A Game-theoretical Method of the Interactions Among the Nodes Violating the Timing Channel to Obtain Resilience to Jamming Attacks

[1]Penmatsa Naga Venkata Divya, [2]Dr. R.China Appala Naidu
[1]Dept. of Information Technology, St.Martins Engineering College, Hyderabad, Telangana, India
[2]Dept. of CSE, St.Martins Engineering College, Hyderabad, Telangana, India

Abstract
Reactive jamming attacks caused by an energy-controlled malicious node has been countermeasure by using the timing channel. In this channel the information is encoded in the timing between events, and it is a simple logical communication channel. The timing channel information or events can not be jammed, even if a jammer is able to disrupt the attacked packets information, and also delivers the timing information to the receiver on jammed communication channel. The game theory can be used to structure the interactions of attacked nodes and the jammer. This paper, propose a game theoretical method of the interactions among the nodes violating the timing channel to obtain resilience to jamming attacks and a jammer is derived and analyzed. Importantly, Nash equilibrium is discussed under best response changing aspects subjected to uniqueness, existence, and convergence. And also, by considering perfect and imperfect knowledge of the utility procedure of jammer's, jammer reactions on communication nodes setting strategies is modeled and analyzed and a Stackelberg game. Finally, this paper presents the numerical results and visualizes the impact of network parameters on the system performance.

Keywords
Nash Equilibrium , Game Theory, Jamming, Networks, Timing Channel, Communication Channel, Packets.

I. Introduction

The timing channel is a simple logical communication channel, to encode information exploit silence intervals between consecutive transmissions [3]. Timing channels are covert and resilient communication channels, and has been suggested in wireless domains in supporting low rate and energy efficient communications. But in this paper we used to propose these timing channels resilience in purpose of jamming attacks in communication channel [5]. In case of continues jamming it produces a high power disturbing signal in communication channel to disrupt completely the communication channel, but is very much cost effective in energy consumptions. That's why in most situations jammer's energy constraints are characterized, in cases like jammer is powered by battery and non continuous jamming such as reactive jamming [4].During these cases the jammer transmits a high power disturbing signal as soon as it detects an ongoing transmission activity and it continuously listens over the wireless communication channel [1]. Timing channels are more, but not totally exempted from reactive jamming attacks, the jamming can take place only after identifying an ongoing transmission in communication channel, therefore the timing information has been decoded by the receiver [6]. An example of timing channel-base communication method has been proposed to neutralize jamming by constructing a low-rate physical layer on top of the existing physical or data link layers using detection and timing of failed packet receptions at the receiver end.

And also analyzed the communication among the jammer and transmissions of the target node [2]. It is expected that using timing channel the target node wants to maximize the amount of the information to be transmitted per unit, but the jammer wants to minimize such amount of information while reducing the energy expenditure [7]. As these two are contradictory, we propose a game-theoretical structure that designs their communications along with the Nash Equilibrium and StackelbergEquilibrium.

II. Assessment on Previous Collection of Work

(i). TC-Aloha: *A novel access scheme for wireless networks with transmit-only nodes. AUTHORS: L. Galluccio, G. Morabito, and S. Palazzo,*

Several networks structures have developed and deployed transmit-only nodes recently, mean the node without having receiving capacity, and are unable to perform synchronization and carrier-sense. So, these networks have to proceed with a medium-access control such as Aloha. Aloha is a protocol in network's medium access sub layer, which gives low throughput due to collisions and poor in energy efficiency. To overcome, these drawbacks in Aloha, we propose a strategy in protocol is Timing channel Sense Aloha (TS-Aloha) which exploits the timing channel. This TS-Aloha enables multi-transmissions of the same information to improve the communication reliability. As mention earlier timing channel is a logical communication channel among the transmitter and receiver, and information is transferred in terms of timing of events.

(ii). A survey on preventing jamming attacks in wireless communication. *AUTHORS:R. Saranyadevi, M. Shobana, and D. Prabakar*

Network administrator is having security provisions and policies on network to prevent unauthorized access of network resources. In context the jamming is also viewed as a form of Denial-of-Service (DoS) attack, by means of preventing the users from receiving timely and adequate information in the communication channel. In this selectively target high important messages, these selective jamming attacks carried out by performing real-time packet classification at physical layer, to prevent this three schemes have been proposed by combining cryptographic primitives with physical layer properties.

(iii). An attack-defense game theoretic analysis of multi-band wireless covert timing networks. *AUTHORS:S. Anand, S. Sengupta, and R. Chandramouli*

Here, we present an adversary game-theoretic strategy, deals with malicious interference based denial-of-service attacks in multi-band covert timing networks. The covert timing network operates on a set of multiple spectrum bands, when each band is associated with an utility that represents the critical nature of the covert data transmitted in the band.DoS attacks are caused by a malicious attacker, using malicious interferences on bands, to defend these

bands camouflaging resources have been deployed by the covert timing network. To project this situation, a two tier game-theoretic strategy is proposed. The first tier is the sensing game, that the covert timing network determines the amount of camouflaging resources to be deployed in each band and the attacker determines the optimal sensing resources too be deployed in each bank. In the second tier, the attacker determines the optimal transmit powers on each spectral band it chooses to attack. This was proved with its performance.

(iv)Jamming sensor networks: *Attack and defense strategies. AUTHORS:W. Xu, K. Ma, W. Trappe, and Y. Zhang*

Due the shared medium of the wireless sensor network, it makes easier for conduct radio interferences, or jamming, attacks that effectively cause a DoS of either transmission or reception functionalities. These attacks can cause adversary, either bypassing MAC-layer protocols or emitting a radio signal that jamming a particular channel. In this literature we observed various jamming attacks, on sensor network, and presented a two-phase method that diagnosis the attack, followed by suitable defense methods. Also highlighted challenges associated in detecting the jamming, to solve this problem, two different strategies are proposed. One is to simply retreat from the interferer which may be accomplished by either spectral evasion or spatial evasion. And the second one is to compete more actively with the interferer by adjusting resources.

III. Design of the System Architecture Using DFDs

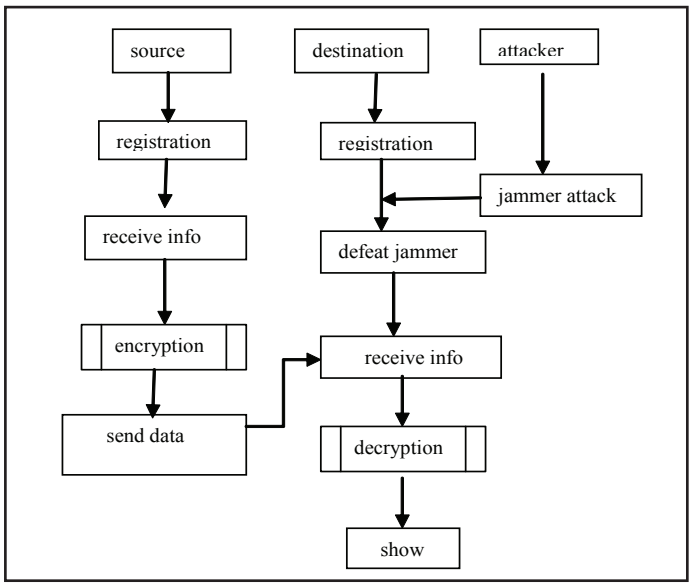

Fig. 1: DFD of Jammer System Architecture

IV. Proposed System

In this paper, we proposed a strategy to overcome the above said disadvantages in existing system:

- A game theoretical method of the interactions among the nodes violating the timing channel to obtain resilience to jamming attacks and a jammer is derived and analyzed.
- Nash equilibrium is discussed under best response changing aspects subjected to uniqueness, existence, and convergence.
- And also, by considering perfect and imperfect knowledge of the utility procedure of jammer's, jammer reactions on communication nodes setting strategies is modeled and analyzed and a Stackelberg game.

The proposed objectives are modularized in the following way:

A. Game-theoretical Method Topology

To examine the proposed game-theoretical method, let us take a situation, two wireless nodes want to communicate that is one is transmitter and another is receiver, while a malicious node targets to disrupting their communication. We considered that malicious node executes a reactive jamming attack on the wireless channel, in this context malicious node as the jammer, J, and the transmitting node under attack as the target node, T.

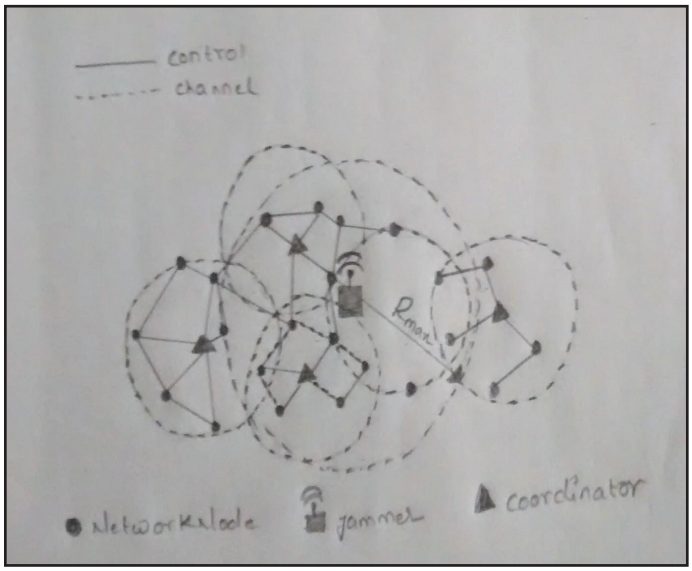

Fig. 2: The Architecture of Jamming Attacks

The jammer senses the wireless channel continuously, and detecting a transmission activity performed by T, J starts emitting a high voltage jammer signal, which is denoted as TAJ is the duration of the time interval among the packet transmission and jamming signal emission. And the duration of the interferences signal emission that jams the transmission of the j-th packet can be taken as continues random variable and it is Yj. To maximize the uncertainty on the value of Yj, we taken exponentially distributed with mean value.

B. Nash Equilibrium Application

In this Section we solve the game described in the above mentioned point, and achieve the Nash Equilibrium points (NEs), in which both players achieve their highest utility given the strategy profile ofthe opponent. In the following we also provide proofs of the existence, uniqueness and convergence to the Nash Equilibrium under best response changing aspects.

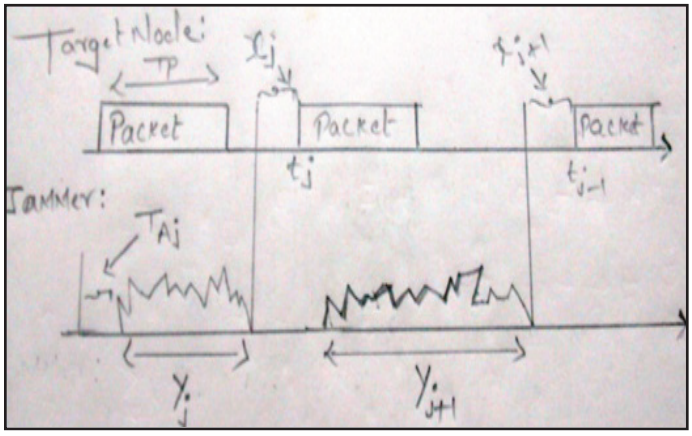

Fig. 3: Interaction Between Jammer and Target Node

C. Presence of NE

The intersection points are within the NEs of the game. Hence, to prove the existence of at least one NE, it ensembles to show that NEs have one or more connection points.

D. NE's Distinctiveness

After proving the NE existence, the uniqueness of the NE specifies that there is only one strategy profile such that no player has motivation to move away one-sidedly.

E. Merging Towards NE

Here, the merger of the game towards the NE, when players following Best Response Dynamics. In BRD the game starts from any initial point , and at each consecutive step, each player plays its strategy by following its best response function.

F. StackelBerg Gaming Model

In this gaming, one of the players acts as the leader by anticipating the best response of the follower. In our proposed structure, the jammer plays its strategy when a transmission from the target node occurs on the censored channel; it makes an assumption that the target node acts as the leader followed by the jammer. The hierarchical structure of the game allows the leader achieve a utility which is at least equal to the achieved utility in the ordinary game at the NE.

Perfect knowledge: It is described as, the target node is completely aware of the utility function of the jammer and its parameters. Then is called perfect knowledge.

Imperfect knowledge: This is described as,if some parameters of the utility function of the jammer are unknown at the target node. Then is called imperfect knowledge.

Table 1: Parameters Setting used in Our Simulations

Name	Value	Unit
TAj	15	µs
△	1	µs
p	2	w
Tp	50	µs

V. Execution Results

The network was successfully implemented and tested. The below pictures shows the various stages of execution.

STEP 1:

Created a wireless network with some nodes and given source and destination range with a message to transmit data from given range. the below which shows successful creation of network with nodes.

Fig. 4: Creation of Nodes in a Wireless Network

STEP 2:

The below figure explains the transmission of message from given source to destination in the wireless network, it shows the range of transmitted packets between the transmission path, the attacker node, number of packets sent and received and loss of packets.

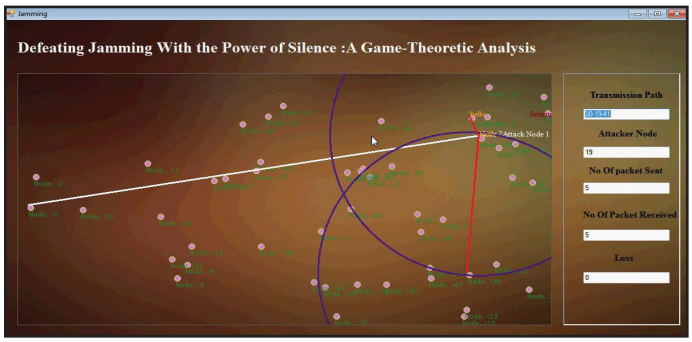

Fig. 5: Transmission of Packets From One Node to Another Node in a Network

VI. Conclusion

This paper described a logical game-theoretical structure of the interactions among a jammer and a communication system the exploits a timing channel to improve flexibility to jamming attacks in the channel. Utility functions parameters of the two players have been analyzed and demoralized to show the existence and independence of the NE and the merger of the game to the NE has been described and presented by analyzing the best response dynamics. Also, a Stackelberg game model has been examined properly, and provided the proof of the SEs existence and independence. As the reactive jammer is assumed to start transmitting its interference signal only after detecting activity of the node under attack is observed. At the end numerical results, derived in various real network settings, has been proved the main idea behind the proposed model that is utilization of timing channels is very well presented. It is also discussed about the imperfect knowledge parameters. Hence providing a framework for the design and understanding of such systems is achieved perfectly.

VII. Acknowledgment

I thank our college St.Martins Engineering College who greatly assisted in the success of the project. I express my thanks and gratitude to r. Ch. A Naidu sir, Head of the Department of CSE, St. Martin's Engineering College for his encouraging support and guidance in presenting this paper.

References

[1] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo,"Efficiency analysisofjamming-based countermeasures against malicious timing channel intactical communications," In Proc. IEEE ICC, 2013, pp. 4020–4024.

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

[3] E. Altman, K. Avrachenkov, A. Garnaev,"A jamming game inwireless networks with transmission cost," In Network Control andOptimization. Berlin, Germany: Springer-Verlag, 2007, pp. 1–12.

[4] M. Strasser, S. Capkun, M. Cagalj,"Jamming-resistant key establishmentusing uncoordinated frequency hopping," In Proc. IEEE Symp. SP,2008, pp. 64–78.

[5] S. Anand, S. Sengupta, R. Chandramouli,"An attack-defense gametheoretic analysis of multi-band wireless covert timing networks", In Proc.IEEE INFOCOM, 2010, pp. 1–9.
[6] V. Anantharam, S. Verdu,"Bits through queues," IEEE Trans. Inf.Theory, Vol. 42, No. 1, pp. 4–18, Jan. 1996.
[7] Y.W. Law, L. Van Hoesel, J. Doumen, P. Hartel, P. Havinga, "Energyefficient link-layer jamming attacks against wireless sensor networkMAC protocols," In Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw., 2005, pp. 76–88.
[8] Computer Security Technology Planning Study (James P. Anderson, 1972)
[9] NCSC-TG-030, Covert Channel Analysis of Trusted Systems (Light Pink Book), 1993 from the United States Department of Defense (DoD) Rainbow Series publications.
[10] Covert Channels in the TCP/IP Protocol Suite, 1996 Paper by Craig Rowland on covert channels in the TCP/IP protocol with proof of concept code.
[11] Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, P. Kocher

P.N.V DIVYA received the B.Tech degree Information Technology from the Jawaharlal Nehru Technological University (JNTU) , Kakinada, India, in 2013 and is currently pursuing M.Tech at St.Martins Engineering College, Hyderabad.

Dr.R.Ch.A.Naidu completed his M.Tech, Ph.D from University of Mysore, Mysore and Andhra University, Vishakhapatnam respectively. He has more than 15 years of teaching experience. He is presently working in CSE Dept as a Professor in St Martin's Engineering College, Hyderabad. His area of interest is Network security, Computer networks, Digital Image processing, Data base management systems .He has life membership in professional bodies like ISTE, CSI.