Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.336 – 342

AVOIDANCE OF JAMMING WITH CONTINUOUS FREQUENCY TIME CHANNELS THROUGH EQUILIBRIA TECHNIQUE

[1]Ms. M.Jayanthi, [2]Mr. L.Mani, [3]Mr. S.Mohan Raj, [4]Mr. A.B.Prashanth

[1]Department of Information Technology, Prathyusha Engineering College, Thiruvallur, India
[2]Department of Information Technology, Prathyusha Engineering College, Thiruvallur, India
[3]Department of Information Technology, Prathyusha Engineering College, Thiruvallur, India
[4]Department of Information Technology, Prathyusha Engineering College, Thiruvallur, India
[1] jayanthi.it@prathyusha.edu.in, [2] manilogan11@gmail.com, [3] mohanraj4095@gmail.com, [4] prashanthab39@gmail.com

ABSTRACT: The Main aim of our project is to transmit/convey the information from transmitter to the receiver even if there is jammer or a malicious node placed between them. Jammer is device which emits high power and high bandwidth signal which blocks the low power communication signals. Jammer is designed in such a way to block particular frequency spectrum. In this, our work is based on time signals which are obtained by taking time samples. Sampling is nothing but chopping of signals with respect to duty cycle. The Jammer can block only the signal so we recommending this project which conveys data in the form of time intervals which cannot be blocked. Along with this we analyze the characteristics of jammer such that strength as well as weakness. In this paper, we are using two equilibria techniques which is Nash Equilibria (NEs) and Stackelberg Equilibria (SEs).

Keywords: Jammer, Nash Equilibria, Stackelberg Equilibria

I. INTRODUCTION

The timing pathway is a transmitting pathway which use silence intervals within the continuous transmissions to encrypt information. In recent times, the utility of timing pathway [3] has been determined in the wireless dominion to cooperate short rate, energy efficient transmissions in addition to hidden and flexible communications. In this summary we target the flexibility of timing pathway to jamming attacks. Almost, this initiative can entirely disturb the interactions whereas the jammer constantly it explore a huge power threating signal, i.e. during repeated jamming is accomplished. In spite of, repeated jamming is pure expensive in conditions of energy consuming for the jammer. That is the logic how best scheme based on energy compulsion since a jammer.eg: During the jammer is battery energize non-repetitive jamming specific as receptive jamming is designed. Here the jammer repeatedly accepts done the wireless pathway and give impulse to the communication of a huge power disrupting signal nearly it find an ongoing communication action. Efficiency of conscious jamming has been determined and it's even cost designed.

Timing pathways are higher even though not totally allowed against conscious jamming attacks [7]. Actually, the interrupting signal activate its disrupting action opposite to the transmission only later analyze an ongoing communication and hence later the timing data has been decrypt by the recipient.

In this summary, we determine the interplay in the middle of a jammer and the knot whose communications are below attack, whatever we command target node. Respectively, we believe that the target knot desire to increase the quantity of data that can be send per unit of time by the method of timing pathway. Because, the jammer desire to decrease such quantity of data although compressing the energy amount the target knot and the jammer have contrary interests, we expand a game theoretical schema [4] that typical their communications. We check out both the container in whichever these two attacker play their actions concurrently and the position while the target knot(leader) expect the action of the jammer (follower). To this intention, we analyze the pair of the Nash Equilibrium (NEs) and Stackelberg Equilibrium (SEs) [9] of our suggested games.

The main benefaction of this summary can be outline as follows: 1) We design the communication within a jammer and a target knot as a jamming game, 2) We establish the duration, singleness and merging to the Nash Equilibrium (NE) below most excellent result in action, 3) We establish the duration and singleness of the balance of the stackelberg game place the target knot perform as a commander and the jammer reacts as a consequence, 4) We consider in this latest stackelberg scheme the force on the attainable execution on imperfect knowledge on the jammers efficiency action 5) We control an extended numerical design which demonstrated that our suggested models well catching the main point following the operation of timing pathways, hence defining desirable scheme for the model and accepting of such systems.

Correspondingly, the remainder of this summary is arranged as follows. Similar work is provided. In the suggested jamming game design is given. A theoretical analyze of the duration and uniqueness of the NE besides of the merging of the game to that equilibrium below best reacting movement is explained. Duration and singleness of the SE are considers, composed with some application consistent to imperfect knowledge scheme. Later, numerical results illuminated. Lastly, completions are draw.

II. LITERATURE SURVEY

A. TC-Aloha: A novel access scheme for wireless networks with transmit-only nodes

In the recent past several network scenarios have emerged where transmit-only nodes - i.e., nodes without receiving capabilities - are deployed. Such nodes cannot perform carrier sensing and cannot be synchronized. Therefore, they have to apply an Aloha-like medium access control. However, it is well known that Aloha achieves low good put due to the possibility to incur in collisions, and this results in poor energy efficiency too. In order to achieve better performance, in this paper a scheme called Timing-Channel Aloha (TC-Aloha) is introduced which exploits the timing channel. The timing channel is the logical communication channel established between a transmitter and a receiver in which the information is transferred by means of the timing of events. Another feature of TC-Aloha is that it enables multiple transmissions of the same information to improve the communication reliability. In this paper the TC-Aloha scheme is described in detail and an analytical framework is derived for the evaluation of its performance. The numerical results assess the advantages of TC-Aloha over traditional solutions.

B. Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications

A covert channel is a communication channel that creates a capability to transfer information between entities that are not supposed to communicate. A relevant instance of covert channels is represented by timing channels, where information is encoded in timing between events. Timing channels may result very critical in tactical scenarios where even malicious nodes can communicate in an undisclosed way. Jamming is commonly used to disrupt this kind of threatening wireless covert communications. However jamming, to be effective, should guarantee limited energy consumption. In this paper, an analysis of energy-constrained jamming systems used to attack malicious timing channels is presented. Continuous and reactive jamming systems are discussed in terms of their effect on the achievable covert channel capacity and jammer energy consumption. Also, a simple experimental set up is illustrated and used to identify proper operating points where jamming against malicious timing channels is effective while achieving limited energy consumption.

C. Jamming sensor networks: Attack and defense strategies

Wireless sensor networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. These attacks can easily be accomplished by an adversary by either bypassing MAC-layer protocols or emitting a radio signal targeted at jamming a particular channel. In this article we survey different jamming attacks that may be employed against a sensor network. In order to cope with the problem of jamming, we discuss a two-phase strategy involving the diagnosis of the attack, followed by a suitable defense strategy. We highlight the challenges associated with detecting jamming. To cope with jamming, we propose two different but complementary approaches. One approach is to simply retreat from the interferer which may be accomplished by either spectral evasion (channel surfing) or spatial evasion (spatial retreats). The second approach aims to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, to achieve communication in the presence of the jammer.

D. A survey on preventing jamming attacks in wireless communication

Network security consists of provisions and policies adopted by network administrator to prevent unauthorized access of network accessible resources. Jamming can be viewed as a form of Denial-of-Service attack, whose goal is to prevent users from receiving timely and adequate information. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. This paper presents a survey of the existing jamming attack prevention techniques. Selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes are also presented in this paper.

E. An attack-defense game theoretic analysis of multi-band wireless covert timing networks

We discuss malicious interference based denial of service (DoS) attacks in multi-band covert timing networks using an adversarial game theoretic approach. A covert timing network operating on a set of multiple spectrum bands is considered. Each band has an associated utility which represents the critical nature of the covert data transmitted in the band. A malicious attacker wishes to cause a DoS attack by sensing and creating malicious interference on some or all of the bands. The covert timing network deploys camouflaging resources to appropriately defend the spectrum bands. A two tier game theoretic approach is proposed to model this scenario. The first tier of the game is the sensing game in which, the covert timing network determines the amount of camouflaging resources to be deployed in each band and the malicious attacker determines the optimal sensing resources to be deployed in each band. In the second tier of the game, the malicious attacker determines the optimal transmit powers on each spectral band it chooses to attack. We prove the existence of Nash equilibriums for the games. We compare the performance of our proposed game theoretic mechanism with that of other well known heuristic mechanisms and demonstrate the effectiveness of the proposed approach.

III. SYSTEM ARCHITECTURE

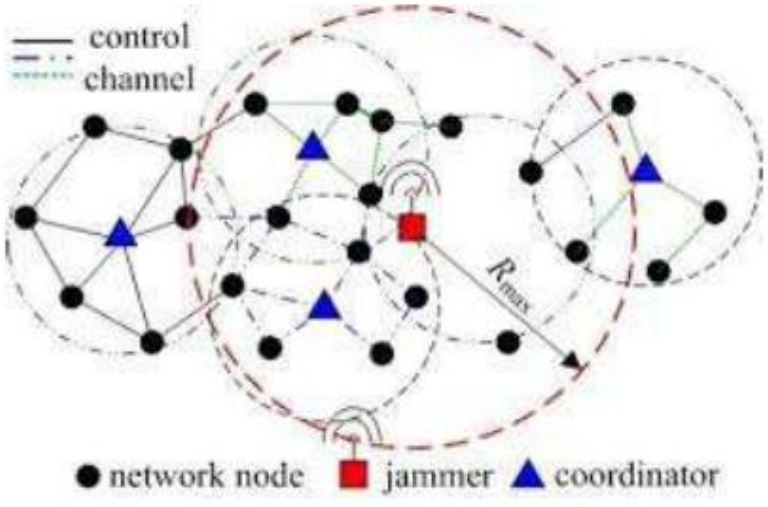

Fig:-1 System Architecture of jamming attacks

The modules that are available in this system are

- Network Setup
- Malicious node/Jammer
- Time sampling
- Stackelberg Analysis

A. Network Setup

This module describes the designing phase of the Network. We know that in order to communicate we are in need of a transmitter and a receiver intermediate nodes and a network while communicating a malicious node aims at disrupting the communication. we assume that the malicious node executes a reactive jamming attack on the wireless channel. In the following we refer 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. 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*. Along with this we analyze the characteristics of jammer such that strength as well as weakness.

B. Malicious node/Jammer

The Data is transferred from source to destination in between we may have n no of nodes there might be a malicious node. Malicious node is nothing but a hacker or foreign node which leads to packet drop here the malicious node is referred to jammer which blocks the data transfer from source to destination. Jammer emits high power signal to block the data transfer. Our aim is to transfer the data from source to destination even jammer is present.

C. Time sampling

Time sampling is a sampling method that involves the acquisition of representative samples by observing subjects at different time intervals. These time intervals can be chosen randomly or systematically. In our Project we follow systematic time intervals. Time sampling is similar to encryption here we going to convert signal into time intervals this is achieve by taking sampling of signal. Sampling is nothing but chopping of signal. Signal may be sin or cos wave we have specific duty cycle by dividing duty with some chopped value. In receiver side we again going to decrypt or convert the time sample into signal by which we can retrieve the information.

D. Stackelberg Analysis

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 which shows efficiency of our project .

IV. GAME THEORY DEFINITIONS ALGORITHM

The game theory definition algorithm are as follows

- Dominant strategy
- Nash Equilibrium
- Maximin strategy

A. Dominant strategy

A player will have a dominant strategy [5] if its choice is optimal regardless of what the opponent does. A strategy is dominant if it pays at least as much as any other strategy regardless the action of the other player.

B. Nash Equilibrium

In a Nash Equilibrium, each firm is doing the best it can, given what its competitors are doing. Nash equilibria are usually non-cooperative outcomes [9] . Each firm chooses the strategy to maximize its profits given its opponent's actions. At the equilibrium, there is no incentive to change strategies, since you cannot improve payoffs.

C. Maximin strategy

It is the strategy that minimizes a player's worst possible outcome. This strategy may be used by players concerned about their opponent's rationality.

D. Stackelberg model

In a Stackelberg model, equilibrium is reached when Firm 1 pre-emptively expands output and secures larger profits. Hence the term "**first mover advantage**". In fact, Firm 2 is forced to curtail output given that the leader (firm 1) has already produced a large output ("As I produce more, you react by producing less.

V. FUTURE ENHANCEMENTS

In this paper we finding the jammer characteristics and also we send the message to the receiver. This paper mainly concentrates on the communication between source to destination node without jammer knowledge. This concept is very use full to the defense purpose.

VI. CONCLUSION

In our paper, we have used a game theory analysis for defeating the jammer by providing the continuous timinig channels. The continuous timing channel frequency was given by Nash and Stackelberg equilibria techniques. Analytical values of the efficiency functions of both players are designed and used to confirm the duration and singleness of the NASH Equilibrium. Jammer strategy will be found by using Nash Equilibrium and hence it will send the high frequency message and overcome the jammer. Stackelberg game has been correctly examined, and evidence on the time period and singleness of the stackelberg balance has been maintained at the receptive jammer. Therefore by using these techniques, the message will be send without the interruption of jammer while transmission and reception. Here we have modeled the jammer strategy and overcoming from the jammer by using nash and stackelberg equilibrium.

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 ACM Conf. 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] 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.

[7] 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

[8] R.-T. Chinta, T. F. Wong, and J. M. Shea, "Energy-efficient jamming attack in IEEE 802.11 MAC," in Proc. IEEE MILCOM, 2009, pp. 1–7.

[9] Y. W. Law, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MACprotocols," in Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw., 2005, pp. 76–88.

