International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue V, May- 2016

EFFICIENT JAMMING AWARE TRAFFIC DISTRIBUTION FOR MULTIPLE PATH ROUTING USING PORTFOLIO SELECTION

B. SATHIYAPRIYA, IInd ME (CSE),
K.ASHOK KUMAR M.E., Associate Professor/CSE,
M. SAKTHIVEL M.E., (Ph.D.,) Head of the Department/CSE
Sengunthar Engineering College, Tiruchengode, Tamilnadu, India
jegan.san@gmail.com

ABSTRACT

The timing channel is a logical communication channel in which information is encoded in the timing between events. Recently, the use of the timing channel has been proposed as a countermeasure to reactive jamming attacks performed by an energy-constrained malicious node. In fact, while a jammer is able to disrupt the information contained in the attacked packets, timing information cannot be jammed, and therefore, timing channels can be exploited to deliver information to the receiver even on a jammed channel. Since the nodes under attack and the jammer have conflicting interests, their interactions can be modeled by means of game theory. A game-theoretic model of the interactions between nodes exploiting the timing channel to achieve resilience to jamming attacks and a jammer is derived and analyzed. More specifically, the Nash equilibrium is studied in terms of existence, uniqueness, and convergence under best response dynamics. Furthermore, 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.

1. Introduction

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

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

Technical measures like login passwords, anti-virus are essential a secure physical space is the first and more important line of defense. Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present. Human threats are not the only concern. Computers can be compromised by environmental mishaps or physical trauma. Make sure the physical location of your computer takes account of those risks as well. The University's networks and shared information systems are protected in part by login credentials. Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer, if the software provides that capability. Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals. Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer). Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities. Almost all anti-virus have automatic update features. Keeping the "signatures" of malicious software detectors up-to-date is essential for these products to be effective. Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives. CDs/DVDs, or flash drives to store critical, hard-to-replace data. If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

2. Related Work

W.Xu.W.Trappeetal (2014) [1] made a study about theWireless communication is susceptible to radio interference, which prevents the reception of communications. Although evasion strategies have been proposed, such strategies are costly or

ineffective against broadband jammers. Analternative to evasion strategies that involves the establishment of a timing channel that existsin spite of the presence of jamming. The timing channel is built using failed packet reception times. It shows that it is possible to detect failed packet events in spite of jamming. W.Xu.K.Ma.etal (2014) [6] made a study about the 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.

W.Xu.K.Ma. etal (2014) [2] made a study about the Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style at-tacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and consequently, mechanisms are needed that can cope with jamming attacks. D.Yeng etal (2014) [4] made a study about the jamming defense is an important yet challenging problem. The jamming defense problem in the presence of a smart jammer, who can quickly learn the transmission power of the user and adaptively adjust its transmission power to maximize the damaging effect. Consider both the single-channel model and the multi-channel model. By modeling the problem as a Stackelberg game, the optimal transmission power for the user to maximize its utility, in the presence of a smart jammer can be computed.

L.Galluccioetal (2013) [5] made a study about 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 the 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. S.D'Oroetal (2013) [3] made a study about the 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

R.Saranyadevi etal (2013) [6] made a study about the Communication in wireless network is possible with an air medium. Due to the high security threats in the system, the network may face various difficulties. One of the major threats is jamming attack which comes under Denial of Service (DOS) attack. Jamming attack is common among many exploits that compromises the wireless environment. The work of authorized users is by denying service to as legitimate traffic

is jammed by the overwhelming frequencies of illegitimate traffic.

Y.W.Lawetal (2013) [7] made a study about the wireless local area networks that use the Distributed Coordinated Function (DCF) of the IEEE 802.11 Medium Access Control (MAC) protocol, a collision may occur when two or more devices transmit simultaneously. When a collision results in failed reception of a packet, the stations involved increase their back off window, which decreases the probability of transmission and hence that of further potential collision. A jammer trying to disrupt the communications can take advantage of this back off mechanism to reduce the throughput of the system significantly with little energy expense.

3. Security for Wireless Communication

The 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. Several solutions against reactive jamming have been proposed that exploit different techniques, such as frequency hopping, power control and unjammed bits. Continuous jamming is very costly in terms of energy consumption for the jammer. Existing solutions usually rely on users' cooperation and coordination, which might not be guaranteed in a jammed environment. In fact, the reactive jammer can totally disrupt each transmitted packet and, consequently, no information can be decoded and then used to this purpose.

4. Jamming Attack Discovery and Control Model

The motivation of work stems from the concern that if an attacker can program and deploy a general-purpose link-layer jamming network that is able to jam any WSN effectively and energy-efficiently, and if a high entry barrier is not maintained for such a low cost attack, a WSN can never in any practical sense be secure. A counter-argument might be that energy efficiency is no concern to powerful attackers, but even powerful jammers come with a finite energy supply and they would advertise their presence and location if they simply blast away with an exorbitant amount of radio waves this is something a sensible attacker would avoid.

Since the attacker is solely interested in jamming data packets, our first observation is that since data packets are longer than control packets, It can focus on jamming long packets. It can do this by sorting packets according to their length and predict when long packets would arrive. This strategy might not work however because the data packets might be generated spontaneously, rendering our prediction inaccurate, and data packets are sparse, e.g. 1 packet every 5 minutes from each node. Sparse packets require us to observe for a long time before get a working prediction model, and offer us little opportunities to re-adjust our prediction.

The communications between the jammer and the node whose transmissions

are under attack, call target node. Particularly, 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 outflow. As the target node and the jammer have conflicting interests, a game theoretical framework that models their interactions. An investigate both the case in which these two adversaries play their strategies simultaneously and the situation when the target node anticipates the actions of the jammer.

It 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. The interactions between the jammer and the node whose transmissions are under attack, which we call target node. Specifically, 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, it develops a game theoretical framework that models their interactions. In both the case these two adversaries play their strategies simultaneously and the situation when the target node anticipates the actions of the jammer. To this purpose, a study both the Nash Equilibria (NEs) and Stackelberg Equilibria (SEs) of our proposed games.

5. Portfolio Selection Based Jamming Aware Traffic Distribution

The interactions between a jammer and a target node as a jamming game. The existence, uniqueness and convergence to the Nash equilibrium (NE) under best response dynamics. The existence and uniqueness of the equilibrium of the Stackelberg game where the target node plays as a leader and the jammer reacts consequently. The impact of the Stackelberg scenario is to achievable performance of imperfect knowledge of the jammer's utility function. 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. The system is divided into five major modules. They are Network Model, NASH Equilibrium Analysis, Existence of the Nash Equilibrium, Uniqueness of the Nash Equilibrium and Convergence to the Nash Equilibrium.

5.1. Network Model

First module is 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, the malicious node executes a reactive jamming attack on the wireless channel. In the following it refers 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. 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.

5.2. 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 it provide proofs of the existence, uniqueness and convergence to the Nash Equilibrium under best response dynamics.

5.3. Existence of the NASH Equilibrium

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

5.4. Uniqueness Of The NASH Equilibrium

After proving the NE existence in Theorem, let us prove the uniqueness of the NE, that is, there is only one strategy profile such that no player has incentive to deviate unilaterally.

5.5. Convergence to the NASH Equilibrium

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

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 NE, assume perfect knowledge, that is, the target node is completely aware of the utility function of the jammer and its parameters, and thus it is able to evaluate bJ(x). Whereas, if some parameters in the utility function of the jammer are unknown at the target node.

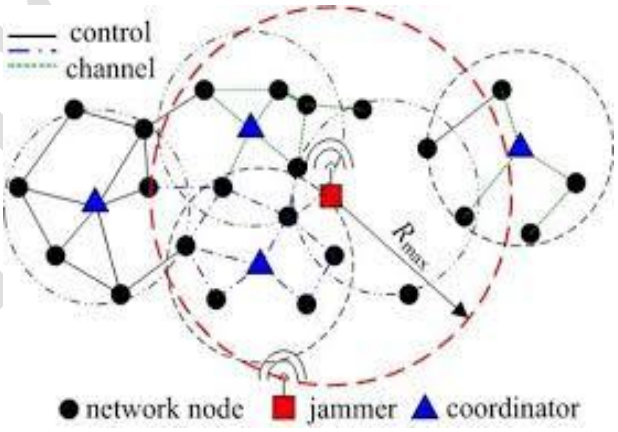

Fig. 1. System Architecture

7. Conclusion and Future Work

A game-theoretic model the interactions between a jammer and a communication node that exploits a timing channel to improve resilience to jamming attacks. Structural properties of the utility functions of the two players have been analyzed and exploited to prove the existence and uniqueness of the Nash Equilibrium. The convergence of the game to the Nash Equilibrium has been studied and proved by analyzing the best response dynamics. Furthermore, as the reactive

jammer is assumed to start transmitting its interference signal only after detecting activity of the node under attack, a Stackelberg game has been properly investigated, and proofs on the existence and uniqueness of the Stackelberg Equilibrium has been provided. Finally, the case of imperfect knowledge about the parameter cT has been also discussed. Numerical results, derived in several real network settings, show 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.

In Future there are many different attack strategies that jammers can perform to disrupt wireless communications. It is impractical to cover all the possible jamming attack models that might exist. In this system addressed the problem of localizing jammers in wireless networks, aiming to extensively reduce estimation errors. The jammers could be several wireless devices causing unintentional radio interference or malicious colluding jamming devices who coexist and disturb the network together. Most of the existing schemes for localizing jammers rely on the indirect measurements of network parameters affected by jammers, for example, nodes' hearing ranges, which makes it difficult to accurately localize jammers. Localizedjammers by exploiting directly the JSS. Estimating JSS is considered challenging because they are usually embedded with other signals. Our estimation scheme smartly derives ANFs as the JSS utilizing the available signal strength measuring capability in wireless devices. The scheme samples signal strength regardless of whether the channel is busy or idle and estimates the ANF by filtering out regulartransmission to obtain the JSS.

References

[1] Yang.D, Xue.G, Zhang.J, Richa.A and Fang.X, "Coping with a smart jammer in wireless networks: A Stackelberg game approach," IEEE Trans. Wireless Commun., vol. 12, no. 8, pp. 4038–4047, Aug. 2014.

[2] Anand.S and Chandramouli.R, "An attack-defence game theoretic analysis of multi-band wireless covert timing networks," in Proc. IEEE INFOCOM, 2010.

[3] Morabito,G "Exploiting the timing channel to increase energy efficiency in wireless networks," IEEE J. Sel. Areas Commun., vol. 29, no. 8, pp. 1711–1720, Sep. 2012.

[4] Poisel.R, Modern Communications Jamming Principles and Techniques. Norwood, MA, USA: Artech House, 2014, ser. Artech House information warfare library.

[5] Saranyadevi.R, Shobana.M and Prabakar.D, "A survey on preventing jamming attacks in wireless communication," Int. J. Comput. Appl., vol. 57, no. 23, pp. 1–3, Nov. 2013.

[6]Wang.B, Wu.Y, Liu.K.R and Clancy.T.C., "An anti-jamming stochastic game for cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 29, no. 4, pp. 877–889, Apr. 2013.

[7]Xu.W, Ma.K, Trappe.W and Zhang.Y, "Jamming sensor networks: Attack and defense strategies," IEEE Netw., vol. 20, no. 3, pp. 41–47, May/Jun. 2014.