Mohammed Ghowse.M.E *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 5, May- 2016, pg. 29-33 **ISSN: 2321-8363**
Impact Factor: 4.123

AN ATTEMPT TO FIND A SOLUTION FOR DESTRUCTING JAMMING PROBLEMS USING GAME THERORITIC ANALYSIS

Mohammed Ghowse.M.E[1], Mr. E.S.K.Vijay Anand[2]
[1]P. G Scholar, E-mail: ghowsegk2326@gmail.com
[2]Assistant Professor, Email: samuelvijayanand@gmail.com
[1],[2]G.K.M.College of Engineering and Technology, Chennai, Tamilnadu, India

Abstract

The timing channel is a logical statement channel in which information is encoded in the timing between actions. A force-constrained malicious node performed has been planned as a countermeasure to reactive active jamming attacks using logical timing channel. In fact, while a jammer is able to interrupt the information contained in the attacked packets, timing information cannot be jammed, and so timing channels can be broken to deliver information to the receiver even on a jammed channel. Since the nodes below attack and the jammer have conflicting interests, their communications can be modeled by means of game theory. A game-theoretic model of the communications between nodes exploiting the timing channel to achieve flexibility and secure to jamming attacks and a jammer is derived and analyzed. More specifically, the Nash equilibrium is studied in terms of existence, individuality, and convergence under best reaction dynamics. Also, the case in which the communication nodes set their approach and the jammer reacts therefore is modeled and analyzed as a Stackelberg game, by considering both ideal and damaged knowledge of the jammer's utility function. Extensive numerical results are presented, screening the impact of network limitation on the system performance.

Index terms- Anti-jamming, Timing channels game-theoretic models, Nash equilibrium models, Logical Timing channels.

1. Introduction

Computer or Cyber security

It is also known as cyber security is information security as apply to computers and networks. Which computer-based equipment covers the all process and mechanism, information and services are protected from unauthorized change or destruction, unintended or unauthorized access. Information security also includes defense from unexpected events and natural mischances. Otherwise, in the computer industry, the them security or the expression computer safety refers to techniques for certifying that information stored in a computer cloud not be compromised or read by any individuals without authorization. Most computer security procedures involve data passwords and encryption.

1. Physical Safety

Technical events like login keywords, anti-virus are essential. The first and more important line of defense is a secure physical space. Human threats are not the only concern. Our computer takes account of those risks as well in physical location.

2. Access passwords

The networks and common information systems are protected in share by login identifications (user-IDs and keywords).Access keywords are also an important protection for personal computers in maximum conditions. Organizations are regularly open and shared spaces, so that physical access to computers cannot be completely controlled by unauthorized.

To protect your computer, you should be considering setting passwords for sensitive applications resident on the computer (e.g., data analysis software), if the capability of that software provides.

3. Snooping eye protection

Deal with all facets of clinical, research, administrative information and educational here on the health site, it is key to do all possible to exposure minimize of data to unauthorized individual persons.

4. Anti-virus software

Up-to-date, continuously configured anti-virus software is essential. While server-side anti-virus software on our network computers, you also need it on the client side (your base station).

5. Firewalls

Infrastructures among your computer and the external world are monitor by firewall software and hardware. Anti-virus products check files on your computer and in email. That is essential for any networked computer.

6. Software updates

It is serious to have the software up to time, mostly the effective system, anti-virus and anti-spyware, correspondence and browser software products. Almost all anti-virus have automatic update features. Keeping a signature (digital patterns) of mean software sensors up-to-date is essential for these products to be effective.

7. Keep secure backups

Prepared for the worst making backup copies of sensitive data, and keeping those backup copies in a separate files are secure location. For example use additional hard drives, CDs/DVDs, or flashy motivations to collection acute, hard-to-replace figures.

2. Proposed System

Timing channels to jamming attacks. In overall, these occurrences can totally upset infrastructures when the jammer incessantly produces a high power disconcerting signal, i.e., when constant jamming is performed. Analyze the relations between the jammer and the node whose broadcasts are under attack, which call target node. Specifically, assume that the board node needs to exploit the sum of information that can be transmitted per unit of time by income of the control network, whereas, the jammer needs to minimize such amount of information while reducing the drive spending.

As the board node and the jammer have conflicting interests, progress a game theoretic outline that models their connections. Investigate both the case in which these two adversaries play their strategies simultaneously, and the condition when the board node (the leader) expects the actions of the jammer (the follower). To this purpose, training equally the Nash Equilibria (NEs) and Stackelberg Symmetries (SEs) of our proposed games.

Advantages of Proposed System

- Perfect the connections among a jammer and a target node as a jamming game
- prove the presence, uniqueness and union to the Nash symmetry (NE) under best reply dynamics
- prove the presence and individuality of the symmetry of the Stackelberg ready where the board node plays as a leader and the jammer reacts consequently

System Architecture

Configure node settings to the nodes to your specific needs. For those settings that have default values, can retain those default settings or modify them. Jamming attacks are severe Denial-of service attacks against wireless medium considering the role of wireless opposition, which targets the packets of high importance by emitting radio frequency indications and do not track fundamental network construction. Encryption is the most operative way to accomplish data safety. To read an encoded data, you must have access to a secret key or password that enables you to decrypt it.

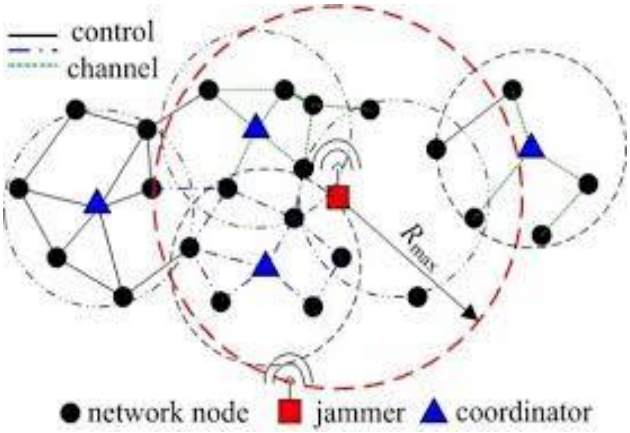

Fig 1.System Architecture

3. Modules Description

3.1. Network Prototypical

In the main component is System Model. Consider the situation where two wireless nodes, a receiver and a transmitter, want to communicate, while a malicious node aims at distracting their communication. To this purpose, assume that the malicious node executes an immediate jamming attack on the wireless channel. In the following refer to the malicious node as the jammer J, and the transmitting node under attack as the target node T. Sensing a probable broadcast movement done by T, J starts from emitting a jamming signal. The jammer senses the wireless channel continuously. The duration of the interfering signal production that jams the transmission of the j-th package it can be showed as an unceasing accidental variable, which calls Yj. To maximize the uncertainty on the value of Yj, assume that it is exponentially distributed with mean value y.

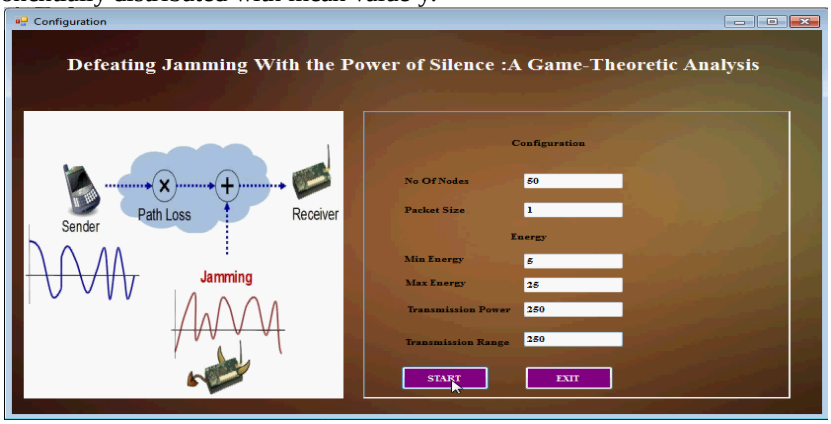

Fig 2.Configuration

3.2. Source

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

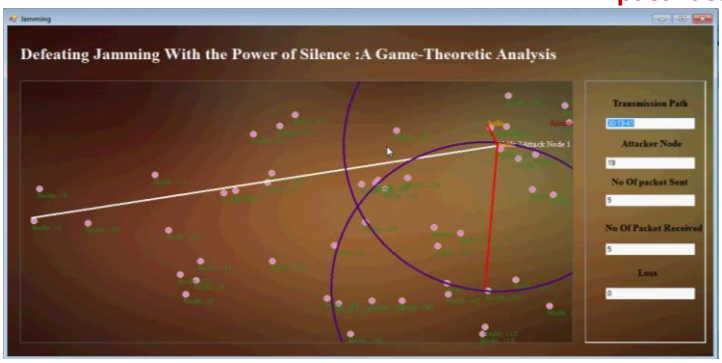

Fig 3.Jamming source

3.3. 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.

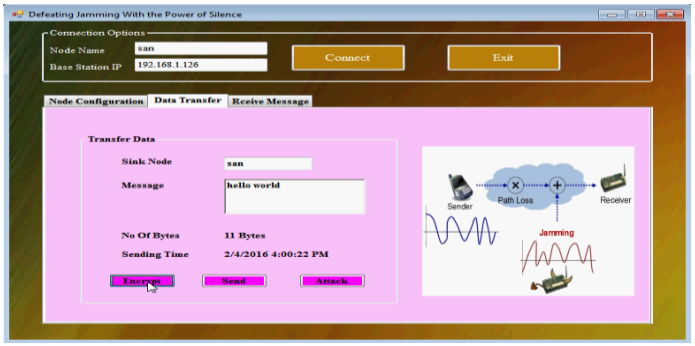

Fig 4.Encryption data in destination

3.4. 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.

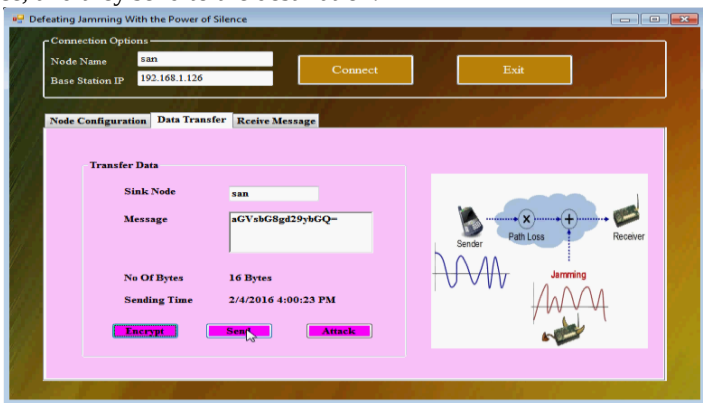

Fig 5.Data Transfer in attacker side

3.5. NASH Equilibrium Analysis

Nash Equilibrium points (NEs) is, which both players achieve their highest value given the strategy profile of the opponent. In the following also provide proofs of the existence, convergence and uniqueness to the Nash Equilibrium under best response dynamics. Uniqueness of the Nash Equilibrium is providing the NE subsistence in Theorem, let us prove the uniqueness of the NE, there is only one strategy profile such that no one player has incentive to deviate unilaterally.

4. Conclusion

The joining of the diversion to the Nash Equilibrium has been concentrated on and demonstrated by breaking down the best reaction progress. An amusement theoretic model of the connections between a jammer and a correspondence hub that adventures a timing channel to enhance flexibility to sticking assaults. Auxiliary properties of the utility elements of the two players have been investigated and misused to demonstrate the presence and uniqueness of the Nash Equilibrium. Besides, as the receptive jammer is expected to begin transmitting its impedance flag strictly when identifying movement of the hub under assault, a Stackelberg diversion has been appropriately explored, and proofs on the presence and uniqueness of the Stackelberg Equilibrium has been given. Numerical results, inferred in a few genuine system settings, demonstrate that our proposed models well catch the fundamental elements behind the use of timing channels, in this way speaking to a promising structure for the outline and comprehension of such frameworks.

References

[1] 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.
[2] V. Anantharam and S. Verdu, "Bits through queues," IEEE Trans. Inf. Theory, vol. 42, no. 1, pp. 4–18, Jan. 1996.
[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] 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
[6] 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.
[7] 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. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46–57.
[8] M. Strasser, B. Danev, and S. C˘ apkun, "Detection of reactive jamming in sensor networks," ACM Trans. Sensor Netw., vol. 7, no. 2, p. 16, Aug. 2010.
[9] M. Strasser, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in Proc. IEEE Symp.SP,2008,pp.64–78.

