The Nucleus ***54****, No. 4 (2017) 214-218*

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Quantum Bayesian Game Modeling for Intrusion Detection

S. Munawar[1,2]*, M. Hamid[1,3] and S. A. Lodhi[1]

[1]*School of Computer Science, National College of Business Administration & Economics, Lahore, Pakistan*

[2]*Department of Computer Science, Virtual University of Pakistan, Lahore, Pakistan*

[3]*Department of Statistics and Computer Science, UVAS, Lahore, Pakistan*

ARTICLE INFO

Article history :
Received : 02 October, 2016
Accepted : 22 December, 2017
Published : 31 December, 2017

Keywords:
Anomaly intrusion detection,
Classical game theory,
IP packet analysis,
Quantum game theory,
Cyber security,
Bayesian game,
Cognition

ABSTRACT

In cybersecurity, intrusion detection plays a vital role in network boundary detection. It develops preventive measures for network defense. In this paper, quantum cognition with game theory strategy is presented to detect target attacks and normal packet classification in the network. The Quantum Bayesian game theory offers an efficient model of cognition to human rationality rather than classical Bayesian game theory. This is inspired cognitive defense model in which game modeling acts as the brain to determine abnormal activity of network traffic rationally. It also analyzes the operation of the quantum game model between attacker and defender detection system. The defender takes effective decision strategy in this model which maximizes their payoffs, according to non-cooperative and incomplete imperfect information game strategy. Our modeling emphasized that quantum game theory is the effective dynamic solution, as a procedure of two player game to improve the probability of a defender issuing a correct alarm and reduced the probability of defender issued a false alarm. This modeling is effective as well as establishes a rapid response of the system that uses in real time reconfiguration network security system.

1. Introduction

The predictive model is built to classify the IP (Internet Protocol) abnormal packet activity for intrusion detection. It is still improving through different techniques such as machine learning, information theory, data mining, spectral and theory statistics [1].

Game theory offers mathematical model to consider decision making, conflict strategy, cooperation, and non-cooperation between rational decision maker's agents. Quantum game theory is different from classical game theory in primary ways, such as initial states, superposition, and entanglement and strategies states. Generally, it is the extension of classical game theory.

Quantum game theory is more efficient due to entanglement, which allows communication of less information in order to play games. It is employed in different fields such as designing of cybersecurity and constructing new quantum algorithms [2]. Quantum game theory is used to develop and create algorithms of quantum theory for modeling as human cognition abilities such as decision making, knowledge management, judgment, superposition and entanglement of information processing as does the human brain. It is based on a quantum prototype that brain-like functionality and information processing can be performed according to the mathematical design model of cognition. It is based on information and probability theory related to quantum. It led to advance the model and supplanted traditional classical probability theory [3, 4].

Bruza et al. [5] described the comparison of Bayesian and quantum models of cognition. They found that quantum models are more efficient work in decision making and judgment as compared to Bayesian models. It also discussed issues of quantum cognitive processes. Pothos and Busemeyer [6] explained empirically the importance of quantum probability that it provides cognitive modeling in new ways. Penrose [7] discussed that the physical quantum system establishes the human mind with its decisions and actions. It is also modeled according to the laws of quantum mechanics. This led to a quantum game theory in which players like an agent is supposed to execute action /decisions. The decision of the quantum player generally renovates qubit vectors.

The primary objective of this paper is how to improve the probability of defender issuing a correct alarm and reduce the probability of defender issued a false alarm to make rapid response to the system. It is based on a Bayesian game model which can define different types of attacks on the network. In practical formulation, quantum cognition based IDS (Intrusion Detection System) /defenders determine the value of the payoff. It also shows their effectiveness using quantum Bayesian game strategy.

2. Background

Furthermost IDS manages network traffic according to different preventive system. It is enforced on different locality of network traffic such as, it is tied to network hosts, hub, WAN backbone, network perimeter, server farms, network switch and LAN backbones. Signature or

*Corresponding author : saima.munawar@vu.edu.pk

misuse detection and anomaly detection are two basic types of detection system [8]. Due to its theoretical potential, it is generally used in academic research for addressing new attacks [9]. The basic purpose of anomaly detection is to know about the different kinds of attackers and to know about the behaviour of the attackers [10].

Game theory offers mathematical model to examine the decision making strategy for a decision maker's agent. The agents are used as players in the game, the probability of an agent's action, specify the strategy that player within the game can take actions such as pure strategy and mixed strategy. Pure strategy is playing with given number of moves and mixed strategy is used to select the moves randomly. Later this action strategy, players are moved due to positive and negative rewards; by using the payoff matrix. It gives the mathematical value of each player according to their strategies. The basic purpose of player is that he wants to optimize the payoff/ utility within the principles of the game. Game theory has different types such as symmetric and asymmetric, cooperative or non-cooperative, combinatorial, discrete and continuous, infinitely long games, perfect and imperfect information, stochastic outcomes, zero-sum, nonzero-sum, many-player, simultaneous, sequential, metagame, population games and differential games. Game theory is applied in different fields of philosophy, modeling logic of computer science, normative analysis, business, biology, economics and political science [2].

Harsanyi introduced Bayesian game as a model, which describes the nature of the player in a game and the payoff /utility of information about the characteristics of the other player is incomplete and imperfect. The author described the nature assigns a random value to each player according to the type of player and such kind of player determine the payoff or utility functions of the other player [11].

Shen et al. [12] presented different game theory solutions for cyber security, which has provided the survey taxonomy of network security issues through game theory approaches and applications. He discussed the work done earlier to demonstrate that which type of game theory is applied to different categories of network security issues such as DOS (Denial of Service) attacks, intrusion detection, strengthening security, malicious sensor nodes. Some beneficial research areas or issues for further direction regarding WSN (Wireless Sensor Network) have been suggested. Anuvarsha and Rajesh [13] presented a survey related to automatic intrusion response system through fuzzy game and zero-sum game theoretical approach. It also provided the current issues of network security. It is beneficial discuss about existing games used in network security perspectives in terms of analysis of player strategy, methods of games and analysis of game equilibrium.

Liu et al. [14] presented a Bayesian game approach for detection of intrusion detection, which is deployed in wireless adhoc networks. They described the Nash equilibrium strategy for the defender game in both static and dynamic game situations and without complete information. The authors claimed in this Bayesian model to save significant energy and minimize the hidden attacker damages. They also discussed in another work [15] about mixed strategies for efficient detection of an intrusion by both zero-sum and non-zero-sum game modeling.

Poongothai and Jayara [16] also describe the non-cooperative and non-zero sum game method for intrusion detection in MANET. They presented the payoff matrix for detecting the misbehavior of attacker in both static and dynamic states. They also analyzed game theory strategy which is used to find optimal actions and diagnose the steady consequences. Otrok et al. [17] also described unified framework for detecting the intruders through cooperative and non-cooperative game strategy with incomplete information. The authors discussed that framework was beneficial for detecting intrusion in MANET. Marchang and Tripathi [18] also presented the deployment of Intrusion Detection System (IDS) through the non-cooperative game approach in MANET. They have mainly focused on general IDS which are to determine the optimal deployment strategy.

Quantum game theory is different from classical game theory in these primary ways, such as initial states superposition, entanglement and strategies states. Albert Einstein stated that "God does not play dice with the universe," he was speaking about a planned work as a form of dice, laws of nature and superposition state. Quantum game theory includes the source of two qubits for each player, manipulation of qubits and determines the state of qubits through the measurement device. Quantum game theory is more efficient due to less need for information to be exchanged. It is also a useful design of quantum algorithms, quantum cryptography and quantum computing. Quantum game theory is practiced as general construction of protein folding and electrons can be seen as a survival game and prisoner game can be viewed as bacteria colonies. It is likewise applied in economic theory, diplomacy and secure communications [3, 19].

Recently Blunter and Graben [20] have presented a resolution of several puzzle games of bounded rationality using quantum cognition probabilities, but they do not supply the explanation and deeper apprehension of these puzzles because it can be simply fitted to data empirically and it is unnecessary to explain in depth. They also discussed the prima facie evidence that may be helpful for future assumptions of quantum cognition. There are two practical ways to formulate probabilistic mathematical models of cognition that is either connected to classical probability theory or quantum probability theory. Referable

to the resource limitation and computational cost using traditional probability theory, quantum cognitive models using quantum probability theory may offer optimal results with less computational cost [21].

3. Proposed Game Modeling

Analysis of intrusion detection system through quantum game theory has been demonstrates. This approach basically provides decision analysis and patterning. IDS addresses network issues such as model of attack, action and the response to decision analysis of potential threats [22-26]. Classical Bayesian game theory strategies have been used with quantum cognition for the first time here. Quantum strategy gives beneficial results as compare to classical strategy [27, 28]. This method addressed the interaction between two players which are the defender and attacker as a non-cooperative Bayesian game. This method/model gives the analysis of the behaviour of these players based on decision and detection processes. IDS is the monitoring process in which analysis of attackers and intruders events of network environment are performed. It is shown as diagram in Fig. 1.

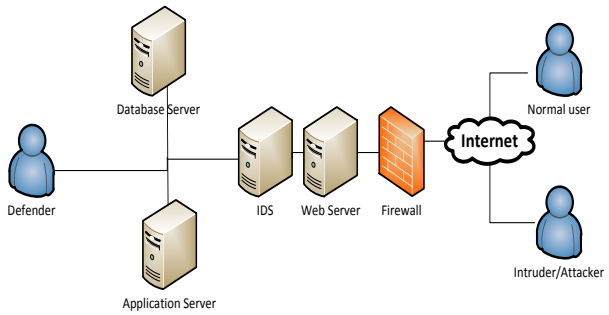

Fig. 1: Monitoring process of IDS in a network environment

The whole work is divided into these main processes which are

1. Classical Bayesian game theory, modeling for intrusion detection.
2. Quantum Bayesian game theory, modeling for intrusion detection.

3.1 Classical Bayesian Game Theory, Modeling for Intrusion Detection

Non-cooperative Bayesian game includes the action sets of players, the strategy of each player; specifies the type of player, beliefs and payoff utility functions for every participant. The strategy is the plan of action to take and type for every player by beliefs. The other player's type is shown by player uncertainty, according to the beliefs of the player and these beliefs are used as another player's probability with the type of player.

Defence modeling of intrusion detection Bayesian game looks like the following, using Eqs. 1 to 6, respectively.

$$\text{Two players } N = \{1,2\} \tag{1}$$

Action sets of player 1: $A_i = \{Defend, \sim Defend\}$,

$$\text{Player 2: } A_t = \{Attack, \sim Attack\} \tag{2}$$

Types sets of player1 is $\varphi_1 = \{Defender\}$ and player 2 is

$$\varphi_2 = \{Attac\,\text{ker}, Normal\} \tag{3}$$

Payoff utility functions: u_i: Actions, A × type, Ø→return payoff, R

$$u_i = \{A \times \phi \to R\} \tag{4}$$

Belief of players:

Player 1: $\{(\varphi_1 = Defender|\varphi_2) = p(probability)\}$,

Player 2 : $\{(\varphi_2 = Normal|\varphi_1) = 1-p\}$

$$\&\ (\varphi_2 = Attac\,\text{ker}|\varphi_1) = p \tag{5}$$

A mixed strategy of player 1,

$$S_i = Defender \to Defend|\sim Defend$$

and player 2,

$$S_i = Attac\,\text{ker} \to Attack|\sim Attack \tag{6}$$

The payoff matrix of two players is granted as the normal form Bayesian game of intrusion detection as shown in Table 1.

Table 1: Payoff matrix of intrusion detection game

Player 2 / network traffic	Action space		Player 1 (Defender/IDS)	
			Defend	Not Defend
Intruder/ Attacker/ abnormal behavior	Attacks [20]	Back Buffer_overflow FTP_write Guess_passwd Imap Ipsweep Multihop Neptune Nmap Phf Pod Portsweep Rootkit Satan Smurf Teardrop Warezclient Warezmaster	-1,1	1,-1
Normal behavior	Not attack		1,-1	1,1

In this matrix, the payoff mentions the players, action space of each player. The payoff is given according to the probability of defender and attacker. If defender successfully defends the attacks, the payoff utility given to the defender is 1 otherwise loss for missed attacks is -1. If an attacker successfully attacks the system, the payoff utility given to the attacker is 1 otherwise loss attack by defending is -1.

3.2 Quantum Bayesian Game Theory Modeling for Intrusion Detection

The Quantum Bayesian game sets the initial states, superposition, entanglement and strategies. Defense modeling of intrusion detection quantum Bayesian game looks like the following:

1. Players are indicated by state vector |ψ⟩
2. Player 1 is as (defender), with vector notation expressed as |ψ⟩
   |Defend⟩ and |not Defend⟩ is a linear combination vector and these two vectors are two-dimensional space vectors. There are two constants 'a & b' called amplitudes and have two possibilities such as defend or not defend in a superposition state as given in Eq. 7.
   $$\left|\psi\right\rangle = a\left|Defend\right\rangle + b\left|\sim Defend\right\rangle \quad (7)$$
3. Player 2 is as (Intruder/Attacker), their vector notation expressed as |ψ⟩
   |attack⟩ and |not attack⟩ state vectors is a linear combination vector and these two vectors are two-dimensional space vectors. There are two constants 'a' and 'b' called amplitudes and have two possibilities such as attack or not attack in a superposition state as given in Eq. 8
   $$\left|\psi\right\rangle = a\left|attack\right\rangle + b\left|\sim attack\right\rangle \quad (8)$$
4. Suppose that the probability of defender has a particular property which depends on the projection of |ψ⟩ and it onto the subspace corresponding to the property using Eqs. 9 to 14 respectively.

The probability reduces in to Eq. 9.

$$\left\|P_{defend}\left|\psi\right\rangle\right\|^2 = |a|^2 \; or \left\|P_{\sim defend}\left|\psi\right\rangle\right\|^2 = |b|^2 \quad (9)$$

5. Probability that player1 is defending, certainty Player is defender means the state vector is
   $$\left|\psi_{defender}\right\rangle = P_{defender}\left|\psi\right\rangle / \left\|P_{defender}\left|\psi\right\rangle\right\| \quad (10)$$

Therefore,

$$\text{Prob}\left(defend\left|defender\right.\right) = \left\|P_{defend}\left|\psi defender\right\rangle\right\|^2 \quad (11)$$

This leads to

$$\text{Prob}\left(defender \wedge defend\right) = \left\|P_{defend}P_{defender}\left|\psi\right\rangle\right\|^2 \quad (12)$$

$$\text{Prob}\left(\sim defend\left|defender\right.\right) = \left\|P_{\sim defend}\left|\psi defender\right\rangle\right\|^2 \quad (13)$$

This leads to

$$\text{Prob}\left(defender \wedge \sim defend\right) = \left\|P_{\sim defend}P_{defender}\left|\psi\right\rangle\right\|^2 \quad (14)$$

6. The operation of tensor product is used for compatible outcomes of vector space regarding defending, written as given Eq. 15
   $$\left|D\right\rangle = d\cdot\left|defend\right\rangle + d^{'}\cdot\left|\sim defend\right\rangle \quad (15)$$

The player is defending or not this state vector shows and allows to compute this probability. Likewise, the operation of tensor product is used for compatible outcomes of vector space regarding attacker, written as given Eq. 16,

$$\left|A\right\rangle = e\cdot\left|attack\right\rangle + e^{'}\cdot\left|\sim attack\right\rangle \quad (16)$$

As long as possible compatibility of attack and defend which are *|D⟩* and *|A⟩,* the tensor product between both is given by Eqs. 17 and 18, respectively

$$\left|\text{Product State}\right\rangle = \left|D\right\rangle \otimes \left|A\right\rangle \quad (17)$$

$$\begin{aligned} &= d\cdot e\left|defend\right\rangle \otimes \left|attack\right\rangle + d\cdot e^{'}\left|defend\right\rangle \otimes \\ &\left|\sim attack\right\rangle + d^{'}\cdot e\cdot\left|\sim defend\right\rangle \otimes \left|attack\right\rangle + \\ &d^{'}\cdot e^{'}\cdot\left|\sim defend\right\rangle \otimes \left|\sim attack\right\rangle \end{aligned} \quad (18)$$

The tensor product has specified two spaces in which the state vector is defined, one is the defender's intent (choice option) to defend or not defend and another belief is whether it will attack or not attack? The unitary operator which defines the rotation of state vector is also specified. It depends on amplitudes increased by action combination and payoffs. It likewise depends on belief which maximizes the final payments.

4. Conclusion

This paper has presented the proposed model of quantum Bayesian game theory for intrusion detection, which specified the problem as a two player game which is non-cooperative and incomplete imperfect information game of which is an IDS/detector and attacker. This model presents a quantitative method for analyzing network security. The defender takes effective strategy to optimize their profits, according to Bayesian quantum strategy. Quantum Bayesian-based IDS can improve the probability of defender issuing a correct alarm and reduces the probability of defender issuing a false alarm. According to the cognition of network environment, it describes a rapid response of the system and defenders to determine the value

of payoffs. In future, it is proposed that this model will help design an advanced intelligent system with learning capacity to get the quantum architecture of the whole arrangement. It can also be used in microelectronics technology to develop FPGAs control chips for monitoring network traffic in a web environment.

References

[1] V. Chandola, A. Banerjee, V. Kumar. "Anomaly detection: A survey", ACM computing surveys (CSUR), vol. 41, no. 3, pp. 15, 2009.

[2] A.K. Dixit and S. Skeath, "Games of Strategy", 4th Int. Student Edition, WW Norton & Company, new Jersey, USA, 2015.

[3] R.T. Perry, "The temple of quantum computing", Riley Perry standard, Australia, Available on: http://www. toqc. com/TOQCv1_1.pdf. Accessed: April, 27, 2006.

[4] U. Faigle and M. Grabisch, "Game theoretic interaction and decision: A quantum analysis", Games, vol. 48, no. 8, pp. 1-29, 2017.

[5] P. Bruza, J. Busemeyer and L. Gabora, "Introduction to the special issue on quantum cognition", arXiv preprint arXiv, pp. 1309.5673, 2013.

[6] E.M. Pothos and J.R. Busemeyer, "Can quantum probability provide a new direction for cognitive modeling?", Behavioral and Brain Sciences, vol. 36, no. 3, pp. 255-274, 2013.

[7] R. Penrose, "Shadows of the Mind", Oxford University Press, USA, vol. 4, 1994.

[8] C.M. Chen, Y.L. Chen and H.C. Lin, "An efficient network intrusion detection", Computer Communications, vol. 33, no. 4, pp. 477-484, 2010.

[9] M. Tavallaee, E. Bagheri, W. Lu and A.A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", Proc. of the 2nd IEEE Symp. on Computational Intelligence for Security and Defence Applications, Ottawa, Ontario, Canada, pp. 53-58, July 08-10, 2009.

[10] S.T. Powers, J. He ,"A hybrid artificial immune system and Self Organizing Map for network intrusion detection", Information Sciences, vol. 178, no. 15, pp. 3024-3042, 2008.

[11] J.C. Harsanyi, "Games with incomplete information played by "Bayesian players", The Basic Model & Management Science, vol. 50, no.12, Supplement, pp. 1804-1817, 2004.

[12] S. Shen, G. Yue, Q. Cao and F. Yu, "A survey of game theory in wireless sensor networks security", J. Networks, vol. 6, no. 3, pp. 521-532, 2011.

[13] G. Anuvarsha and K.J. Rajesh, "Survey on automated intrusion response system using game theory", Int. J. Adv. Res. Comp. and Commun. Engg., vol. 3, no. 11, pp. 8384-8387, 2014.

[14] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", Proc. of Workshop on Game theory for Communications and Networks ACM,vol.199, pp. 4, 2006.

[15] Y. Liu, H. Man and C. Comaniciu, "A game theoretic approach to efficient mixed strategies for intrusion detection", IEEE Int. Conf. on Communications, vol. 5, pp. 2201-2206, 2006.

[16] T. Poongothai and K. Jayara, "A noncooperative game approach for intrusion detection in mobile adhoc networks," Proc. of Int. Conf. on Computing Communication and Networking, St. Thomas, VI, December 18-20, pp. 1-4, 2008.

[17] H. Otrok, N. Mohammed, L. Wang, M. Debbabi and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks", Comp. Commun., vol. 31, no.4, pp.708-721, 2008.

[18] N. Marchang and R. Tripathi, "A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks", Int. Conf. in Adv. Computing and Communications, ADCOM 2007, pp. 460-464, 2007.

[19] M. Rédei and S.J. Summers, "Quantum probability theory", Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics, vol. 38, no. 2, pp. 390-417, 2007.

[20] R. Blutner and P.B. Graben, "Quantum cognition and bounded rationality", Syntheses, vol.193, no.10, pp. 3239–3291, 2015.

[21] A. Iqbal, J.M. Chappell, Q. Li, C.E. Pearce and D. Abbott, "A probabilistic approach to quantum Bayesian games of incomplete information", Quantum Information Processing, vol. 13, no. 12, pp. 2783-2800, 2014.

[22] S. Zahir, J. Pak, J. Singh, J. Pawlick and Q. Zhu, "Protection and deception: Discovering game theory and cyber literacy through a novel board game experience", 2015 USENIX Summit on Gaming, Games and Gamification in Security Education, 2015.

[23] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection", Decision and Control, Proc., 42nd IEEE Conf., vol. 3, pp. 2595-2600, 2003.

[24] E.O. Ibidunmoye, B.K. Alese, O.S. Ogundele, "A Game-theoretic scenario for modelling the attacker-defender interaction", J. Comput. Eng. Inf. Technol, vol. 2, no. 1, pp. 27-32, 2013.

[25] H. Wei and H. Sun H, "Using bayesian game model for intrusion detection in wireless ad hoc networks", Int. J. Communications, Network and System Sciences, vol. 3, no. 7, pp. 602, 2010.

[26] L. Yu, Q. Donghua, "A Bayesian Game Approach for Security Defense Strategy in WSN", Proc. of 2nd international Conference on Computer Application and System Modeling, Atlantis Press, Paris,France,vol.21. pp. 1084-1086, 2012.

[27] A.P. Flitney and D. Abbott, "An introduction to quantum game theory", Fluctuation and Noise Letters, vol.2, pp. R175-R187, 2002.

[28] A.P. Flitney and D. Abbott, "Advantage of a quantum player over a classical one in 2× 2 quantum games", Proc. of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 459, no. 2038, pp. 2463-2474, 2003.