment require that the devices share a secret spreading

key (or code) prior to the start of their communication. This requirement creates a circular dependency between anti jamming spread-spectrum communication and key establishment, which has so far not been addressed. In this work, we propose an Uncoordinated Frequency Hopping (UFH) scheme that breaks this dependency and enables key establishment in the presence of a communication jammer. We perform a detailed analysis of our UFH scheme and how its feasibility, both in terms of execution time and resource requirements.

4. Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks (2008).
Authors: Alberto Lopez Toled and Xiaodong Wang.
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.

5. Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks (2007).
Authors: Mingyan Li, Radha Poovendran
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 lack 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.

III. SURVEY of PROPOSED SYSTEM

This paper We develop a gambling based model to derive the message invalidation ratio of the time-critical application under jamming attacks. 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, we design and implement the JADE system (Jamming Attack Detection based on Estimation) to achieve efficient and reliable jamming detection for power networks.

Advantageous Of Proposed System:

1. JADE system achieves efficient and robust jamming detection for power networks.
2. JADE system is reliable.
3. It is more appropriate than conventional performance metrics for time-critical applications.
4. JADE is more robust than the LLR (Likelihood ratio) test in the presence of a sophisticated time varying jammer.

IV. MATHEMATICAL MODEL

Let W be the whole system which consists:

W = {input, process, output}.

Input: {p, N, F, i}.

Where,

1. p probability of jamming.
2. N is number of samples taken for estimation.
3. F is the frequency of number of jamming events.

Process:

We implement the JADE system 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∗.

V. ENHANCED PROPOSED ALGORITHM

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

```
Initialization: $n \leftarrow 0, p` \leftarrow 0$.
repeat
    Transmit a packet and $n \leftarrow n + 1$.
    if transmission failure then
        $p` \leftarrow ((n - 1) * p` + 1)/n$
    else
        $p` \leftarrow (n - 1) * p`/n$
    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.

AES ALGORITHM

AES is an iterated symmetric block cipher, which means that:

- AES works by repeating the same defined steps multiple times.
- AES is a secret key encryption algorithm.
- AES operates on a fixed number of bytes

AES as well as most encryption algorithms is reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement and explain.

This key is expanded into individual sub keys, a sub keys for each operation round. This process is called KEY EXPANSION, which is described at the end of this document.

As mentioned before AES is an iterated block cipher. All that means is that the same operations are performed many times on a fixed number of bytes. These operations can easily be broken down to the following functions:

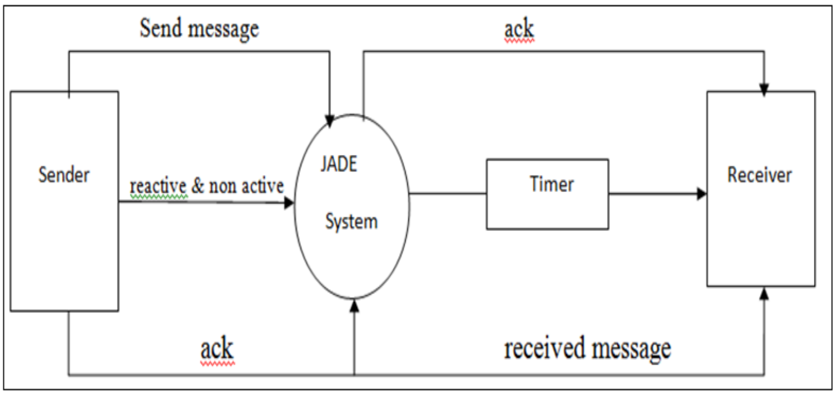
ADD ROUND KEY
BYTE SUB
SHIFT ROW
MIX COLUMN

An iteration of the above steps is called a round. The amount of rounds of the algorithm depends on the key size.

Key Size (bytes)	Block Size (bytes)	Rounds
16	16	10
24	16	12
32	16	14

The only exception being that in the last round the **Mix Column** step is not performed, to make the algorithm reversible during decryption.

VI. SYSTEM ARCHITECTURE



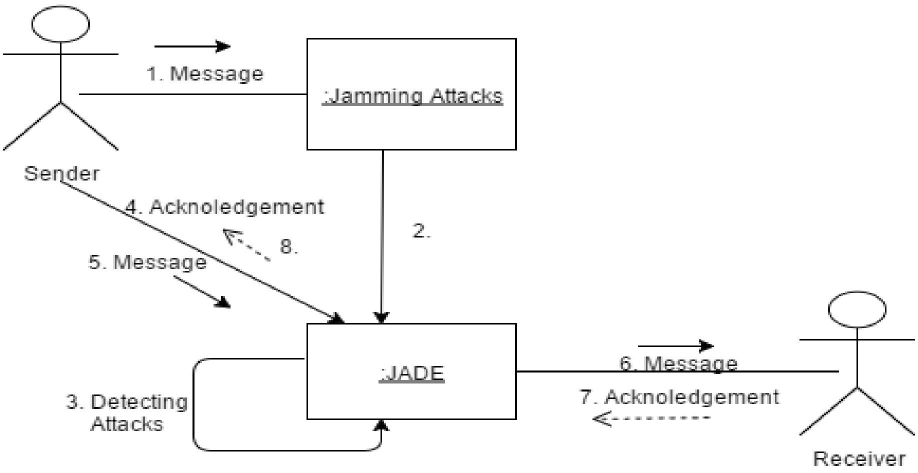
1. First, the online profiling based methods are used in adhoc or sensor networks where network parameters for a node (e.g., number of nodes, background traffic) are usually considered unknown.
   Therefore, online profiling is essential for jamming detection to accommodate changes of network setups and topologies.

2. 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.

3. 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.

4. 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.

SYSTEM FLOW:



VII. RESULT ANALYSIS

A. *Input:*

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system based on this atributes we getting following result for our proposed JADE system against LLR test and GOOSE system.

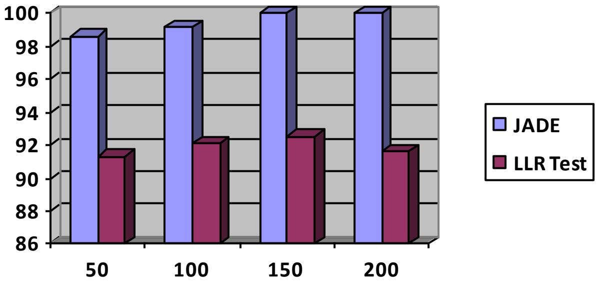
B. *Expected Result:*-

In the Existing system we used JADE method while in the proposed system we used LLR method.
LLR method gives better performance than the Existing system Existing system not support more than 100 samples while Proposed system gives support to more samples packet.

Reactive Jamming:
We first consider the detection performance of JADE on reactive jamming. 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.

Samples	JADE	LLR Test
50	98.6	91.3
100	99.1	92.1
150	100	92.5
200	100	91.6

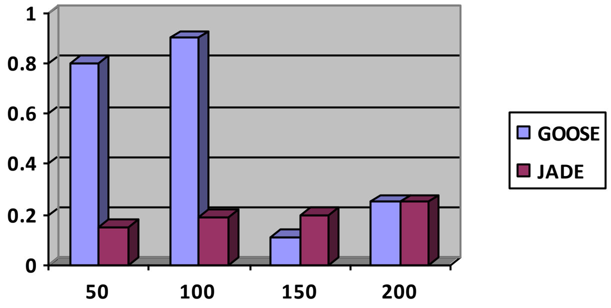
Table1. Reactive jamming of JADE & LLR Test



Non Reactive Jamming
In the Existing system we used GOOSE method while in the proposed system we used JADE method.
JADE method gives better performance than the Existing system Existing system not support more than 100 samples while Proposed system gives support to more samples packet.
The impact of a periodic jammer on GOOSE messages transmitted for the periodic jammer, increasing unsaturated traffic load also has negligible effect on the message invalidation ratio.

Samples	GOOSE	JADE
50	0.8	0.15
100	0.9	0.19
150	0.11	0.20
200	0.25	0.25

Table2. Non Reactive jamming of JADE & GOOSE Test



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 modelling and real-time experiments.

CONCLUSION AND FUTURE WORK

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.

We aim to delivery data or message securely in wireless application by avoiding the attacker which attack the data while in transmit. In Broadcast communications ,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 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 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, “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.

AUTHORS

Swati Baban Kobal, Pursuing B.E. in Department Of Information Technology, Jspm's Rajashri Shahu Collage of Engineering,Tathwade,Pune.

Sucheta Rajendra More, Pursuing B.E. in Department Of Information Technology, Jspm's Rajashri Shahu Collage of Engineering,Tathwade,Pune.

Shraddha Tanaji Kumbhar, Pursuing B.E. in Department Of Information Technology, Jspm's Rajashri Shahu Collage of Engineering,Tathwade,Pune.

Jyoti Shravan Sonawane, Pursuing B.E. in Department Of Information Technology, Jspm's Rajashri Shahu Collage of Engineering,Tathwade,Pune.