A Survey on Detection of Jamming Attacks in Time-Critical Wireless Applications

Sheetal S Shete[1], N. D. Kale[2]

[1]Department of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

[2]HOD and Professor, Department of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

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 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: Performance modelling, wireless network, time-critical messaging, jamming attack detection, smart grid applications.

1. 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. Therefore, towards time-critical wireless applications, a fundamental question remains unsolved: How to model, analyze, and detect jamming attacks against time critical traffic?

2. Types of Jammers

Jamming nodes are classified depending on the different characteristics these nodes posses.

Reactive Jammer

This type of jammer is quiet until the medium is idle and when it senses transmission on the medium it starts injecting false data which avoids the legitimate user to send data. These types of jammer are difficult to detect.

Non-reactive Jammer

This type of jammer is not aware of any behaviour of legitimate nodes and transmit the radio interference over the wireless channel following their own jamming strategies like continually emits a radio signal or continuously sends regular packets on the channel without any gap between the packets.

3. Literature Survey

3.1 Efficient Application of GPRS and CDMA networks in SCADA System.[1]

This paper presents a communication system using GPRS and CDMA wireless communication networks in SCADA(Supervisory Control And Data Acquisition) system.

Additional security management, dual network online synchronously, packet assembly disassembly and other new functions is the fundamental solution.The SCADA system used for reliability and the overloading of the bandwidth has to be improved.

3.2 On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming [2].

This presents the algorithms that determine optimal jamming strategies against RAAs for a given jamming budget, and experimentally shown that efficiency of these smart jamming attacks, which can be orders of magnitude more efficient than naive jamming. The function of the RAA is to enable WLAN users to adaptively choose the best transmitting rate according to current wireless link conditions in order to achieve the maximum thoughtput possible.

3.3 From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time-Critical Traffic.[3]

The paper aims at modeling and detecting jamming attacks against time-critical traffic. Author introduced a new metric, message invalidation ratio to quantify the performance of time-critical applications. A key insight that leads to 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.

3.4 Efficient Spread Spectrum Communication without Preshared Secrets.[4]

We introduce an efficient and adversary-resilient secret sharing mechanism based on two novel paradigms i.e. intractable forward decoding and efficient backward decoding called Time Reversed Message Extraction and Key Scheduling (TREKS) that enables SS(Spread Spectrum) communication without preshared secrets.

4. Existing System

The existing data services are based on packet-switched networks. So, 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, 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. For example, 100% packet delivery ratio does not necessarily mean that all messages can be delivered on time to ensure reliable operations in a cyber-physical system.

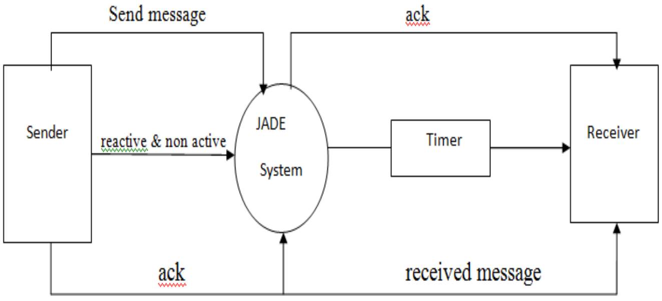
5. Drawbacks

1) Conventional performance metrics cannot be readily adapted to measure the jamming impact against time-critical messages.
2) It is not efficient and robust jamming detection technique for power networks.
3) Increases the detection time.

6. Related Work

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.

7. System Architecture



8. Advantages

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.

9. Conclusion

In this paper, we discussed the various techniques that can be used to avoid the data loss and also to protect it till it reaches its destination securely. Under the survey, the SCADA system provides feasibility and benefits through the pilot projects and the other system that provides the optimal jamming strategies that exploit the weakness found in IEEE 802.11 MAC and RAAs. Based on the analysis, we implemented a JADE system at the application layer to achieve efficient and robust jamming detection for power networks like smart grid applications.

References

[1] H. J. Zhou, C. X. Guo, and J. Qin, “Efficient application of GPRS and CDMA networks in SCADA system,” in *Proc. IEEE PESGeneral Meeting*, Minneapolis, MN, USA, Jul. 2010.

[2] 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.

[3] Z. Lu, W. Wang, and C. Wang, “From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic,” in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011.

[4] 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.

[5] S. Emrich, “Dispelling the myths associated with spread spectrum radio technology in electric power SCADA networks,” in *Proc.IEEE PES General Meeting*, Shanghai, China, Jun. 2007.

[6] 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.

[7] 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.