International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Defeating Jamming With the Power of Silence: A Game-Theoretic Analysis

Mr. P.Vijender

Mr.K.Raju,

ABSTRACT:

The timing channel is a logical communication channel in which information is encoded in the timing between events. Recently, the use of the timing channel has been proposed as a countermeasure to reactive jamming attacks performed by an energy- constrained malicious node. In fact, while a jammer is able to disrupt the information contained in the attacked packets, timing information cannot be jammed, and therefore, timing channels can be exploited to deliver information to the receiver even on a jammed channel. Since the nodes under attack and the jammer have conflicting interests, their interactions can be modeled by means of game theory. Accordingly, in this paper, a game-theoretic model of the interactions between nodes exploiting the timing channel to achieve resilience to jamming attacks and a jammer is derived and analyzed. More specifically, the Nash equilibrium is studied in terms of existence, uniqueness, and convergence under best response dynamics. Furthermore, the case in which the communication nodes set their strategy and the jammer reacts accordingly is modeled and analyzed as a Stackelberg game, by considering both perfect and imperfect knowledge of the jammer's utility function. Extensive numerical results are presented, showing the impact of network parameters on the system performance.

Index Terms—Anti-jamming, timing channel, game-theoretic

INTRODUCTION

A *timing channel* is a communication channel which exploits silence intervals between consecutive transmissions to encode information [1]. Recently, use of timing channels has been proposed in the wireless domain to support low rate, energy efficient communications [2], [3] as well as covert and resilient communications [4], [5]. Timing channels are more—although not totally [4]— immune from reactive jamming attacks. In fact, the interfering signal begins its disturbing action against the communication only after identifying an ongoing transmission, and thus after the timing information has been decoded by the

receiver. In [4], for example, a timing channel-based communication scheme has been proposed to counteract jamming by establishing a lowrate physical layer on top of the traditional physical/link layers using detection and timing of failed packet receptions at the receiver. In [5], instead, the energy cost of jamming the timing channel and the resulting trade-offs have been analyzed. In this paper we analyze the interactions between the jammer and the node whose transmissions are under attack, which we call *target node*. Specifically, we assume that the target node wants to maximize the amount of information that can be transmitted per unit of time by means of the timing channel,1 whereas, the jammer wants to minimize such amount of information while reducing the energy expenditure.2 As the target node and the jammer have conflicting interests, we develop a game theoretical framework that models their interactions. We investigate both the case in which these two adversaries play their strategies simultaneously, and the situation when the target node (the leader) anticipates the actions of the jammer (the follower).

RELATED WORK

Wireless networks are especially prone to several attacks due to the shared and broadcast nature of the wireless medium. One of the most critical attacks is *jamming* [6], [7]. Jamming attacks can partially or totally disrupt ongoing communications, and proper solutions have been proposed in various application scenarios [6], [9], [10]. *Continuous* jamming attacks can be really expensive for the jammer in terms of energy consumption as the transmission of jamming signals needs a significant, and constant, amount of power. To reduce energy consumption while achieving a high jamming effectiveness, *reactive* jamming is frequently used [5], [11]–[13]. In [12] and [13] the feasibility and detectability of jamming attacks in wireless networks are analyzed. In these papers above, methodologies to detect jamming attacks are illustrated; it is also shown that it is possible to identify which kind of jamming attack is ongoing by looking at the signal strength and other relevant network parameters, such as bit and packet errors. In [11] Wilhelm *et al.* investigate the feasibility of reactive jamming attacks by providing a real implementation of a reactive jammer in a software-defined radio environment where a reactive jammer prototype is implemented on a USRP2 platform and network users are implemented on MICAz motes. Authors show that reactive jamming attacks are

feasible and efficient, and that low reaction times can be achieved; then, they highlight The need to investigate proper countermeasures against reactive jamming attacks.

GAME MODEL

Let us consider the scenario where two wireless nodes, a transmitter and a receiver, want to communicate, while a malicious node aims at disrupting their communication. To this purpose, we assume that the malicious node executes a reactive jamming attack on the wireless channel. In the following we refer to the malicious node as the *jammer*, *J*, and the transmitting node under attack as the *target node*, *T*. The jammer senses the wireless channel continuously. Upon detecting a possible transmission activity performed by *T*, *J* starts emitting a jamming signal. As shown in Fig. 1, we denote as *TAJ* the duration of the time interval between the beginning of the packet transmission and the beginning of the jamming signal emission. The duration of the interference signal emission that jams the transmission of the *j*-th packet can be modeled as a continuous random variable, which we call *Yj* . To maximize the uncertainty on the value of *Yj* , we assume that it is exponentially distributed with mean value *y*. We assume that when no attack is performed the target node communicates with the receiver by applying traditional transmissions schemes; on the other hand, when it realizes to be under attack,

PROPOSED SYSTEM:

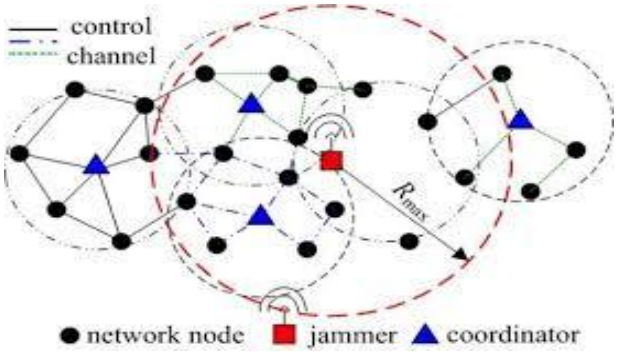
- In this paper we focus on the resilience of timing channels to jamming attacks. In general, these attacks can completely disrupt communications when the jammer continuously emits a high power disturbing signal, i.e., when *continuous jamming* is performed.
- In this paper we analyze the interactions between the jammer and the node whose transmissions are under attack, which we call *target node*. Specifically, we assume that the target node wants to maximize the amount of information that can be transmitted per unit of time by means of the timing channel, whereas, the jammer wants to minimize such amount of information while reducing the energy expenditure.
- As the target node and the jammer have conflicting interests, we develop a game theoretical framework that models their interactions. We investigate both the

case in which these two adversaries play their strategies simultaneously, and the situation when the target node (the leader) anticipates the actions of the jammer (the follower). To this purpose, we study both the Nash Equilibria (NEs) and Stackelberg Equilibria (SEs) of our proposed games.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ We model the interactions between a jammer and a target node as a jamming game
- ✓ We prove the existence, uniqueness and convergence to the Nash equilibrium (NE) under best response dynamics
- ✓ We prove the existence and uniqueness of the equilibrium of the Stackelberg game where the target node plays as a leader and the jammer reacts consequently
- ✓ We investigate in this latter Stackelberg scenario the impact on the achievable performance of *imperfect knowledge* of the jammer's utility function;
- ✓ We conduct an extensive numerical analysis which shows that our proposed models well capture the main factors behind the utilization of timing channels, thus representing a promising framework for the design and understanding of such systems.

SYSTEM ARCHITECTURE:



CONCLUSION

In this paper we have proposed a game-theoretic model of the interactions between a jammer and a communication node that exploits a timing channel to improve resilience to jamming attacks. Structural properties of the utility functions of the two players have been analyzed and exploited to prove the existence and uniqueness of the Nash Equilibrium. The convergence of the game to the Nash Equilibrium has been studied and proved by analyzing the best response dynamics. Furthermore, as the

reactive jammer is assumed to start transmitting its interference signal only after detecting activity of the node under attack, a Stackelberg game has been properly investigated, and proofs on the existence and uniqueness of the Stackelberg Equilibrium has been provided. Finally, the case of imperfect knowledge about the parameter *cT* has been also discussed. Numerical results, derived in several real network settings, show that our proposed models well capture the main factors behind the utilization of timing channels, thus representing a promising framework for the design and understanding of such systems.

REFERENCES

[1] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 4–18, Jan. 1996.

[2] G. Morabito, "Exploiting the timing channel to increase energy efficiency in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1711–1720, Sep. 2011.

[3] L. Galluccio, G. Morabito, and S. Palazzo, "TC-Aloha: A novel access scheme for wireless networks with transmit-only nodes," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 3696–3709, Aug. 2013.

[4] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proc. 1st ACMConf.Wireless Netw. Security*, 2008, pp. 203–213.

[5] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications," in *Proc. IEEE ICC*, 2013, pp. 4020–4024.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[7] R. Saranyadevi, M. Shobana, and D. Prabakar, "A survey on preventing jamming attacks in wireless communication," *Int. J. Comput. Appl.*, vol. 57, no. 23, pp. 1–3, Nov. 2012.

[8] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2004, ser. Artech House information warfare library. [Online]. Available: http://books.google.it/books?id=CZDXton6vaQC

[9] R.-T. Chinta, T. F. Wong, and J. M. Shea, "Energy-efficient jamming

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

attack in IEEE 802.11 MAC," in *Proc. IEEE MILCOM*, 2009, pp. 1–7.

[10] Y.W. Law, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energyefficient link-layer jamming attacks against wireless sensor networkMAC protocols," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw*

Author's Profile

Mr. K.Raju received M.Tech degree from Jayamukhi Institute of Technological Science,Narsampet, Warangal affiliated to JNTUH, Hydearabad. He is currently working as Assistant professor, Department of CSE, in Vinuthna Institute of Technology & Science ,Hasanparthy, Warangal, Telangana, India. Hisinterest includes Data Base Management Systems.

Mr. P.Vijender received B.Tech Degree fromVinuthna Institute of Technology & Science Hasanparthy, Warangal affiliated to KU, Warangal. He is currently pursuing M.Tech Degree in Software Engineering specialization in Vinuthna Institute of Technology & Science Hasanparthy, Warangal, Telangana, India.