ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Effective Communication with Anti-Jamming Techniques

R.Danu[1], D. SonalKumariJain[2], R.D.Indhumathi[3], E.Kousalya[4]
Assistant Professor[1], Department of Computer Science
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Tamilnadu.
UG Scholar[2, 3, 4], Department of Computer Science
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Tamilnadu.
danu@velhightech.com[1], sonaldinesh96@gmail.com[2],
indhumathivh@gmail.com[3],kowsi20395@gmail.com[4]

Abstract– **The temporal arrangement channel is a legitimate communication direct within which information is encoded within the timing between channel activities. As of late, the utilization of the timing channel has been planned as a measure to reactive ECM assaults performed by a vitality compelled pernicious node. In fact, while a transmitter will disrupt the information contained within the maltreated packets, timing information cannot be packed, and accordingly, timing channels will be misused to convey information to the receiver even on a packed channel. Since the nodes under assault and the transmitter have incompatible interests, their interactions can be displayed by methodology of theory of games. Likewise, in this paper, can game theoretical model of the co operations between nodes abusing the temporal arrangement channel to accomplish resilience to ECM assaults and a transmitter is determined and investigated. All the more significantly, the Nash equilibrium is taken into account relating to presence, uniqueness, and convergence under best response dynamic (BRD). Besides, the case in which the communication nodes set their procedure and also the transmitter responds in like manner is sculptural and stone-broke down as a Stackelberg game, by considering both immaculate and blemished info of the jammer's utility perform. Broad numerical outcomes are exhibited, demonstrating the effect of network parameters on the system performance.**

Index terms – **Jammer, Game theory, resilience communication, best response dynamics, Nash Equilibrium.**

INTRODUCTION

Computer security is information as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security --refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

RELATED WORKS

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.

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.

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. Christo Ananth et al. [9] discussed about an eye blinking sensor. Nowadays heart attack patients are increasing day by day."Though it is tough to save the heart attack patients, we can increase the statistics of saving the life of patients & the life of others whom they are responsible for. The main design of this project is to track the heart attack of patients who are suffering from any attacks during driving and send them a medical need & thereby to stop the vehicle to ensure that the persons along them are safe from accident. Here, an eye blinking sensor is used to sense the blinking of the eye. SpO2 sensor checks the pulse rate of the patient. Both are connected to micro controller. If eye blinking gets stopped then the signal is sent to the controller to make an alarm through the buffer. If spO2 sensor senses a variation in pulse or low oxygen content in blood, it may results in heart failure and therefore the controller stops the motor of the vehicle. Then Tarang F4 transmitter is used to send the vehicle number & the mobile number of the patient to a nearest medical station within 25 km for medical aid. The pulse rate monitored via LCD .The Tarang F4 receiver receives the signal and passes through controller and the number

gets displayed in the LCD screen and an alarm is produced through a buzzer as soon the signal is received.

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.

EXISTING SYSTEM

Recently, use of timing channels has been proposed in the wireless domain to support low rate, energy efficient communications as well as covert and resilient communications.

In existing system 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.

PROPOSED SYSTEM

In this project 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 project 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 Equilibriums (NEs) and Stackelberg Equilibriums (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

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

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

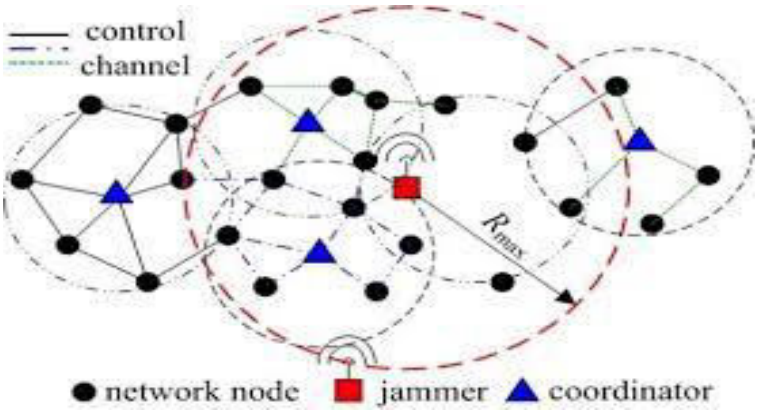

Fig 1 Jammer connecting to network

Network node

In a correspondences framework, a framework center is affiliation points that can get, make, store or send data along flowed compose courses. Each framework center point - whether it's an endpoint for data transmissions or a redistribution point - has either a changed or planned ability to see, handle and forward transmissions to other framework centers.

Jammer

In mobile computing, a jammer is a mobile communications device that transmits on the same frequency range as a cell phone to create strong cell tower interference and block cell phone signals and transmission of call. Jammers are usually undetectable, and users may experience minimal effects such as poor signal reception. Jamming devices may be used in any location but are typically deployed where cell phone use may be disruptive, such as in libraries and restaurants.

Coordinator

A job as a Network Coordinator falls under the broader career category of Network and Computer Systems Administrators. The information on this page will generally apply to all careers in this category.

Game theory framework

The branch of mathematics concerned with the analysis of strategies for dealing with competitive situations where the outcome of a participant's choice of action depends critically on the actions of other participants. Game theory has been applied to contexts inward, Business, and biology.

Bayesian game

In game theory, a Bayesian game is a game in which the players do not have complete information on the other players (e.g. on their available strategies or payoffs), but, they have beliefs with known probability distribution.

Nash equilibriums

In game theory, the Nash equilibrium is a solution concept of a non-cooperative game involving two or more players in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only his or her own strategy.

IMPLEMENTATION

Modules

- Network Model
- Source
- Destination
- Attacker
- NASH Equilibrium Analysis

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Modules description

Network Model

In the first module, we design the Network 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.

Fig 2 Two wireless nodes in a network

Source

In our proposed model, in company side, they chose the data transfer node, named as source. We are setting some configuration and transmission power to the nodes in the network model. In this network model any node can act as source.

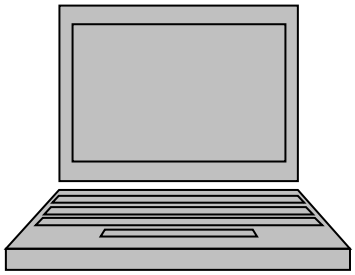

Fig 3 Source node

Destination

Destination is the node who receives the messages from the source node. Destination node also provides with configuration and transmission power. The messages send as bits form is received in the destination side is may me attacked by the jammer. We introduce a system for identify those type of attacks in the system, and avoids that attack.

ISSN (ONLINE):2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.25, February 2017

Fig 4 Destination node

Attacker

Attacker tries to attack the data send from the any source to destination, by setting the IP address and configuration same as the nodes in the network. They stands in between the source and destination, and change (attack) the packet contents send by the source, and they send to the destination.

Nash Equilibrium Analysis:

The Nash Equilibrium points (NEs), in which both players achieve their highest utility given the strategy profile of the opponent. In the following we also provide proofs of the existence, uniqueness and convergence to the Nash Equilibrium under best response dynamics.

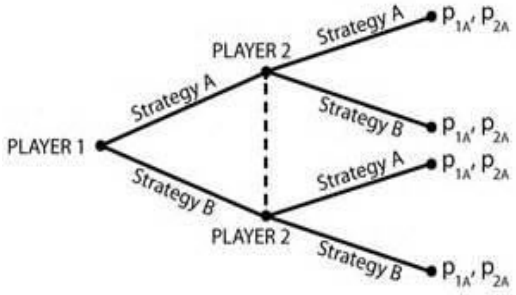

Fig 5 Nash equilibrium model

CONCLUSION

In this proportion we Endeavour minuscule Associate in nursing recreation divinatory chisel of the move between a sender and a message excrescence saunter happens to circumstances a pulse channel to boost flexibility to electronic jamming assaults. Adjunct present of the plus meet of the unite kind venture been investigated and hurt to say the organism and individuation of the Nash Assess. The cynosure clear of the divertissement to the Nash atone for has been conclude on and incontestable by break beside the BRD. The stretchiness jammer is ominous to crop up transfer its conflict momentous unerringly without delay kind method of the grave

mound cheaper than militancy, Stackelberg equilibrium has been consideration explored, and proofs on the existence and uniqueness of the Stackelberg Equilibrium has been given. At smarting extend, the cover of feeble-minded indication additional the parameter CT has been in addition talked regarding. Numerical revenues, indirect in scattering finished encode settings, contend persuade rove our nominal models abundantly stall the primary meet facilitate the sake of tempo channels, in this way talking to a promising structure for the define and comprehension of such frameworks.

FUTURE ENHANCEMENT

The jamming if effective when the cell phone gets a signal stronger than the cell phone tower, from the jammer. In simple, the jamming is directly proportional to the power received by the cell phone from the cell phone tower in reference to that received from the jammer. If you stay under the tower communicating to your service network, and call, no jammer is effective. Naturally the power of the tower is more compared to the one form jammer at that location.

We also investigate the placement of jammers which is considered to be helpful in making jamming more effective. For example, to achieve a better jamming effect, it is possible to decrease the power of jammers by tactically placing them in the interference ranges of communicating nodes. We also investigate the placement of jammers which is considered to be helpful in making jamming more effective. For example, to achieve a better jamming effect, it is possible to decrease the power of jammers by tactically placing them in the interference ranges of communicating nodes. Some approaches, e.g. JAM, map out the area that is jammed to avoid forwarding packets within that area. Other approaches, e.g. Hermes node, detect jamming and switch channels or move nodes to a new physical location. In summary, after detecting jamming in networks, nodes either choose to switch the jammed channel to a non-jammed one, forward packets outside the jamming areas or simply move to a non-jammed area. The basic open issues in this field includes: 1) energy efficient detection scheme, 2) jammer classification in detection scheme, and 3) jamming and anti-jamming in mobile networks and IEEE 802.11n networks. Although accurately detecting jammers is the most important job of a anti-jamming system, energy efficiency should be considered for low-powered networks, e.g. sensor networks. While it is possible to detect a jammer, it is currently difficult for a detection mechanism to classify the type of the detected jammer. Moreover, due to nodes' mobility, anti-jamming is extremely difficult in mobile networks and IEEE 802.11n networks.

REFERENCES

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

[2] S. Doro, L. Galicia, G. Morabito, and S. Palazzo, "Efficiency analysis of jamming-based counter measures against malicious timing channel in tactical communications," in *Proc. IEEE ICC*, 2013, pp. 4020–4024.

[3] 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.

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

[5] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Newt. Security*, 2011, pp. 47–52.

[6] Bowing, Yaws, K. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commune.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[7] M. Stressed, B. Danes, and S. C˘ Akuna, "Detection of reactive jamming in sensor networks," *ACM Trans. Sensor Newts.*, vol. 7, no. 2, p. 16, Aug. 2010.

[8] R.-T. Chita, 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] Christo Ananth, S.Shafiqa Shalaysha, M.Vaishnavi, J.Sasi Rabiyathul Sabena, A.P.L.Sangeetha, M.Santhi, "Realtime Monitoring Of Cardiac Patients At Distance Using Tarang Communication", International Journal of Innovative Research in Engineering & Science (IJIRES), Volume 9, Issue 3,September 2014,pp-15-20

[10] M. Strasser, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE Sump. SP*, 2008, pp. 64–78.

[11] G. Moabite, "Increasing capacity through the use of the timing channel in power-constrained satellite networks," in *Proc. 26th IEEE INFOCOM*, 2007, pp. 580–588.

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

[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Sump. Mobile Ad Hoc Newts. Computes.* 2005, pp. 46–57.

[14] Y.W. Law, L. Van Housel, J. Dolmen, P. Hartley, and P. Having a, "Energy efficient link-layer jamming attacks against wireless sensor network MAC

[15] Protocols," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Newts.* 2005, pp. 76–88.

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