Security Analysis of Cognitive Radio Netwoks Using Game Theory

Ajay Singh
Deptt. of Electronics and Communication Engg.
National Institute of Technology
Hamirpur, India
E-mail: ajaysingh@nith.ac.in

Ritu Rana
Deptt. of Management and Humanities
National Institute of Technology
Hamirpur, India
E-mail: riturana2222@gmail.com

***Abstract*—In this paper, a cognitive radio network is considered where Alice wants to send confidential information to the Bob in the presence of primary user and eavesdropper. Effect of number of antennas in Bob and eavesdropper is discussed using the game theory. It is observed that number of antennas in Bob improves the security of the system.**

***Keywords*—cognitive radio, security, game theory, Nash equilibrium.**

I. INTRODUCTION

Apart from accruing great benefits from the network technologies applications, users encounter challenges of network security also. Networks are a convenient way to access information and provide a sufficient communication channel to users. At the same time, networks also have several security issues, namely: cyber crimes, internet attacks, flooding Denial of Service (DoS) attacks, illegal data access, etc. Public institutions or private entities can lose financial status, important data, and even their reputations as a cause of network attacks. Reports of new hackers, cyber crimes, and cyberspace incidents [1], [2], [3] indicate that network security is a challenging task. The conventional solutions to network security face several flaws. The implementation of these conventional solutions include: employing of a preventive device (e.g. firewall) or a reactive device (e.g. anti-virus program) or using both together. But, these conventional solutions are no longer sufficient to counter network attacks. Intrusion Detection Systems (IDSs), which are reactive devices, have become a necessary addition to every organization's security due to increasingly severe types of attacks in recent years [4]. An IDS is a software or hardware system that is used to monitor events occurring in a network or computer system; an IDS is also used to analyze these events in order to determine whether an attack has occurred using such methods as attack signature identification, pattern detection, and statistical analysis [5].

This work was supported in part by SERB, DST, Government of India, for the Project "Physical Layer Security of Cognitive Radio Networks." (Project Ref. no. : YSS/2015/001738).

Some types of IDSs are capable of reacting to a detected attack without notifying the administrator [6], and such reacting IDS are called Intrusion Prevention Systems (IPSs). Two weaknesses of IDSs are that they are not very sophisticated and that they rely on ad hoc schemes and experimental work [7]. Due to these, IDSs need design tools to handle sophisticated, organized attackers. Many researchers have proposed Game theoretic approaches to enhance network security. The insufficiency of conventional solutions to network security is the cause for lack of a quantitative decision framework [8].On the one hand, game theory is a mathematical tool to analyze the strategic interactions among multiple decision makers [12] that compete with each other. It can provide a mathematical framework for modeling and analyzing network security problems. Game theory is also capable of analyzing several possible scenarios before determining an appropriate course of action [9]. This greatly helps an administrator in decision making. On the other hand, security measurement [10] is an important part of network security as it evaluates integrity, confidentiality, vulnerability, availability, and security risks. Every aspect of network security is measured in network security measurement. Risk assessment [11] is one of these measures. In the words of [13], network security measurements involve the interactions of attackers and defenders, and the result of a measurement can be affected by their interactions. For example, one of the metrics in risk assessment for a network system is the probability of it being attacked. There is a need to predict the actions of both the defenders and the attackers. Since the interaction process between attackers and defenders is a game process, game theory can be applied in every possible scenario to predict the actions of the attackers and then to determine the decisions of the defenders. Therefore, game theory-based solutions have been proposed for network security problems.

II. Game Theory And Nash Equilibrium

A. Game Theory

Game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers". In some respects, game theory is the science of strategy, or at least the optimal decision-making of independent and competing actors in a strategic setting. The key pioneers of game theory were mathematicians John von Neumann and John Nash, as well as economist Oskar Morgenstern.

The concept of "game" simply means any interactive situation in which independent actors share more-or-less formal rules and consequences. The formal application of game theory requires knowledge of the following details: the identity of independent actors, their preferences, what they know, which strategic acts they are allowed to make, and how each decision influences the outcome of the game. Depending on the model, various other requirements or assumptions may be necessary. Finally, each independent actor is assumed to be rational.

B. Nash Equilibrium

In economics and game theory, Nash Equilibrium is a stable state of a system involving the interaction of different participants, in which no participant can gain by a unilateral change of strategy if the strategies of the others remain unchanged. 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 their own strategy.

III. System Model and Hypothesis Formulation

Based on the basic concept of Game theory and the related Nash Equilibrium, a model of two receiver antennas and one transmitter case can be formulated as follows:

A. The Model

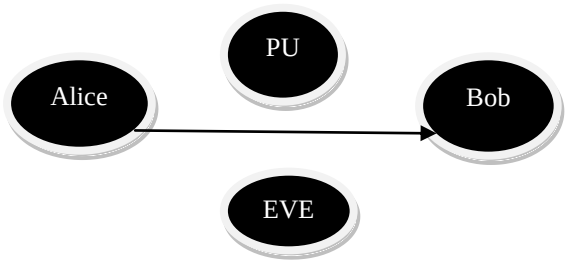

Fig 1: The Model

Assume a situation where there are two players with different numbers of antennas, namely, Bob (with N_B number of antennas) and Eve (with N_E number of antennas) and both being aware of each others' strategy to increase or decrease the number of antennas to acquire significant amount of information. They try to receive information signals transmitted through only one transmitter, namely, Alice in the presence of primary user (PU). Assume that the motive of Alice's transmission is to send the information to Bob only but Eve is also a key player as a security threat to both Alice and Bob's information exchange.

This situation gives rise to the introduction of game theory for determining the number of antennas that Bob should use in order to minimise the security threat that both Alice and Bob may face caused by Eve's interest in stealing the information transmitted.

The model can be illustrated easily with the help of Fig.1.

To tackle this situation, a hypothesis can be formulated as follows:

B. The Hypothesis

The Null Hypothesis for Bob to minimise the security threat is to have an appropriate number of antennas (N_B) which is higher than that of the number of antennas used by Eve (N_E). Considering this in mind, the null hypothesis in this case thus becomes:

$$H_0: N_B > N_E$$

Alternatively, if this hypothesis is not satisfied, we will have the alternative hypothesis that Eve gets success in stealing the information. In this case, the number of antennas that Eve is using (N_E) will be greater than that of the number of antennas Bob is using (N_B). Based on this information, the alternative hypothesis in our case becomes:

$$H_a: N_B < N_E$$

IV. Nash Equilibrium in CR Network

Based on the system model and the hypothesis, Nash equilibrium in our case can be achieved as shown in Table 1.

Table 1: Nash Equilibrium in CR Network

		Eve	
Bob	Number of Antennas	More	Less
	More	[1]Fair	[2]**Good**
	Less	[3]Poor	[4]Fair

Table 1 indicates that Nash equilibrium can be achieved in case 1 i.e., when both the players have same number of antennas but our Null hypothesis (H_0) can be achieved in case 2 i.e., when $N_B > N_E$. If this is not the case, the alternative hypothesis holds true.

V. Conclusion

A cognitive radio network is considered where Alice wants to send confidential information to the Bob in the presence of primary user and eavesdropper. Effect of number of antennas in Bob and eavesdropper is discussed using the game theory. It is observed that number of antennas in Bob improves the security of the system.

References

[1] "Security focus," security focus bugtraq vulnerability notification database, 2009. Available: http://www.securityfocus.com/archive.

[2] "US-CERT," United States Computer Emergency Readiness Team, 2009. Available: http://www.us-cert.gov.

[3] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, "A Survey of Cyber Crimes," (Wiley Journal of) Security and Communication Networks, Vol. 5, No. 4, pp. 422-437, Apr. 2012.

[4] R. Bace and P. Mell. Intrusion detection systems. NIST Special Publication on Intrusion Detection Systems. Available:http://www.snort.org/docs/nist-ids.pdf.

[5] T. Alpcan and T. Baser, "A game theoretic analysis of intrusion detection in access control systems," Proc. 43rd IEEE Conference on Decision and Control, Vol. 2, pp. 1568-1573,2004.

[6] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem,". IEEE Conference on Descision and Control, pp. 6283-6288, 2006.

[7] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," In Proc. IEEE International Conference on Computer Communications (INFOCOM), pp. 1307 - 1315, 2007.

[8] T. Alpcan and T. Baser, "An intrusion detection game with limited observations," Proc. 12th Int. Symp. on Dynamic Games and Applications, 2006. Available: http://www.tansu.alpcan.org/papers/isdg06.pdf.

[9] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "The role of game theory in information warfare," Proc. 4th information survivability workshop (ISW-2001/2002), 2002. Available:http://www.cert.org/research/isw/isw2001/papers/index.html.

[10] Security measurement- white paper, http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaperv3.0.pdf.

[11] W. He, C. Xia, H. Wang, C. Zheng, and Y. Ji, "A game theoretical attack-defense model oriented to network security risk assessment," 2008 International Conference on Computer Science and Software Engineering, pp. 498 - 504, 2008.

[12] K. J. Ray Liu and B. Wang, "Cognitive Radio Networking and Security: A Game-Theoretic View,"Cambridge University Press, pp.47, 2010.

[13] X. Liang and Y. Xiao, "Game Theory for Network Security," IEEE Communications Surveys & Tutorials, Vol. 15 (1), pp. 472-486, 2013.