Timing Channel Algorithm used 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, 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.*

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

I. 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 protection from unplanned events and natural disasters. Otherwise, in the computer industry, the them security or the phrase computer security refers to techniques for ensuring 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 security:

Technical measures like login passwords, 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 part by login credentials (user-IDs and passwords).Access passwords are also an important protection for personal computers in most circumstances. Offices are usually 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 medical campus, it is important to do everything possible to exposure minimize of data to unauthorized individual persons.

4. Anti-virus software:

Up-to-date,continusily 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:

Communications between your computer and the outside 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 critical to keep the software up to date, particularly the operating system, anti-virus and anti-spyware, email and browser software products. Almost all anti-virus have automatic update features. Keeping a signature (digital patterns) of malicious software detectors 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 supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

8. Report problems:

If you believe that your computer or any data on it has been compromised, you should make an information security event report. That is required by University policy for all data and information on our systems, and legally required for financial, health, education, and any other kind of record containing identifiable personal information.

Benefits of secure computing:

- **Protect yourself - Civil liability**:

  You may be held legally responsible to compensate third party users should they experience financial damage or distress as a result of their personal data being stolen from you or leaked from you.

- **Protect credibility - Compliance**:

  Compliancy with the Data Protection Act, FSA and SOX or other regulatory standards. Each of these bodies stipulates that certain events be taken to protect the data on your network.

- **Protect reputation – Spam:**

  A common use for a contaminated system is to join them to a botnets (a collection of contaminated machines which takes orders from a command server) and use them to send out the spam. This spam can be traced back to you, and your server could be blacklisted and you could be unable to send email.

- **Protect income - Competitive advantage:**

  There are a number of "hackers-for-hire" internets selling their skills in advertising their services on the skills in breaking into servers to steal client databases, proprietary software, unification and acquisition information, personnel detail set al.

- **Protect your business – Blackmail**:

  A seldom-reported source of benefits for hackers is to· break into your server and database, change all your passwords and lock you out of it. The password is then sold back. The "hackers" may implant a malicious program on your server so that they can repeat the exercise.

- **Protect your speculation - Free storage:**

  Server's hard drive space is used to house the hacker's video, music, pirated software or worse. Your computer or server then becomes continuously slow and your internet connection speeds get worse due to the number of people connecting to your server in order to download the offered wares.

II. PROPOSED SYSTEM

MODULES DESCSRIPTION

1. Network Model:

In the first module is Network 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 a 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. Detecting a possible transmission activity performed 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 packet it can be modeled as a continuous random variable, which calls Yj. To maximize the uncertainty on the value of Yj, assume that it is exponentially distributed with mean value y.

2. 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.

3. Existence of the Nash Equilibrium:

It is that the intersection points between bT(y) and bJ(x) are the NEs of the game. To express the existence of at least one NE, it suffices to prove that bT(y) and bJ(x) have one or more connection points. In other words, it is sufficient to find one or more pairs.

4. Uniqueness of the Nash Equilibrium:

Proving 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.

5. Convergence to the Nash Equilibrium:

Analyze the convergence of the game to the Nash Equilibrium when players follow Best Response Dynamics (BRD). In BRD the game starts from any of the initial point(x (0).y (0))∈ Sand, at each successive step, each player plays its strategy.

6. Performance Analysis:

The game allows the leader to achieve a utility which is at least equal to the utility achieved in the ordinary game at the Nash Equilibrium, if assume perfect knowledge, that is, the target node is completely aware the utility function of the jammer and its parameters, and it is able to evaluate bJ(x). Whereas, if some parameters in the effective function of the jammer are unknown at the target node.

7. System Architecture:

The network model Configure node settings to the nodes to your specific needs. 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 signals and do not follow underlying network architecture. Encryption is the most effective way to achieve data security.

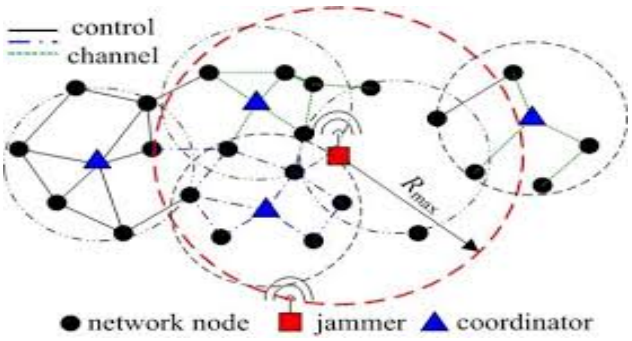

Fig 1.System Architecture

9. Features of .Net

Microsoft .NET is a set of implementation technologies in Microsoft software technologies for rapidly building and integrating XML Web services is Web solutions, and Microsoft Windows-based applications. The .NET Framework is a language-neutral platform for writing programs that can be easily and securely interoperate. There's no language barrier with .NET: there are many languages available to the developer including Managed C, C++, C#, Visual Basic and Java Script. It standardizes communications protocols and common data types so that components created in different languages can easily interoperate. The .NET framework provides the basis for components to interact seamlessly, whether locally or remotely on different platforms .NET is also the combined name given to various software components built upon the .NET platform. These will be both products is (Windows.NET (Win.NET) Server and Visual Studio.NET, for instance) and services (like Passport, .NET My Services, and so on).

10. The Advantage Encryption Standard

- The advanced encryption standard (AES) is a symmetric-key block cipher published by national institute of standards and technology (NIST).
- Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.
- AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

AES METHODS:

- Convert to state array
- Transformations

- Add round key
- Sub bytes
- Shift rows
- Mix-columns

ADVANTAGES of AES:

- AES is more secure (it is less susceptible to cryptanalysis than 3des).
- AES is faster in both hardware and software.
- AES supports larger key sizes than 3Des's 112 or 168 bits.
- AES 128-bit block size makes it less open to attacks than 3des with its 64-bit block size.

III. RESULTS

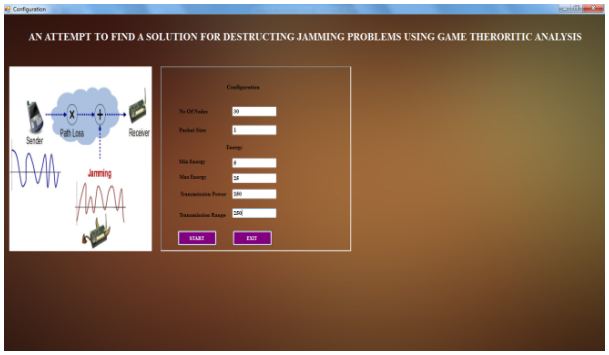

Fig 2.Configuration

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. Also can modify settings either when create the node, or at any time after have created it.

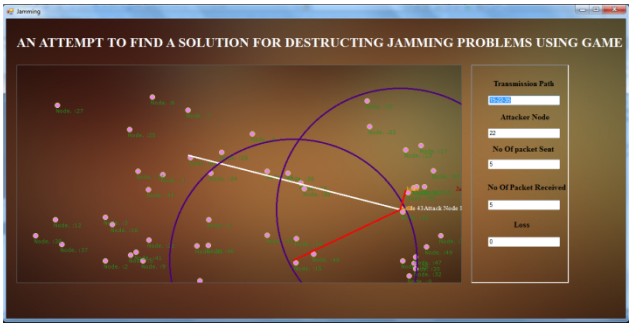

Fig 3.Jamming

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 signals and do not follow underlying network architecture.

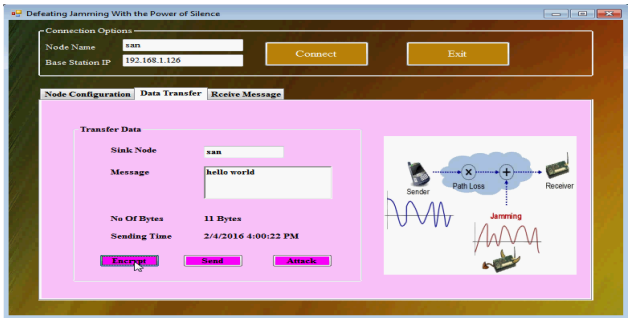

Fig 4.Encryption

Encryption is the most effective way to achieve data security. To read an encrypted data, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

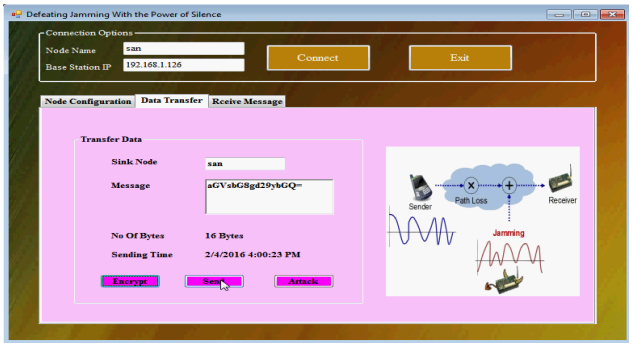

Fig 5.Data Transfer

IV. CONCLUTION

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. The joining of the diversion to the Nash Equilibrium has been concentrated on and demonstrated by breaking down the best reaction progress. 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

V. FUTURE EXTENSION

In this project I reduced the timing channel for jamming attacks. In future any one of the person can do to reduce the more timing channel for jamming attacks and also used the various game theoretic analysis. In future 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. Investigate in this latter Stackelberg scenario the impact on the achievable performance of imperfect knowledge of the jammer's utility function.

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] 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., 2005, pp. 76–88. 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 Netw. Security, 2011, pp.47–52.

[8] 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.

[9] M. Strasser, B. Danev, and S. Cˇ apkun, "Detection of reactive jamming in sensor networks," ACM Trans. Sensor Netw., vol. 7, no. 2, p. 16, Aug. 2010.

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