International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time Critical Traffic

P. Sudha[1], K. Durairaj[2]

[1]MCA (final year), Veltech Technical University

[2]Assistant Professor MCA/IT Veltech Technical University

Abstract: ***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 modeling 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 modeling is that the behavior of a jammer who attempts to disrupt the delivery of a time-critical message can be exactly mapped to the behavior of a gambler who tends to win a gambling game. We show via the gambling-based modeling 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 to 1. 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.***

Keywords: Time critical, emerging network-healthcare and smart grids, gambling based modeling jamming attacks, wireless network.

1. Introduction

The main advancement of today's wireless technologies (e.g., 3G/4G and Wi-Fi) 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 . The 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 equipment's.

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 . 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. (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.

2. Motivation

In this paper we develop a complete system to detect network attacks without any kind of signatures or previous knowledge of context traffic.

Licensed Under Creative Commons Attribution CC BY

We show how to use the information provided by the multi clustering approach to characterize an identified group of malicious flows, automatically producing easy-to-interpret signatures of the attack.

These signatures provide useful information on the nature of the attack, and can be directly exported to any security device to easily detect its occurrence in the future.

We evaluate the detection and characterization performance of the system in real traffic captured in two operational networks: the backbone network of the Japanese WIDE project and the French RENATER research network.

Moreover, we compare the approach against previously proposed methods Easy to interpret signature of attacks complete system find a network attacks Detection and characterization of system.At last we develop a gambling-based model to derive the message invalidation ratio of the time-critical application under jamming attacks.

Moreover, we compare the approach against previously proposed methods Easy to interpret signature of attacks complete system find a network attacks Detection and characterization of system.At last 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.

3. Problem Definition

In this paper, we introduce models for time-critical applications and jamming attacks, then define a metric, message Invalidation ratio for later analysis. It is very easily to use any device to handle it. The LLR test can easily send information perfectly. We have to develop a system network attacks .It is a group of malicious flow.

4. Architecture Diagram

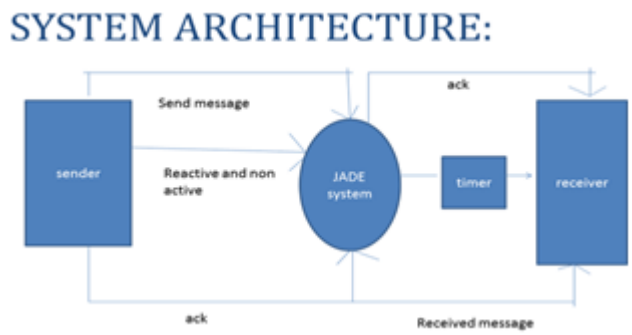


Figure 1: System Architecture

The sender sends a message to jade system and get a acknowledge to system. The timer can give a maximum time otherwise it will turn off. The receiver receive the message and it gives back to a acknowledgment. JADE test can also perform for detect rhe maximum times of jamming. The LLR test can send a information perfectly.

Table 1:

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 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 [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 above Table, 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 [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 than1000 ms.

The sender sends a message to jade system and get a acknowledge to system. The timer can give a maximum time otherwise it will turn off. The receiver receive the message and it gives back to a acknowledgment. JADE test can also perform for detect rhe maximum times of jamming. The LLR test can send a information perfectly.

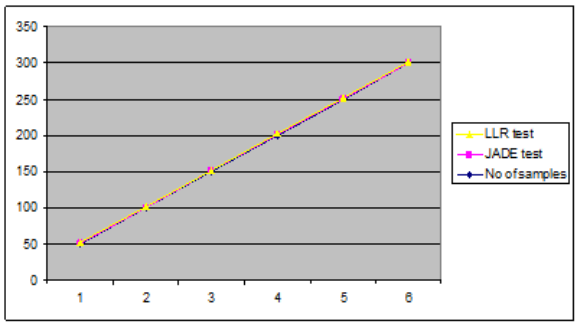
5. Experimental Results

Table 2:

No f Samples	JADE test	LLR test
50	97.60%	91.30%
100	98.10%	92.10%
150	99%	92.50%
200	100%	91.60%
250	100%	95.50%
300	100%	96.50%

Detection Ratios of both JADE and Likelihood Ratio Test in the Presence of a Time-Varying Jammers

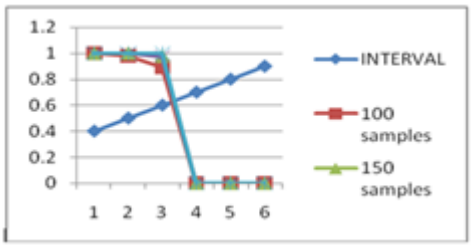
Licensed Under Creative Commons Attribution CC BY



Jamming probability

Figure 2: Jamming Detection Ratios of JADE for Periodic Jamming with Different Jamming Intervals

INTERVA	0.4	0.5	0.6	0.7	0.8	0.9
100	100.00	98.00%	89%	0	0	0
150	100.00	100.00	97.60	0	0	0
200	100%	100.00	97.40	0	0	0
250	100%	100.00	100%	0	0	0



Jamming Probability

Figure 3: Different interval given different experimental results

Innovative Content

- How such a robust unsupervised detection approach may work in practice, we develop a complete system to detect network attacks without any kind of signatures or previous knowledge of context traffic.
- We show how to use the information provided by the multiclustering approach to characterize an identified group of malicious flows, automatically producing easy-to-interpret signatures of the attack.
- These signatures provide useful information on the nature of the attack, and can be directly exported to any security device to easily detect its occurrence in the future.
- We evaluate the detection and characterization performance of the system in real traffic captured in two operational networks: the backbone network of the Japanese WIDE project and the French RENATER research network.
- Moreover, we compare the approach against previously proposed methods

6. Justifications of 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 Jr(p) and Jnr(I), respectively.

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 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.

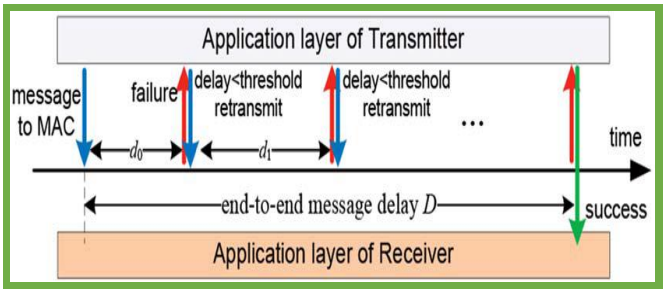


Figure 4: transmission process of time critical message

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.

7. 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.,

Licensed Under Creative Commons Attribution CC BY

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 IEE 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,"vin *Proc. ACM MobiHoc*, Urbana-Champaign, IL, USA,v2005, pp. 46–57.

[9] L. Sang and A. Arora, "Capabilities of low-power wireless jammers,"vin *Proc. IEEE INFOCOM Mini-Conf.*, Rio de Janeiro, Brazil,vApr. 2009.

[10] E. Bayraktaroglu *et al*., "On the performance of IEEE 802.11 undervjamming," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008,vpp. 1265–1273.

[11] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jammingvattacks and network defense policies in wireless sensorvnetworks," in *Proc. IEEE INFOCOM*, May 2007, pp. 1307–1315.

[12] A. L. Toledo and X. Wang, "Robust detection of MAC layervdenial-of-service attacks in CSMA/CA wireless networks,"v*IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 347–358, Sep. 2008.

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

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

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

Licensed Under Creative Commons Attribution CC BY