ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Game Theoretical Analysis of Exploiting Timing Channels to Overcome Jamming

C.Gowdham[1], E.Praveen[2], B.Gari Gabreil [3]

Assistant Professor, Department of CSE, Karpaga Vinayaga College of Engineering and Technology, Chennai, India[1]

UG Students, Department of CSE, Karpaga Vinayaga College of Engineering and Technology, Chennai, India[2,3]

ABSTRACT: Jammers are the devices that give out high energy signals with the purpose of disrupting wireless communication between the systems it is the nature of wireless medium which allows the intentional attacks like jamming. jamming is also known well by the name 'Denial of Service Attacks'. They have applications in many places where wireless communication needs to be prohibited. They may be used with a malicious intention also, for intentionally disrupting the wireless communication system in a particular area.

A timing channels is a logical communication channel which exploits the time interval between alternative transmissions to encode information this covert channels creates a capability to communicate in the channels where the communication is restricted.This project proposes a method to overcome the potential threat posed by jammers on wireless communication, by employing the timing channel for communication. Furthermore, this project models this scenario based on the concepts of Game Theory, and goes on to prove that a Nash Equilibrium as well as stackelberg Equilibrium exist here, where the target node is the 'leader' and the jammer node is the 'follower'.

The proposed system exploits a weakness of reactive jammers, that they send the jamming signal only when they have detected the presence of some kind of traffic on the wireless channel. The proposed system has the considerable advantage that it can be used for transferring some information even when all the packets sent by the target node are disrupted by the jammer

I. INTRODUCTION

A timing channel is a communication channel which exploits silence intervals between consecutive transmissions to encode information[1]A covert channel states that "a channel that exist,mutually opposite to design, in a computer system" [8]. Recently, use of timing channels has been proposed in the wireless communication domain to support low rate,energy-efficient communications[2],[3] as well as Timing channel and resilient communications.[4],[5].

In this paper we focus on the resilience of timing channels to the reactive jamming attacks[6],[7]. In general, these attacks can completely disrupt communications when the jammer continuously emits a very high power disturbing signal, i.e., when continuous jamming is performed. However, continuous jamming consumes lot of energy for the jammer. This is the reason why in most scenarios characterized by energy constraints for the jammer, e.g., when the jammer is battery powered, non-continuous jamming such as reactive jamming is considered.

In this case the jammer continuously listens over the transmission channel and begins the transmission of a high energy disturbing signal as its detects an going transmission activity. Effectiveness of reactive jamming has been demonstrated and its energy analyzed. Timing channels are more although not totally immune from reactive jamming attacks. In fact, the interfering signal begins its disturbing action against the communication channel only after identifying an on going transmission, and thus after the timing information has been decoded by the receiver.Target node and Jammer working is clearly explained in Figure 1.

In this paper we analyze the communication between the jammer and the target node whose transmissions are under attack, which we call target node. we consider that the target node wants to maximize the amount of information that can be transmitted of time by means of the Timing channel.whereas,the jammer wants to minimize such amount of information while decreasing the energy expenditure. The target node and the jammer have conflicting interests, we develop a game theoretical framework that models their communication. We investigate both the case in which these two adversaries play their strategies continously, and the situation when the destination node (the leader) anticipates the actions of the jammer (the follower).

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

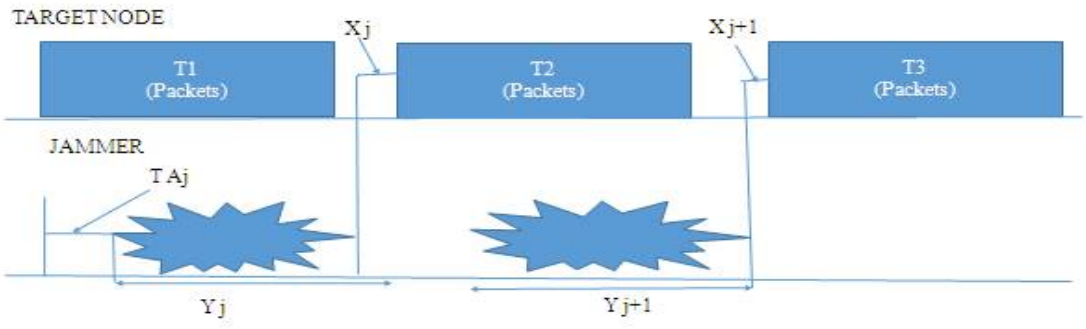

Figure 1: Interaction between Target node and Jammer

we study both the Nash Equilibrium(NEs) and Stackelberg Equilibrium (SEs) of our proposed games. the Node formation between target node and jammer is explained clearly in Figure 2. The main contributions of this paper can be therefore Explained as follows:

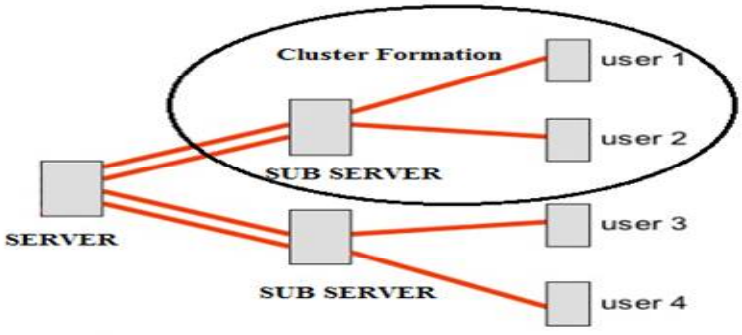

Figure 2:Node Formation

1) We model the interactions between jammer and the target node as a jamming game

2) 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 follower

3) we investigate in this latter Stackelberg scenario the impact on the achievable performance of knowledge of the jammer's utility function

4) we conduct an extensive numerical analysis which explains that our proposed models well capture the important factors behind the utilization of timing channels, thus representing a framework for the design and verifying

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

of such systems.

II. WORKING PRINCIPLE

The target node establishes a covert channel that exploit the silence period between the end of an attack and the beginning of a packet transmission to counteract an ongoing jamming attack.We study both the Nash Equilibrium and Stackelberg Equilibrium. Furthermore, we compare the achievable performance of each node, and find that the SE dominates the NE, thus allowing each player to improve its own utility. The target node is able to transmit covert information even if the continous jammer has successfully disrupted all the bits contained in a packet. By exploiting our proposed timing channel implementation, it is possible to transmit some data even when the jammer has successfully corrupted each packet.

III.GAME MODEL

The hypothetic methods have two wireless nodes, a transmitter and a receiver, want to communicate, while a harmfull node aims at their communication. To this purpose, we assume that the harmfull node executes a reactive firry attack on the wireless channel. In the following we refer to the harmfull node as the firry, Ja. and the transmitting node under attack as the destination node, Ta.

The firry method senses the wireless channel continuously. Upon identfying a possible link-up activity performed by Ta, Ja starts executing firry signal. we indicate as TAJ the duration of the time interval between the beginning of the packet transmission and starting of the firry signal emission. The time taken of the structural color signal emission that jams the transmission of the j-th packet can be modeled as a repeatable random variable. To maximize the uncertainty on the value of Yj , we assume that it is exponentially distributed with mean value y.

We clear that there is no attack is performed the target node communicates with the receiver by applying traditional transmissions schemes. In the next method, when it realizes to be under attack, it exploits the timing channel to transmit part of(or all) the information.3 The latter is encoded in the duration of the interval between the instant when the jammer Ja terminates the emission of the jamming signal and the beginning of the transmission of the next packet. Hence, it is possible to consider a fourier time axis and refer to each timing channel utilization by means of an integer index j.

The silence period durations scheduled after the transmission of the j-th packet and the corresponding firry signal can be explaned as a continuous random variable, X j , uniformly distributed4 in the range [0, x].The amount of data executed per each use of the timing channel depends on the value of x and the precision Δ of the clocks of the sharing nodes as shown in [2]. In our model we assume that the parameters Δ and T AJ which are hardware depends are known a-priori to both the destination node and the firry, whereas the strategies x and y are estimated by means of a training phase. This is consistent with the complete data assumption which is common in game theoretic frameworks.

In our model we assume that firry is energy-constrained, e.g., it is battery powered; hence, its choice of y (i.e., the time taken for the signal emission that jams the packet transmission) stems from a trade-off between two requirements, i.e.,

i)Reduce the amount of information that the target node Ta can transmit to the perspective receiver, and
ii) Keep the energy exploitation as low as possible.
Observe that requirement
i) would result in the selection of a high value for y, whereas requirement
ii) would result in a minimum value for y.

On the other hand, the target node has to properly choose the value of x (i.e., the high silence period of time scheduled following the transmission of the j-th packet and the subsequent firry signal) in order to maximize the achievable capacity C (x, y), i.e., the amount of information that can be sent by means of the timing channel, while reducing its energy exploitation. Therefore, it is reasonable to consider that the values of x and y represent the strategies for the target node Ta and the fiiry Ja, respectively.

Accordingly, the set of strategies for both players, S Ta and S Ja, can be defined as the set of

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

all the feasible strategies x and y, respectively. The utility set of the game is defined as U = (U Ta, U Ja),where UT and UJ are the utility functions of the target node and the firry, respectively. As already said, the target node aims at maximizing its own achievable capacity, C (x, y) while also reducing its energy exploitation. The firry, on its side, aims at reducing the capacity achieved by the target node by generating interference signals, whose duration is y(in average), while keeping its own energy consumption low. Accordingly, the utility functions U Ta(x, y) and U Ja (x, y) to be maximized are defined as follows:

UTa (x, y) = +C(x, y) − cTa∗ · TP · PT

UJa(x, y) = −C(x, y) − cTa · y · P

PT and PJ are the transmission power of the destination node and the firry, respectively, TP is the duration of a transmitted packet in seconds, c Ta and c T are positive transmission costs expressed in [bit/(s · J)] which weight the two contributions in the utility functions and therefore, in the following will be referred to as weight parameters. Note that while the energy consumption of the firry varies as a function of the strategy y of the jammer itself, on the contrary the energy consumption of the destination node during a cycle only depends on the duration TP of the packet and not on the strategy.

Furthermore, a low value of c Ta means that the jammer considers its jamming effectiveness more important than its energy consumption, while a high c Ta value indicates that the jammer is energy-constrained and as a consequence, it prefers to save energy rather than minimizing the capacity of the destination node. We observe that cT = 0 models the case of continuous firry without any energy constraint which is of limited interested and out of the scope of this paper since we see the trade-off between the achievable capacity and the consumed energy. We note that U Ta (x, y) increases when x increases until reaches a threshold after which the service function starts decreasing. This is due to the fact that, when x is higher than sucha brink, the silence time is large enough to cause an increase in the transmission delay and, consequently, a reduce in the explotiation capacity. This is a well known result in timing channel communications [2]. In Fig. 2 we also note that the achievable performance notice able depends on the firry signal duration y.

In fact, when y increases, the capacity of the destination node decreases as the firry attack forces the transmitter in delaying its timing channel communications by increasing x. Fig. 3 shows the impact of the energy consumption on the achieved by the node. As expected, the higher the product cTa. P is, the lower the achieved utility is. Note that, as the energy exploitation in any cycle is constant and does not depend on either x or y, the energy cost of the target node UTa (x, y) would only result in a slight shift in the utility function of the target node.

IV.NASH EQUILIBRIUM

We can say that Nash Equilibrium exists when neither p of players can benefit from changing their strategies. That is i.e,

$\forall(x , y) \in S,$

$UTa (x^* , y^*) \; UTa (x , y^*)$

$UJa (x^* , y^*) \; UJa (x^* , y)$

thus, (x^* , y^*) is a strategy profile where no player is in centiveto deviate unilaterally.

V.STACKELBERG EQUILIBRIUM

In a Stackelberg Game, one of the players acts as the leader by anticipating the best response to the follower. In our scenario, the firry plays its strategy when a communication from the destination node is detected on the list channel. Thus it is natural to assume that the target node acts as the leader and the firry as the follower. So, given the strategy of the target node, the firry will play the strategy that high its service. This hierarchical structure of the game allows the leader service which is at least equal to utility achieved in the ordinary game at Nash Equilibrium, if we assume perfect knowledge, that is, the destination node is completely aware of the service function of the firry and its parameters, and thus it is able to evaluate the best response of the firry. In the case of perfect ability, there is a unique Stackelberg Equilibrium for any value of the weight parameter, and it can be demonstrated that the target node can inhibit the jammer under perfect knowledge assumption.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

VI.CONCLUSION

Here, we have tried to analyze the case of a reactive jammer trying to stop the communication between two nodes in a network.And also tried to optimize the rate of transmission between the two nodes involved in the transmission. Modeling the situation based on Game Theory, we have proved that this scenario can be treated as an example of non-cooperative gaming, and a Nash Equilibrium as well as Stackelberg Equilibrium exist in this competition between the jammer and the communicating node. Using this model, we have proved that it is possible for the target node to communicate with another node even in the presence of the jammer.

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 ACMConf.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] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," IEEE Netw., vol. 20, no. 3, pp. 41–47,May/Jun. 2006.
[7] 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.
[8] I. S. Moskowitz and M. H. Kang. Covert Channels — Here to Stay?, Proc. of COMPASS, S. Margherita, Italy, Jun.-Jul. 1994.