ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Jamming Detection System in Time-Critical Wireless Applications

Sheetal .S.Shete[1], Dr.A.M.Dixit[2]

[1]M.E Student, Department of Computer Engineering, PVPIT, Pune University, India

[2]Professor, Department of Computer Engineering, PVPIT, Pune University, Maharashtra, India

ABSTRACT: Advancement of today's wireless technologies (e.g3G/4G and WiFi) has already brought significant change and benefit to people's life, such as ubiquitous wireless Internet access, mobile messaging and gaming has been drawing increasing attention in that it has broad applications for real time message delivery among electronic devices on physical infrastructures. Over-due message delivery may lead to instability of system operations, and even cascading failures and unavoidably exposes the messages in transit to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipments. In this paper, we proposed to representing and detecting jamming attacks against time-critical wireless networks. In contrast to communication networks where packets-oriented metrics, such as packet loss and throughput are used to measure the network performance, we introduce a new metric, message invalidation ratio, to quantify the performance of time-critical applications which is being evaluated at the jamming path. Analytical results for a time-critical application under both reactive and non-reactive jamming attacks are derived with respect to path selection for sending the data. That is, as the probability that a packet is jammed increases from 0 to 1, the message invalidation ratio first increases slightly, then increases dramatically to 1. Jamming Attack Detection based on Estimation (JADE) scheme achieves robust jamming detection.

KEYWORDS:Wireless communication network, time-critical messaging, classification of jammers, jamming attack detection, smart grid applications.

I. INTRODUCTION

Developing time-critical wireless systems, for example wireless e-medicinal services and wireless power networks, gives a new paradigm of modern wireless networks,[1] whose essential objective is efficient and reliable message delivery for checking and control purposes, rather than providing data services for clients. Thus, a large amount of communication traffic is time-critical in such networks.

For instance, data messages in power substations are required to be conveyed with particular latency constraints, ranging from 3 milliseconds (ms) to 1 second. Because of their importance to human beings e.g. e-medicinal services 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 definitely exposes wireless networks to jamming attacks that might extremely corrupt the performance of these time-critical networks. Although great advancement has been made towards jamming characterization and countermeasure for conventional networks, little consideration has been focused on time-critical wireless networks.

In fact, time-critical networks pose challenging issues to existing research on jamming attacks. In conventional networks, the jamming effect 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. [1]

Consequently, conventional performance metrics cannot be promptly adapted to measure the jamming impact on time-critical applications. Further, absence 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 accomplish productive jamming detection since locators are not ready to accurately identify jamming attacks, which can cause potentially severe performance degradation of time critical applications.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II. RELATED WORK

1. Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications. (2014).
Authors: Z. Lu, W. Wang, and C. Wang
Description:
This paper aims at modeling and detection of jamming attacks against time-critical wireless applications to the smart grid. A new metric, message invalidation ratio is introduced to quantify the performance of time-critical applications. There exists a phase transition phenomenon for successful time-critical message delivery under a variety of jamming attacks i.e as the probability that a packet is jammed increases from 0 to 1, the message invalidation ratio increases slightly and then dramatically to 1. JADE (Jamming Attack Detection Based on Estimation) system is used to achieve efficient and robust jamming detection.

2. On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming [7].
This displays the algorithms that determine optimal jamming techniques against RAAs for a given jamming budget, and experimentally demonstrated that efficiency of these smart jamming attacks, which can be requests of magnitude more efficient than naive jamming. The function of the RAA is to empower WLAN users to adaptively pick the best transmitting rate according to current wireless link conditions in order to achieve the maximum throughput possible. The performance of the RAA's for attacks is not accurate. Likewise energy utilization is high.

3. Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks [2]
The paper gives the study about controllable jamming attacks in wireless sensor networks, which are easy to launch and difficult to recognize and confront. The derived solutions for the improvement issues dictate optimal attack and network defense strategies. To discover alternatives for modeling lack of knowledge for the attacker and the network is difficult in real time situation.

4. Jamming-resistant Key Establishment utilizing Uncoordinated Frequency Hopping [5]
The paper elaborates the issue of how two devices that do not share any secrets can establish a shared secret key over a wireless radio channel in the presence of a communication jammer . To implement such type of proposed system is difficult because of configuration issues. If in case such system is implemented then it won't give give proper appropriate solution.

5. User's Deception Mechanisms against Jammers in Wireless Energy Harvesting Networks.
Deception mechanism is used by performing the blank transmission which makes the jammers into ineffective attacks by wasting their energy.

III. ENHANCED PROPOSED SYSTEM

In this system, the packet is send from one node (sender) to another node(receiver) and depending on the node structure the path is being automatically selected with the estimated time for both the secure path as well as the jamming path.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

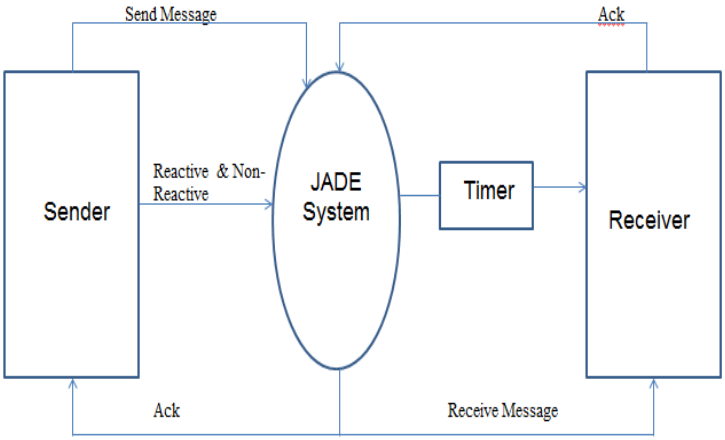

Fig.1 System Architecture.

1. Nodes in a power network are generally static and have nearly predictable traffic (e.g., the raw data sampling rate and meter update rate of IEDs). So, on-line profiling is redundant, [4] 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.

2. The objective of both reactive and non-reactive jammers is to disrupt the message conveyance by jamming packets. Thus, for any jammer, regardless of its jamming behavior, there always exists a jamming-induced probability, denoting the probability that a packet will be disrupted by jamming.

IV. ENHANCED PROPOSED ALGORITHM

Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y.

- Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.
- Set the initial node as current. Mark all other nodes unvisited. Create a set of all the unvisited nodes called the unvisited set.
- For the current node, consider all of its unvisited neighbors and calculate their tentative distances. Compare the newly calculated tentative distance to the current assigned value and assign the smaller one
- When we are done considering all of the neighbors of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.
- If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal; occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.
- Otherwise, select the unvisited node that is marked with the smallest tentative distance, set it as the new "current node", and go back to step 3.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

V. 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 = number of samples taken for estimation.
3. F = the frequency of number of jamming events.
4. i = Time interval

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

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∗.

VI. IMPLEMENTATION OF PROPOSED SYSTEM

Jamming system is being implemented with off-line profiling i.e the node structure is defined with dynamic time.

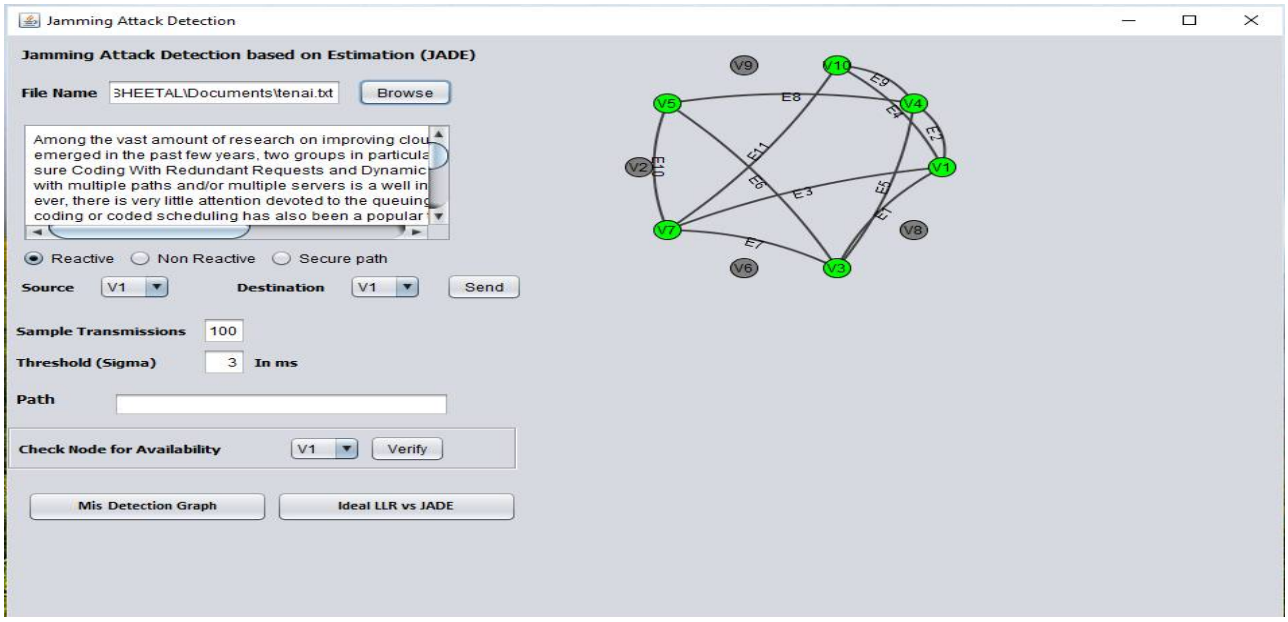

Fig 2: Jamming Detection System

The node structure is defined with 10 nodes out of which 6 nodes are in connected mode as active nodes and all other nodes are inactive mode. If inactive nodes are selected then it displays the selected node is in DoS attack. Availability of nodes are chekedby the function of the 'Check node for Availability'. If the secure path is selected with source and destination then it displays the valid path and also with the estimated time required to send to the destination with all intermediate nodes and which is the shortest path. And in case of Jamming attack i.e reactive or non-reactive with valid path it calculates the jamming probability for both and also the message invalidation ratio.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

VII. SIMULATION RESULTS

- **Reactive Jamming Attack**

In Reactive Jamming Attack, the uploaded message is transmitted with respect to sample transmission and threshold value. The jamming probability is calculated for each transmission and plots message invalidation ratio.

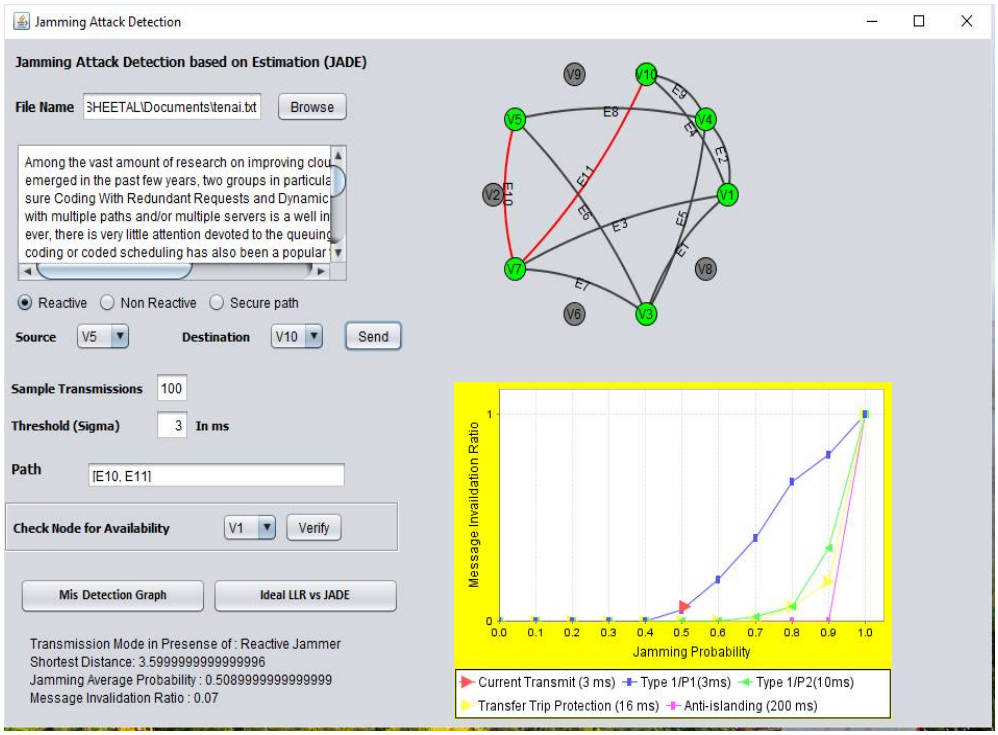

Fig 3 : Reactive Jamming Attack.

- **Non- Reactive Jamming Attack**

In Non- Reactive Jamming Attack, the uploaded message is transmitted with respect to sample transmission and threshold value. The jamming interval is calculated for each transmission and plots message invalidation ratio.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

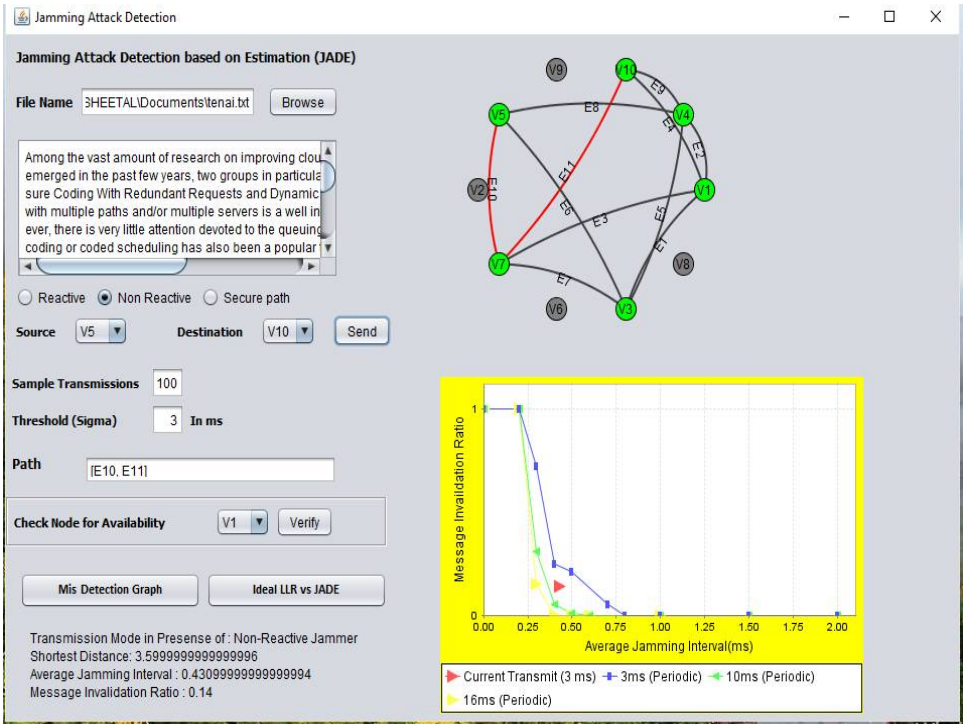

Fig 4 : Non-Reactive Jamming Attack.

VIII. ADVANTAGES& ITS APPLICATIONS

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. High packet successfully delivered rate using time slots.
5. Security of packets
6. Avoid packet delay rate.
7. Using less number of channels in wireless network.
8. New Metric used to measure.

APPLICATION

1. The algorithm is selecting the best anti-jamming strategy for a sensor network, in which different sensor nodes may experience different degrees of jamming attacks.
2. It is an approach for combining the strength of several jamming countermeasures and allows a sensor node to adopt the best anti-jamming technique.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IX. CONCLUSION

In this paper, the effect of jamming attacks against time-critical smart grid is derived by system tests. A metric, message invalidation ratio is to measure the effect of jamming attacks demonstrated through analytical analysis that there exist phase transition phenomena i.e from 0 to 1 in time-critical applications under a variety of jamming attacks. Based on our examination and tests, the JADE system is to accomplish proficient and strong jamming detection for power networks.

REFERENCES

1. Z. Lu, W. Wang, and C. Wang, " Modelling,Evaluation and detection of jamming attacks in time-critical wireless applications," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2014.
2. 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.
3. H. J. Zhou, C. X. Guo, and J. Qin, "Efficient application of GPRS and CDMA networks in SCADA system," in *Proc. IEEE PES General Meeting*, Minneapolis, MN, USA, Jul. 2010.
4. M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. ACM WiSec*, Hamburg, Germany, 2011.
5. M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hop-ping," in Proc. IEEE Symp. Security and Privacy, Washington, DC, USA, May 2008, pp. 64–78.
6. A. Cassola, T. Jin, G. Noubir, and B. Thapa, "Efficient spread spectrum communication without preshared secrets," *IEEE Trans. Mobile Comput.*, vol. 12, no. 8, pp. 1669–1680, Aug. 2013.
7. G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming," in *Proc. ACM WiSec*, Hamburg, Germany, 2011.
8. Basel Alomair and RadhaPoovendran "Efficient Authentication for Mobile and Pervasive Computing"*IEEETranctions on mobile computing, vol.13,NO.3,MARCH2014.*
9. 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.
10. 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.
11. L. Sang and A. Arora, "Capabilities of low-power wireless jammers," in *Proc. IEEE INFOCOM Mini-Conf., Rio de Janeiro, Brazil*, Apr. 2009.
12. D.Niyato ,P.Wang , Dong In Kim , Z. Han and Joseph Chee Ming. "User's Deception Mechanisms against Jammers in Wireless Energy Harvesting Networks, " in IEEE ICC 2015 , *pp.6767 - 6772.*