An-Najah National University

Faculty of Graduate Studies

Mathematical Modeling in Game Theory and Applications in Network Security

BY

Hamza Saleem Hasan Herzallah

Supervisor

Prof. Naji Qatanani

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Computerized Mathematics, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine.

2021

Purification of Water in Palestine from Persistent Pesticides Using New Synthesized Cellulose Nanoparticles

By

Hamza Saleem Hasan Herzallah

This Thesis was defended successfully on 10/3/2021 and approved by:

Defense Committee Members	**Signature**
– **Prof. Naji Qatanani / Supervisor**	.....
– **Prof. Maher Qarawani / External Examiner**	.....
– **Dr. Othman Othman / Internal Examiner**	.....

Acknowledgment

All praise to God who gave me boons and patience, who helped me in passing these wears with good health and wellbeing.

I am very grateful to Prof. Naji Qatanani, who supervised this activity, provided all the support.

I place on record my sincere thanks to the external examiners Prof. Maher Qarawani and Dr. Othman Othman for their useful and valuable comments.

I do not forget to send my sincere gratitude to my parents who urged me to continue my studies, who supported me all the time, I thank all of my brothers and my sister for their support and love.

I thank everyone who helped me directly or indirectly to complete this work.

Dedication

To those who spent their time, efforts and care. Who always urged me to reach to the stars, who tried their best to help me from childhood to this moment and over, who encouraged me to earn the highest levels, to my parents with endless love. Thank you

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان :

Mathematical Modeling in Game Theory and Applications in Network Security

أقر بأنّ ما اشتملت عليه هذه الرسالة إنما هي نتاج جهدي الخاص ، باستثناء ما تمّت الإشارة إليه حيثما ورد ، و أنّ هذه الرسالة ككل ، أو أي جزء لم يُقدّم لنيل أي درجة أو لقب علمي أو بحثي لدى أي مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the researcher's own work and has not been submitted elsewhere for any other degree or qualification.

Student's name: **اسم الطالب: حمزة سليم حسن حرزالله**

Signature: **التوقيع :**

Date: **التاريخ: 10 / 3 / 2021**

Table of Content

List of Figures

List of Tables

List of Symbols

Symbol	Description
a_i	Action for player i
A_i	Set of actions for player i
s_i	Player i's strategy
S_i	Player i's strategy set
s	Strategy profile
s^*	Equilibrium for game
s_{-i}	Strategy profile for all players accept player i
s_i^*	Best response for player i
π_i	Player i's payoff
$\pi_i(s_i^*, s_{-i})$	Player i's payoff when he chooses s_i^* and the other choose s_{-i}
F	A function to arrive to the best solution for all players

Mathematical Modeling in Game Theory and Applications in Network Security

By
Hamza Saleem Hasan Herzallah
Supervisor
Prof. Naji Qatanani

Abstract

This thesis focuses on the implementation of the game theory in network security aspects. The game theory is designed to study conflict between two or more opponents, namely; the hacker and the defender. The aim is to give the defender a superior position in achieving the least possible loss when attacked. Moreover, this work shows how basic algorithms of game theory and Nash equilibrium can be used in network security, which helps to make a better choice for the defender in network security field. Furthermore, the implementation of game theory algorithms in the Internet of Things (IOT) is very crucial.

Introduction

It is needless to say that internet became very important part of our life. It exists in every home, workstation, business field, political facilities, military, industry, medicine … etc. a lot of economic transactions happen on the internet, a lot of confidential information is passed over the internet, and interrupting those transactions or information is very dangerous, which makes the role of network security very necessary.

Network security is devoted to secure the important data on the internet, in order not to be stolen or corrupted by hackers, who aim to steel or destroy these data for the sake of earning money or for any other cause. Specialists in network security field try to understand the cracks and the weak points that may be a target to the hackers to invade the data and corrupt it. This, enables the network security specialist to work out how to construct an algorithm which is able to cover these weak points and defend the system. However, this is a very difficult task unless there is a clear defense strategy to identify the hacker's next move and here cause the role of the game theory.

Game theory studies the conflict model between two or more opponents, then gives each opponent the information required to identity the next move of his enemy. Consequently, minimizing the risks.

In fact, game theory has a wide range of applications in economics, politics, computer sciences, military, physics, medicine, engineering and technology (for more details see [4, 10, 24, 37, 38, 47, 50].

Literature Review

For many years' research on game theory has attracted the attention of many researchers. Jhon Von Neuman and Oskar Morgenstern have published in 1944 the first important text on game theory "theory of games and economic behavior". In addition, Jhon Nash has improved the concept of game theory and stablished the Nash equilibrium [9].

A large number of articles have been published in the field of game theory and network security. Basar [5] has studied the problem of transmitting a sequence of identically disputed independent Gaussian random variables through a Gaussian memoryless channel with an input power constraint in the presence of an intelligent jammer. Saad et al., [42] investigated the use of wireless network nodes in improving the physical layer security of wireless transmission in terms of secrecy capacity in the presence of multiple eavesdroppers. The vehicular ad-hoc networks have been studied by Buchegger and Alpcan [7]. They proposed the game theoretic analysis to investigate the effects of possible malicious users on the system in order to increase reliability and better management of resources. Katz [25] has bridged both the approaches and techniques of game theory with the cryptographic protocol design. Moreover, Aziz et al., [3] have used infinite-horizon symmetric repeated zero-sum game against smart jammer. Wang et al., [48] applied the Bayesian game model to select the optimal defense strategy. Stackelberg game in critical infrastructures from a network science perspective has been used by Li et al., [31]. Moothedath et al., [33] applied a stochastic game model to dynamic information flow tracking for

the detection of advanced persistent threats. Horak et al., [20] has suggested the use of dynamic game approach to deception by designing proactive network security. Shen et al., [43] have used a non-cooperative non-zero-sum game based dependability assessment of heterogeneous WSNs with malware diffusion.

This thesis focuses on the implementation of the game theory in network security aspects. The game theory is designed to study conflict between two or more opponents, namely; the hacker and the defender. The aim is to give the defender a superior position in achieving the least possible loss when attacked. Moreover, this work shows how basic algorithms of game theory and Nash equilibrium can be used in network security, which helps to make a better choice for the defender in network security field. Furthermore, the implementation of game theory algorithms in the Internet of Things (IOT) is very crucial.

This thesis is organized as follows:

In Chapter one, we review the game theory including some important concepts and definitions. Chapter two, presents all aspects of network security and information warfare. Implementation of game theory in network security is illustrated in Chapter three. In Chapter four, we propose a real model in network security, namely; stochastic game model. Finally, conclusion is drawn.

Chapter One

Review of Game Theory

1.1 Main Definitions of Game Theory

One of the famous definitions is stated by Myerson:

Definition (1.1) [34]**:** Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers.

This definition means that game theory searches in the case in which the decision-makers is having conflict or cooperation so that maximum of benefit or minimum of loss is obtained. This real case should be converted to mathematical models to reach the optimization solution using the concepts of game theory.

The decision-makers must be rational; this means that the policies considered by decision-makers should be based on game theory concepts.

The following general examples illustrate the cases that can be covered by game theory:

1- Two or more of firms in the same market and having the same product, these firms compete each other to bring more customers.

2- Two countries contemplating a war with each other.

3- The warfare between administrator of a network and the attacker.

More example are [39]:

1- OPEC members choosing their annual output.

2- General Motors purchasing steel from USX.

3- Two manufacturers, one of nuts and one of bolts, deciding whether to use metric or American standards.

4- Aboard of directors setting up a stock option plan for the chief Executive Officer.

5- United Fruit company hiring workers in Honduras in the 1930^{s}.

6- An electric company deciding whether to order a new power plant given its estimate of demand for electricity in ten years.

When a case is called "game"?

The case must be containing many elements to call it "game" and to apply concepts of game theory on it, these elements are [39]

1− Players

Definition (1.2) [39]**:** Players are the rational entities who make decisions. Such that they aim is to maximize their utility through choosing the best strategy in the model, and it is denoted in this thesis by i.

2− Action or Move

Definition (1.3) [39]**:** An action or move by player i, it is what the players can make through the game, and denoted a_i.

- despite of the players must be rational as the definition of Myerson, but in some cases, there exist a pseudo-player which can be called a nature, such that it takes random actions with specified probabilities. Such that in this case, there are not enough guarantees about what the other player will play.

- **Definition (1.3)** [39]**:** Player i's action set, $A_i = \{a_i\}$, is the set of actions group such that the player i choose his actions from it.

3− Strategy

Definition (1.4) [39]**:** Player i's strategy s_i is what player must choose upon the circumstances in the game and the expectation to strategies for the other player.

- **Definition (1.5)** [39]**:** Player i's strategy set or strategy space $S_i = \{s_i\}$ is the complete plan of action to player over all game.

- **Definition (1.6)** [39]**:** A strategy profile $s = (s_1, \dots, s_n)$ is the general form of the game upon the strategies of all players in this game.

  Such that a strategy profile explained the strategies that players will choose in the game.

4− payoff

Definition (1.7) [39]**:** The player i's payoff $\pi_i(s_1, \dots, s_n)$, is the utility that is received by the player in the end of the game or the expected

utility of this player upon the function of the strategies that was chosen by himself and by all other players in the game.

Example (1.1): Elections

If there are two candidates in a particular country, each of the candidates must choose a political position, and every voter will choose a candidate whose political position is close to the political position of this voter.

In this country there are ten positions, far-right wing and the far-left wing, the rest of the positions are between these two wings and are going to the center (politically moderate positions), and each position represents 10% of voters in this country, as shown in the following figure:

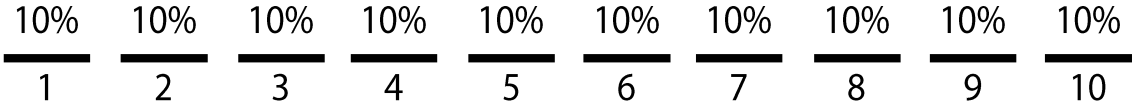

Figure 1: percentage distribution of each position for elections example.

Now, let us analyze this situation:

- Players: two candidates.
- Strategies:

The strategies are the same as actions, since no information is revealed that might affect the action that is chosen by a player, so strategies or actions are to choose each candidate position that guarantees him to win.

- Payoffs:

Winning candidate by the votes higher than the other.

There is another important element in the “game”, which is equilibrium

Definition (1.8) [39]**:** An equilibrium $s^* = (s_1^*, \dots, s_n^*)$ is a strategy profile consisting of a best strategy for each of the n players in the game.

An equilibrium concept or solution concept $F: \{S_1, \dots, S_2, \pi_1, \dots, \pi_2\} \rightarrow s^*$ is a rule or a function which aims to arrive to the best solution for all player based on the strategy that can be made by the player and the resulted payoff function.

There are many important equilibria. For example, Nash equilibrium, Stackelberg equilibrium, saddle-point equilibrium, Bayesian Nash equilibrium, and Markov equilibrium [13].

Types of Game Models

Each type has different solution, these types are divided into many categories, such as

1- First category [14]

a. Cooperative game

A game is called cooperative if the players can communicate with each other and make agreements, and these agreements are binding and enforceable [14].

b. Non-cooperative game

A game is called non-cooperative if players can not communicate with each other or the agreements are not enforceable [14].

2- Second category [9]

   a. Zero-sum game

      Zero-sum game is the game when the summation of the payoff of the players is zero, i.e., when a player wins the other loses with same magnitude [9].

   b. Non-zero-sum game / constant game.

      Non-zero-sum game / constant game is the game when the summation of the payoff of the players is constant [9].

3- Third category [28]

   a. complete information: When every player in the game knows all player' payoff function.

   b. Incomplete information: When at least one of the players does not know all players' payoff functions.

4- fourth category

   a. States game

Definition (1.14) [28]**:** States game is a one-shot game in which players take actions at the same time.

This model of game appears as a standard representation of a game, which is known as normal form game or a game in strategic form [22]

- The set of players is $N = \{1, \dots, n\}$

- Player i has a set of actions, A_i, available.
- Player i's payoff as a function of the vector of actions taken is described by a function $\pi_i: A \to \mathbb{R}$.

Example (1.2): "Hannibal" game

"Hannibal Barca: was a Carthaginian general, considered one of the greatest military commanders in history. His father Hamilcar Barca was the leading Carthaginian commander during the first Punic war" [54]

In this example we will describe one of wars of Hannibal.

An invader is thinking to invade a country, and there are two ways through which he can lead his army.

You are the defender of this country and have to decide which of these ways choose to defend: you can only defend one of these routes.

One route is a hard pass: if the invader chooses this route, he will lose one battalion of his army (over the mountains).

If the invader meets your army, whatever route he chooses, he will lose a battalion.

The strategic form:

Table 1: payoffs table for Hannibal war.

	Attacker		
defender		e	h
	E	1,1	1,1
	H	0,2	2,0

E, e = easy; H, h = hard

Payoffs are the number of attacker's battalions that will arrive in to your country. Such that the first number in the payoffs represented the number of battalions that will be defeated, and the second number in the payoffs represented the number of battalions that will arrive.

Definition (1.15) [39]: A pure strategy maps each of player's possible information sets to one action.

Definition (1.16) [39]: A mixed strategy maps each of player's possible information sets to a probability distribution over actions.

b. Dynamic game

Definition (1.17) [41]**:** Dynamic/ extensive game is a game with more than one stages in each of which the players can consider their action. It can be considered as a sequential structure of the decision-making problems encountered by the players in a static game.

This means that the move taken by the first player can be seen by the other players, the second player determines his move based on the move of the first player. So, in this model the order should be considered.

Example (1.3): Quality choice

There are two players, player 1 is an internet service provider and player 2 is a potential customer. They consider entering into a contract of service provision for a period of time.

The provider decides between two levels of quality of service: High (H) or Law (L), and the buyer decides between two actions: to buy (B) or not to buy (N).

The service provider, player 1, makes the first move, choosing (H) or (L), then the customer, player 2, is informed about that choice. Player 2 can then decide separately between (B) or (N) in each case.

The extensive form of this game:

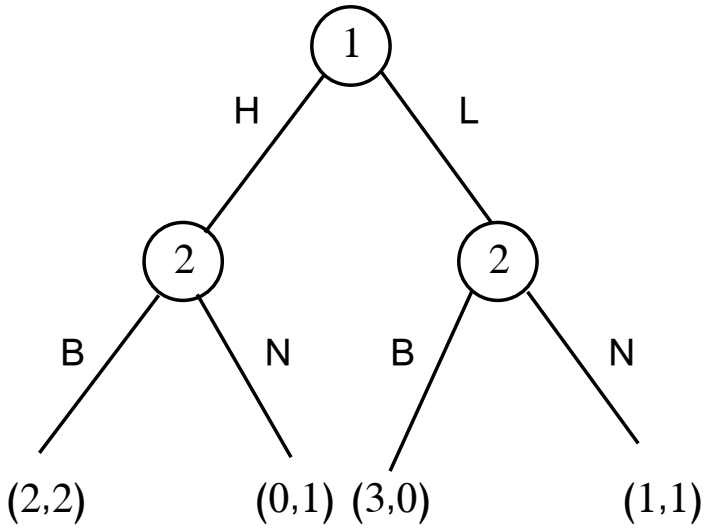

Figure 2: extensive form for quality choice example.

Such that {(2,2), (0,1), (3,0), (1,1)} is the payoff of the game (payoff of player 1, payoff of player 2). For example, in the second payoff (0,1), "0"

payoff for player 1 and "1" payoff for player 2 when the player 1 plays "H" and player 2 plays "N".

There are many concepts and laws to solve these types and models. Some of these concepts will be studied later.

1.2 Dominant Strategies

Theorem (1.1) [39]**:** Player i's best response or best reply to the strategies s_{-i} chosen by the other players is the strategy s_i^* that yields him the greatest payoff; that is

$$\pi_i(s_i^*, s_{-i}) \geq \pi_i(s_i', s_{-i}) \quad \forall s_i' \neq s_i^*$$

Such that $s_{-i} = (s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$

Theorem (1.2) [39]**:** The strategy s_i^* is a dominant strategy if it is a player's strictly best response to any strategies they pick, his payoff is highest with s_i^*. Mathematically

$$\pi_i(s_i^*, s_{-i}) > \pi_i(s_i', s_{-i}), \ \forall s_{-i}, \forall s_i' \neq s_i^*$$

Example (1.4): Prisoner Dilemma

This is the most famous example in game theory:

Scenario:

Police caught two criminals, and put each of them in a separate cell, and told each of them:

If you made a confession that your friend committed the crime and he did the same for you, both of you will by jailed for 5 years.

But if you made the confession that he committed the crime and he did not do that for you, you will be freed from the prison and he stays 10 years.

If both of you did not say anything you will be prisoned for 1 year.

What will every prisoner do to come out with the minimum duration in prison?

- Players

  The criminals {first criminal (1), second criminal (2)}

- Strategy

  S_i= {admitted, not admitted}

- Payoffs

  Spend the minimum duration in prison.

Let’s turn the data to the easiest form so that we can deal with the problem easily, using the following payoff table.

Table 2: payoffs table

Player 2 / Player 1	Strategy 1 for player 2	Strategy 2 for player 2
Strategy 1 for player 1	(payoff for player 1, payoff for player 2)	(payoff for player 1, payoff for player 2)
Strategy 2 for player 1	(payoff for player 1, payoff for player 2)	(payoff for player 1, payoff for player 2)

Table 3: payoffs table of prisoners's dilemma

Prisoner 2 / Prisoner 1	Admitted	Not admitted
Admitted	(5,5)	(0,10)
Not admitted	(10,0)	(1,1)

Let us study each case in this example alone:

Let’s symbolize the admitted by ‘C’ and not admitted by ‘D’

If ‘1’chose ‘C’ then the best strategies for the ‘2’ is ‘C’, because 5<10

If ‘1’chose ‘D’ then the best strategies for the ‘2’ is ‘C’, because 0<1

If ‘2’chose ‘C’ then the best strategies for the ‘1’ is ‘C’, because 5<10

If ‘2’chose ‘D’ then the best strategies for the ‘1’ is ‘C’, because 0<1

Every time the best strategies of the two player is ‘C’

In other words, if each of the prisoners think: “if I male no confession, and my partner do the same, both of us will spend only 1 year which is better than 5 or 10 years”

But every player will re-think again “if the other confesses, I will stay 10 years, so I must confess about him, and even if he doesn’t confess, I will get out of prison which is better than spending 1 year”

Then the strategies of the both players will be to confess.

By the symbols

$$\pi_1(C,C) = 5 < \pi_1(D,C) = 10$$

$$\pi_1(C,D) = 0 < \pi_1(D,D) = 1$$

$$\pi_2(C,C) = 5 < \pi_2(C,D) = 10$$

$$\pi_2(D,C) = 0 < \pi_2(D,D) = 1$$

1.3 Iterated Dominance

An iterated dominance equilibrium is a strategy profile found by deleting a weekly dominated strategy from the strategy set of one of the players, recalculating to find which remaining strategies are weakly dominated, deleting one of them, and continuing the process until only one strategy remains for each player [39].

Such that,

Theorem (1.3) [36]**:** we say player i’s strategy s_i^* is weakly dominated by player i’s strategy s_i if

$$\pi_i(s_i, s_{-i}) \geq \pi_i(s_i^*, s_{-i}) \quad \forall s_{-i}$$

$\pi_i(s_i, s_{-i}) > \pi_i(s_i^*, s_{-i}) \quad \exists s_{-i}$.

Example (1.5): Iterated Dominance

In this example, the idea of iterated dominance is clarified. The table shown is filled with simple figures, it is not related to realistic case, just to clarify the term “iterated dominance”.

The player who achieves the highest figure, is the one who has the highest payoff.

Table 4: payoffs table for the iterated dominance example

	Player 2			
Player 1		l	c	r
	T	1,1	0,1	3,1
	M	1,0	2,2	1,3
	D	1,3	3,1	2,2

It is clear that strategy ‘c’ for player 2 is weakly dominated by strategy ‘r’, so ‘c’ strategy can be deleted.

Table 5: payoffs table for the iterated dominance example, after deleting strategy 'c'

	Player 2		
Player 1		l	r
	T	1,1	3,1
	M	1,0	1,3
	D	1,3	2,2

It is found that strategy ‘M’ for player 1 is weakly dominated by strategies ‘T’ and ‘D’, then strategy ‘M’ can be deleted.

Table 6: payoffs table for the iterated dominance example, after deleting strategy 'M'

	Player 2		
Player 1		l	r
	T	1,1	3,1
	D	1,3	2,2

It is also clear that strategy ‘D’ for player 1 is weakly dominated ‘T’, and strategy ‘r’ for player 2 is weakly dominated by strategy ‘l’.

Finally, the best choice for both of the players is (T,l)

1.4 Nash Equilibrium

John Forbes Nash is an American mathematician whose works in game theory, differential geometry, and partial differential equations have provided insight into the forces that govern chance and events inside complex systems in daily life. His theories are used in market economics, computing, evolutionary biology, artificial intelligence, accounting, politics and military theory. Serving as a Senior Research Mathematician at Princeton University during the latter part of his life, he shared the 1994 Nobel Memorial Prize in Economic Sciences with game theorists Reinhard Selten and John Harsanyi [35].

Definition (1.18) [39]**:** A strategy profile s^* is a Nash equilibrium if no player has incentive to deviate from his strategy given that the other players do not deviate. Formally,

$$\forall i, \pi_i(s_i^*, s_{-i}^*) \geq \pi_i(s_i', s_{-i}^*), \forall s_i'$$

Example (1.6): Nash equilibrium

Table 7: payoffs table for the example of Nash equilibrium

	Player 2			
Player 1		l	c	r
	U	0,4	4,0	5,3
	M	4,0	0,4	5,3
	D	3,5	3,5	6,6

Note that there are no dominated strategy and we cannot use the iterated dominance but we can use the best response

$$BR_1(l) = M$$

$$BR_1(c) = U$$

$$BR_1(r) = D$$

$$BR_2(U) = l$$

$$BR_2(M) = c$$

$$BR_2(D) = r$$

Such that $BR_i(s_{-i})$ is the best response for player i when the other chooses s_{-i}.

Table 8: payoffs table for the previous example

	Player 2			
Player 1		l	c	r
	U	0,4	4,0	5,3
	M	4,0	0,4	5,3
	D	3,5	3,5	6,6

Note that here the profile strategy (D,r) is the best response for each player, then no player has incentive to deviate from his strategy in this profile, so this is the Nash equilibrium.

Example (1.7): partnership game

Two individuals (players) are going to supply an input to a joint project, the two individuals share 50% of the profit, the two individuals

supply efforts individually, and each player chooses the effort level to put into the project (e.g. working hours)

every player can work for 0-4 hours.

s_i= [0,4]

Note: this is the continuous set of strategies

Let's now define the profit to the partnership

Profit=4[$s_1 + s_2 + bs_1s_2$]

Where:

s_i= the effort level chosen by player i.

b= synergy/complementaity.

$0 \leq b \leq {}^{1}/_{4}$

Payoffs

$$\pi_1(s_1, s_2) = \frac{1}{2}[4(s_1 + s_2 + bs_1s_2)] - s_1^2$$
$$\pi_2(s_1, s_2) = \frac{1}{2}[4(s_1 + s_2 + bs_1s_2)] - s_2^2$$

Players share the profit in half, they bear a cost proportional to the square of their effort level.

Note: payoff=benefit-cost

There is no table of strategy and payoff because we have an infinite strategy for each player.

Let us remember what's the best response?

Player i's strategy s_i^* is a BR to strategy s_{-i} of other player if:

$$s_i^* = \arg\max \pi_i(s_i, s_{-i})$$
$$s_1^* = \arg\max\{2(s_1 + s_2 + bs_1s_2) - s_1^2\}$$

So, we differentiate:

First derivative: $2(1 + bs_2) - 2s_1 = 0$

second derivative: -2<0

s_1^*=$1 + bs_2 = BR_1(s_2)$

s_2^*=$1 + bs_1 = BR_2(s_1)$

Now, let's draw the two functions we found and have a look at what we can say.

Let's also fix the only parameter of the game:

b=$1/4$

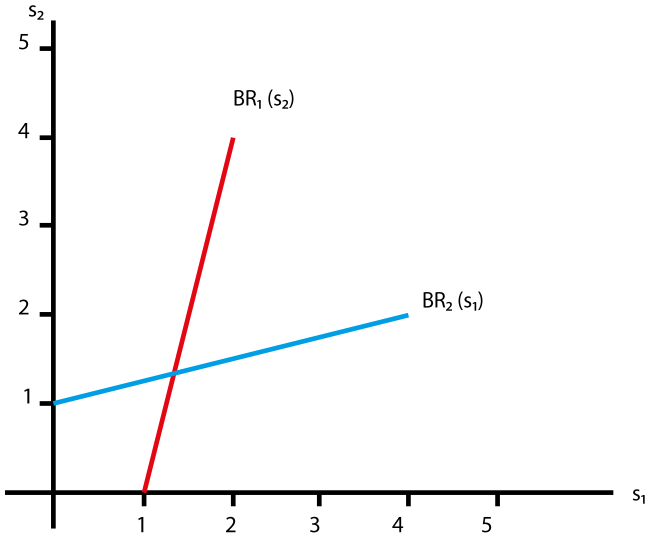

Figure 3: best response of the partnershi fame example

Such that the red line represents the best response of player 1 when player 2 plays as in blue line. And vice versa for the blue line.

Now we know that the player 1 doesn't choose any strategy less than 1, or more than 2 on s_1 line the same goes for the player on s_2 line.

So now if each player knows this than we can delete some strategy.

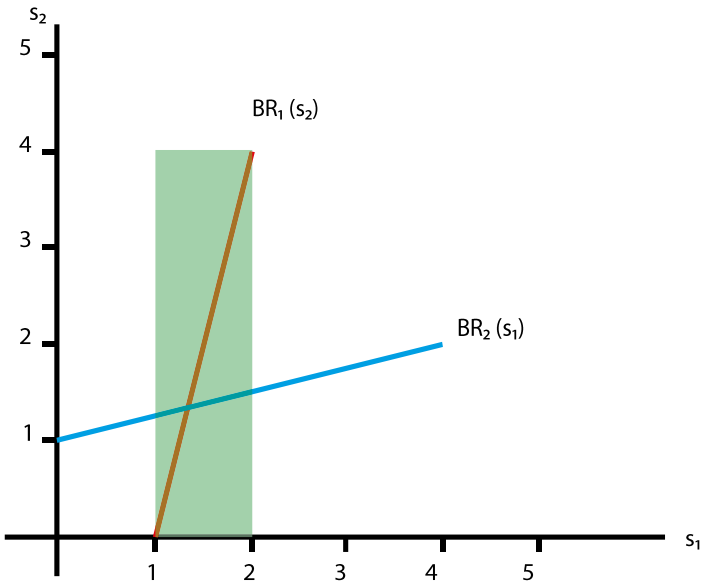

Figure 4: best response of the partnership game, for player 1

As shown in the figure we deleted all the strategies of the second player except the shaded strategies, because the strategies we have removed do not constitute a best response to any best response to the first player.

And this is what we will do for the first player.

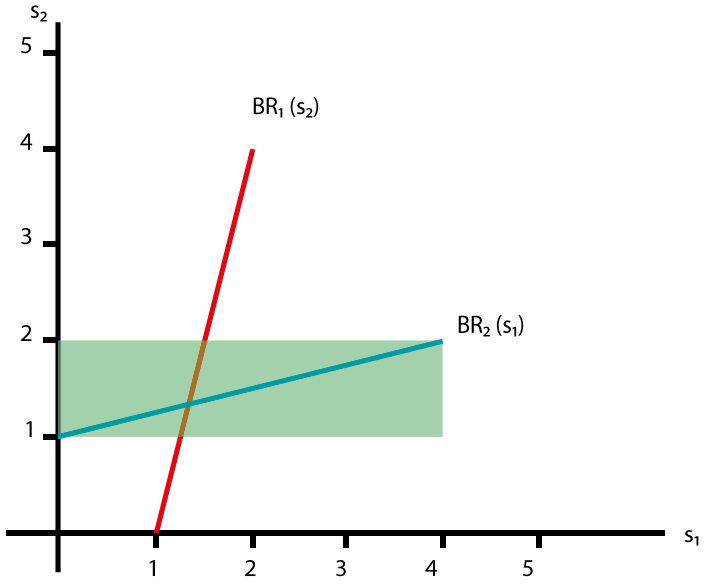

Figure 5: best response for the partnership game, for player 2

After this deletion, we will only have the following region.

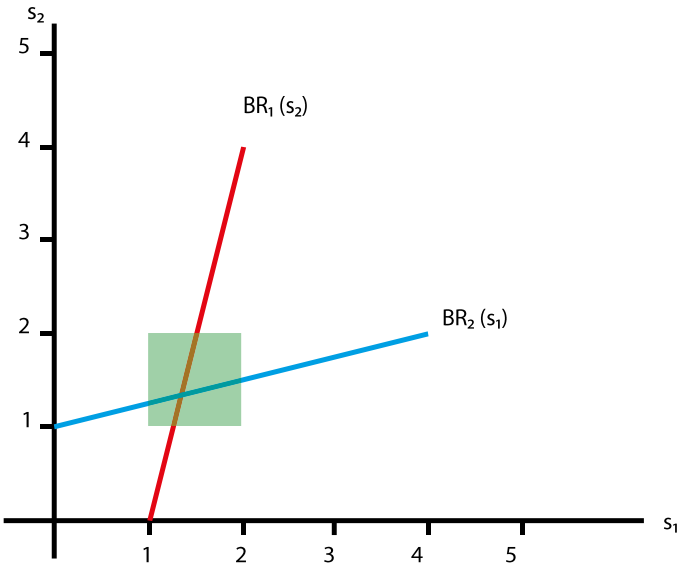

Figure 6: best response of the partnership game, for both players

We are now talking the strategies that are of interest to us and restoring the same processes.

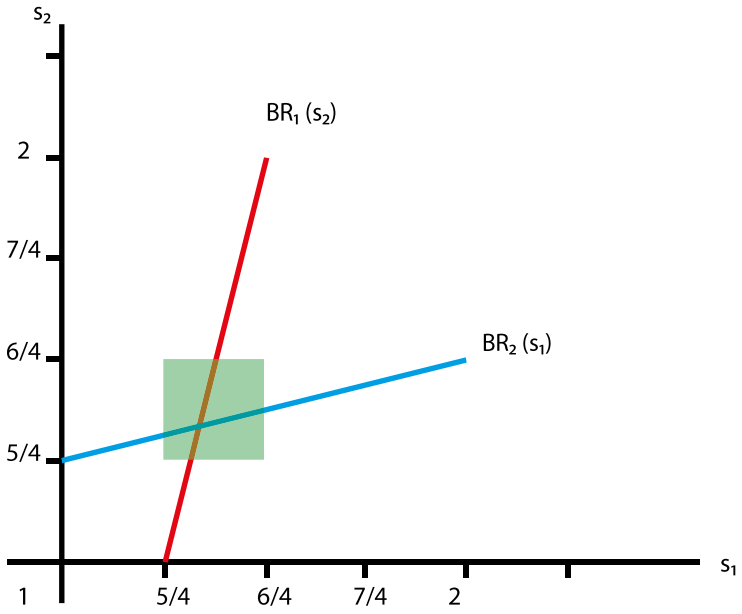

Figure 7: best response for partnership game after deleting strategies

If we continue to do so, we will reach the intersection point of the two lines.

The intersection point of the two lines is the Nash equilibrium.

If we want to know what is the value of the intersection point, we can equate the equation of two line

$$s_1^* = 1 + bs_2$$

$$s_2^* = 1 + bs_1$$

The intersection: $s_1^* = s_2^*$

Then: $s_1^* = 1/(1 - b)$.

Chapter Two

Network Security

2.1 Main Concepts of Computer and Network

Computer became a very important element in our homes. Many aspects of life depend now on this technology; pictures, private files, work files and others. These are stored in the computer and sent by the internet, which makes the word as a small village. On the other hand, it makes all files in danger; so, it is very important to understand how computer and internet work, so that protection of our files and information is possible.

Computer consists of software – which consists of operating system, services, applications … – and hardware.

Operating system managing the operation of the hardware (Input, output, storage) & management of running software.

Applications or services are various programs in computer such as Microsoft word, Microsoft excel, games, photoshop, and others.

The following figure clarifies how computer interact with the user:

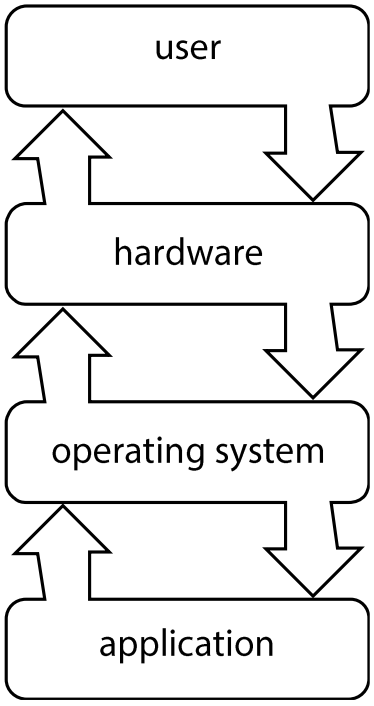

Figure 8: interaction between computer and user

Internet is a huge network connecting millions of users around the world, so if we need to know about the internet, we should answer the question “what is the network?”.

Definition (2.2) [40]**:** Network is a collection of computers (nodes) and transmission channels (links) that allow people to communicate over distances, large and small.

Information elements in network:

- Sender
- Recipient
- Message / information content
- Transmitter tool

Types of connection between computers:

- By cable.
- By wireless.

There are many types of network, but we are interested in just two types of it:

Definition (2.3) [40]**:** LANs. (Local Area /networks) are networks that cover a small area as in a department in a company or university.

This network is used at:

- Schools.
- Small institutions.
- Homes.
- Internet cafes.
- And others

Definition (2.4) [15]**:** WANs. (Wide Area Networks): are networks designed to facilitate communications between users and applications over large distances between the various offices of an international organization that are located in cities all over the world.

This network used in:

- Huge institutions that own many branches.
- Government agencies.

- And others.

The presence of language is essential to make communication; people can’t understand each other without common language, this is applied also for computers connected in a network; the computer language that is used in network communication is called protocol.

Protocols are the rules of operation of a network [40].

The most important types of protocol:

1- TCP. (transmission communication protocol): the fundamental purpose of TCP/IP is to provide computers with a method of transmitting data from one application to another over a network [6].

   The Internet Protocol (IP) is a set of rules, for routing and addressing packets of data, that meaning the IP protocol travel across networks and arrive at the correct destination.

Such that TCP protocol check if the information sent between computers have reached its destination, and it check whether all sent packets are received in the correct order. If a packet did not arrive, the TCP send it again.

The features of TCP

- Reliability: this protocol guarantees the arrival of information without errors.

- TCP creates connection between the two computers before sending message.
- Numbering the packet and sending it according to the order.
- Control the information flow (don’t send any new information before the receiving computer receives the previous packets/parts).

2- UDP. (user datagram protocol): An alternative protocol, UDP, is used for some applications instead of TCP. UDP is a connectionless service. Unlike TCP, there is no communication between the sender and receiver nodes to set up a connection in advance [15].

2.2 Information Warfare

Information warfare becomes common, an many parties used it, so the information now in dangerous, this makes everyone cares about protect their information, for these researches increased about this term.

Cyberbreach becomes scary nightmare to personal and government. Such that NASA was breached in 1999 by a 17-year-old high school student from Colorado Springs [55].

In 2013 adobe is breached, hackers stole login information and nearly 3 million credit card numbers from 38 million Adobe users [52].

A big breach in the American system, where information of social security numbers was accessed for 22 million people, and information belonging to a large group of US government employees [53].

Types of hacking

1- Internal

- By user
- USB
- Another computer in the same network
- Through network devices for examples printers and phones

2- External: through internet, and this way is the most popular

- By mail
- By visiting website
- Through download program
- Through accepting an unknown extension, or downloading file or link

Types of hacking according the attacker

- Individually
- Groups

Types of hacking according method

- By malware
- By vulnerability

Vulnerability is a weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves [1].

Malware is a software that harmfully attacks other software to destroy it, where to harmfully attack can be observed to mean to cause the actual behavior for the software to differ from the intended behavior [26].

Steps of attack [44]

1- Reconnaissance (Footprinting)

2- Scanning

3- Gain access

4- Maintain access

5- Clearing Track (Remove logs)

Footprinting is the process attackers take to understand a target's network and associated system. This is a continuous process used throughout all planned attacks, and in which attackers want to gain as much information about the target as possible [46].

Types of information

- Companies and institution
- Individuals
- System

- Networks

Foot printing for companies and institutions

- Employee data
- The company’s website
- Company privacy policy
- Company server
- And others

Foot printing for individuals

- Personal data
- Contact numbers
- Date of birth
- Location
- Education
- And others

Foot printing for systems

- Name of users
- Name of system
- Passwords
- And others

Foot printing for network

- Domain name
- Internal domain name
- IP address of the system
- VPN points
- And others

Another category for types of foot printing

- Active: the attacker communicates directly with the victim or his website to take the information he needs.
- Passive foot printing: the attacker does not communicate with the victim directly, but rather collects information from other locations.
- Social engineering: is the ability to manipulate people to perform actions or acknowledge sensitive information, such as:
    - Contact data
    - Mail
    - Bank information
    - Friends and relationships
    - The work

Port scanning can be defined as “hostile Internet searches for open ‘doors,’ or ports, through which intruders gain access to computers.” [27]

The attacker makes sure that administrator use security tools such as intrusion detection system (IDS) and virtual private network (VPN).

An intrusion detection system (IDs) is a device or software that can detect an attack as it occurs. IDS systems can use different methodologies for monitoring for attacks. In addition, IDS can be installed on either local hosts or networks. An extension of IDS is an intrusion prevention system (IPS) [11].

Definition (2.10) [11]**:** A virtual private network (VPN) is a technology that enables authorized users to use an unsecured public network, such as the Internet, as if it were a secure private network.

Features of VPN

- The internet service provider will not be able to snoop your data.
- Browsing the internet with more secure and confidential.
- Encrypt all data that you use on the internet.

Gain access: This phase is where an attacker breaks into the system/network using various tools or methods. A tailgater stands outside the door and waits until an employee exits the building. He then slips behind the person as he is walking away and grabs the door just before it closes to gain access to the building [11].

Maintain access: the attacker maintains access to the hacked system, so that the attacker does not have to redo the hacking every time he needs to use

the victim’s machine. This is done by using special programs or routines implanted on the victim’s machine.

I will report group of terms, method, and program used by attacker and administrator in the last two steps; gaining access, and maintaining access.

Spyware is a general term used to describe software that secretly spies on users by collecting information without their consent [11].

What does spyware do in system?

Spyware hides all its operations in the system inside a file to avoid reveal and delete it.

Spyware similar to the trojan horse program that disguises the components of free software available on the internet for fee download an installation.

The spyware program allows the attacker to collect data about the victim or the company such as email, login data, passwords, bank account number, etc.

How spyware is spread in systems?

- It is infected by downloading and installing untrusted applications.
- Browser vulnerabilities.
- By cookies.

Network sniffing or packet sniffing is the process of monitoring a network in an attempt to gather information that may be useful in an attack.

With the proper tools a hacker can monitor the network packets to obtain passwords or IP addresses [8].

Not only can it get data packets for the device it is installed on, it can also get data packets for the devices that were connected to the same network as well.

Sniffing works in three steps

1- The attacker operates a sniffing in the local network (LAN) to be able to access all activity logs within the network.

2- Data inside the network may contain sensitive data such as a password or email and unencrypted passwords.

3- The data obtained by the attacker through the sniffing is used in the unauthorized entry process to the target device.

Definition (2.14) [8]**:** Encryption is the process of scrambling the contents of a file or message to make it unintelligible to anyone not in possession of the "key" required to unscramble it.

Cross-Site Scripting (XSS): Not all attacks on websites are designed to steal content or deface it. Instead, some attacks use the web server as a platform to launch attacks on other computers that access it. One such attack is a cross-site scripting (XSS) attack. XSS injects scripts into a web application server to attack at unsuspecting clients [11].

The aim of DoS attack is to make services unavailable to legitimate users, and current network architectures allow easy-to-launch and hard-to-stop DoS attacks. And explanation of this concept follows in this section [21].

SQL injection: Another server-side web application attack that Is done by using specially crafted user response that act as part of SQL rather than a value of the user's response. SQL stands for Structured Query Language; a language used to view and manipulate data that is stored in a relational database. SQL injection targets SQL servers by introducing malicious commands into them [11].

The rootkits program can replace the basic system programs with modified programs that work when the system is running to help run the malware, such as: backdoor, DDoS, Packet sniffers, log-wiping.

The goals of rootkits in system

- Open a channel in the system to permanent login via backdoor.
- Hides attacker activities and movements in the system.
- It collects sensitive data activities and records from the system to benefit the attacker in logging in.
- It installs a lot of malware in the system or server and updates it constantly.

Methods to recognition rootkits

- Integrity-based detection: compare system files, operating logs, and memory with reliable system files.
- Signature-based detection: comparison the system and operational files with rootkits database finger print and movement.
- Heuristic/behavior-based detection: note a change in system behavior.
- Runtime execution path profiling: compare the system operation paths before and after entering the rootkits.
- Cross view-based detection: comparing usual files like system files with algorithms that usually run the same data as operating files.

Steganography: the word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing" [16].

For example: someone may use an electronic picture to transfer text messages or even hidden pictures to another person without anyone knowing, that everyone thinks that the two people exchange pictures, while these pictures are loaded with hidden messages.

The difference between steganography and encryption

When encryption the information, the other people can know that there is communication between two parties, but it cannot understand the information because it is encrypted. But in the steganography, the third party

don’t know that there anything hidden or that there is a connection between the two parties.

Types of steganography

- Steganography in the photos: by tools such as quick crypto.
- Steganography in document: by tools such as wbstego.
- Steganography in audios: by difference tools and methods such as LSB coding, echo data hiding, and spread spectrum method.
- Steganography in videos: the same steps and method to steganography in photos and audios, because the video is slices of photos and audios.

Analyzing of steganography: the science of analyzing methods of steganography depends on discovering the method of converting the message from ordinary to hidden using the techniques of steganography.

The challenges of steganography

- Effective identification and discovery of hidden content within digital images is difficult.
- Texts may be encrypted before they are entered into files, making it difficult to decrypt and identify.

Remove logs (covering tracks): is the last step of penetration steps. After a successful entry into the system or device and having the powers of the administrator, the hacker works to hide his effect from the system so that the breach and movements in the system are not exposed.

Steps for remove logs

- Clear logs
- Manipulation logs
- Disable auditing
- Hide tools

I will report here a type of attack used by the attacker.

Denial of Service ”DoS”: A group of authorized users of a specified service is called to deny service to another group of authorized users if the former group makes the specified service unavailable to the latter group for a period of time which exceeds the limit [17].

Distributed denial- of-service (DDoS) is the same as the “DoS” but it sent by two or more persons [51].

The effect of a DoS attack

- Network crashes
- Financial losses
- Business and corporate crashes
- Service reputation losses

Chapter Three

Implementation of Game Theory in Network Security

Since the network security is the information warfare between two or more players, and all of these players search for the optimized decision to maximize profits or minimize losses. Then we can solve this model using the conflict models in game theory, since the game theory is used to find the optimal solution or optimal decision for any player.

So, in order to use the game theory, we should specify the main elements in this game:

The players are (administrators and attackers) whether we have one admin. And one attacker or more, the model should be controlled according to the case in network.

In order to specify actions, we must know the capabilities of admin and attacker, or in other words what can they do.

In order to specify strategies, we must understand the effect of each action taken by parties, in terms of profits and losses.

Payoff: we should search about the expected payoff for all strategy profile.

It means that we convert the problem of the network security to mathematical model, and this model is different from one case to another, in network security.

In network security there is more and more case different according to number of players, form of movement, actions and strategy for players, and others.

In this section, we will report a literature review related to solving different problems in network security using game theory.

M. Ara et al., [2] talk about zero-sum power allocation game in the parallel gaussian wiretap channel with an unfriendly jammer.

They assumed that the legitimate users, for example (A, and B), such that A is a transmitter (i.e., A transmit messages to B) this channel is the main channel.

They assumed that there exist another two channels, which are (i) the jammer channel, such that it is jamming the main channel, and (ii) there is a user who is not legitimate and he is eavesdropped and he wiretap the messages in main channel.

The authors considered this model is the zero-sum game and they used many theorems to produce the optimal solutions for transmitter and jammer.

They used a theorem which states that if the transmitter strategy s_{ji}^{*} is fixed, $i = 1,2, \dots, n$. Then, the optimal jammer strategy s_{ji}^{*} is:

$$s_{ji}^{*}=\begin{cases}\sqrt{s_{xi}^{2}|\lambda_{mi}|^{4}+\dfrac{4s_{xi}|\lambda_{mi}|^{2}\left|\lambda_{ji}\right|^{2}}{\nu}}-(2+s_{xi}|\lambda_{mi}|^{2}), \\ \dfrac{s_{xi}|\lambda_{ei}|^{4}\left|\lambda_{ji}\right|^{2}}{|\lambda_{mi}|^{2}(1+s_{xi}|\lambda_{ei}|^{2})}\leq\nu<\dfrac{s_{xi}|\lambda_{mi}|^{2}\left|\lambda_{ji}\right|^{2}}{1+s_{xi}|\lambda_{mi}|^{2}} \\ \dfrac{|\lambda_{mi}|^{2}-|\lambda_{ei}|^{2}}{|\lambda_{ei}|^{2}\left|\lambda_{ji}\right|^{2}}, \quad \nu<\dfrac{s_{xi}|\lambda_{ei}|^{4}\left|\lambda_{ji}\right|^{2}}{|\lambda_{mi}|^{2}(1+s_{xi}|\lambda_{ei}|^{2})} \\ 0, \quad \nu\geq\dfrac{s_{xi}|\lambda_{mi}|^{2}\left|\lambda_{ji}\right|^{2}}{1+s_{xi}|\lambda_{mi}|^{2}}\end{cases}$$

T. Spyridopoulos et al., [45] treated the problem about defense frame work against denial of service (DoS) or distributed denial of service (DDoS) cyber-attacks by game theory.

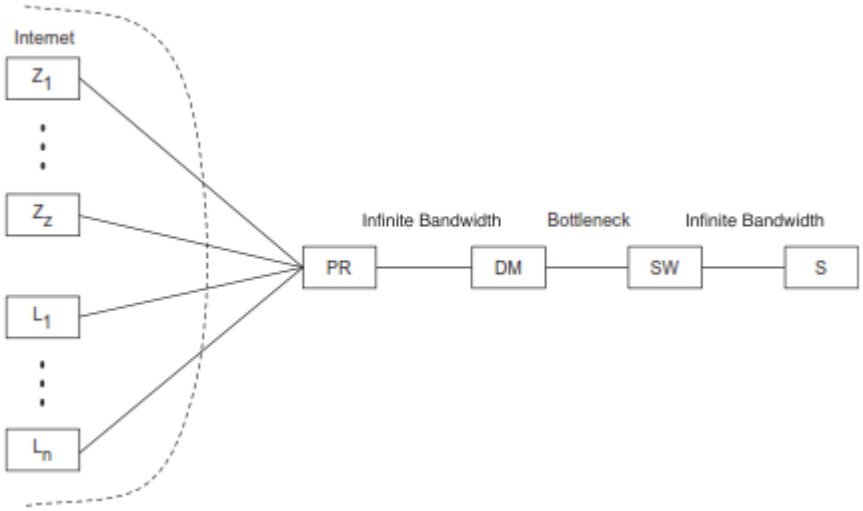

Figure 9: a dumbbell network topology for DoS and DdoS attacks. [44]

They expressed this system by figure 13, such that

S: is a victim server.

SW: is the switch to victim server.

DM: is the node that hosts the defense mechanism (in this case the defense mechanism is a fire wall).

The link between the defense mechanism and the switch is our network's bottleneck.

PR: perimeter router.

L_i: are the legitimate users, such that $i \in [1, n]$ where n is the number of legitimate users that want to connect to the server.

Z_j: are the attacking nodes, such that $j \in [1, z]$ where Z is the number of nodes controlled by the attacker who wants to perform a DDoS attack.

The authors considered the model in game theory that represent this case in network security is non-cooperative zero-sum game. And they build the payoff function based on this model in game theory.

And they take many distributions to the sending legitimate users, such that normal, exponential, Poisson, and others.

As another subject in this section, the microcircuit becomes more developed to becomes the ICs (integrated circuit), but coinciding with the development in ICs, the strategy's attacker developed also. The attacker has the possibility to entering malicious hardware in ICs, this malicious hardware called trojans hardware. On the other hand, the defender checked. These processes become very difficult because limitations of resource and time.

C. A. Kamhoua et al., [23] used the game theory to check this IC takes into account intelligent attackers. These cases are modeled as a zero-sum

game between attacker and defender, and used Nash equilibrium to get best response for defender.

The authors build this model, but I will report here a numerical example in this paper.

They consider a digital circuit with 4 input partitions (N=4), i.e., four classes of trojans and four different strategies of attacker let the values of strategy for attacker:

$$v_A = 1, v_B = 2, v_C = 4, v_D = 12$$

Such that A, B, C and D are the strategies for attacker and the defender strategies are:

AB, AC, AD, BC, BD, and CD.

The payoff is represented in next table.

Table 9: Hardware trojan detection game in normal form. [23]

		Defender					
		AB	AC	AD	BC	BD	CD
Attacker	A	-F, F	-F, F	-F, F	1, -1	1, -1	1, -1
	B	-F, F	2, -2	2, -2	-F, F	-F, F	2, -2
	C	4, -4	-F, F	4, -4	-F, F	4, -4	-F, F
	D	12, -12	12, -12	-F, F	12, -12	-F, F	-F, F

Such that F is fine that the attacker pays to the defender when a trojan is detected.

By studying mixed strategy Nash equilibrium, they get three equilibriums:

{0.323A+0.29B+0.242C+0.145D;0.355AD+0.29BC+0.129BD+0.226CD}

{0.323A+0.29B+0.242C+0.145D;0.29AC+0.065AD+0.419BD+0.226CD}

{0.323A+0.29B+0.242C+0.145D;0.29AB+0.065AD+0.129BD+0.516CD}

These equilibriums represented in follows figures:

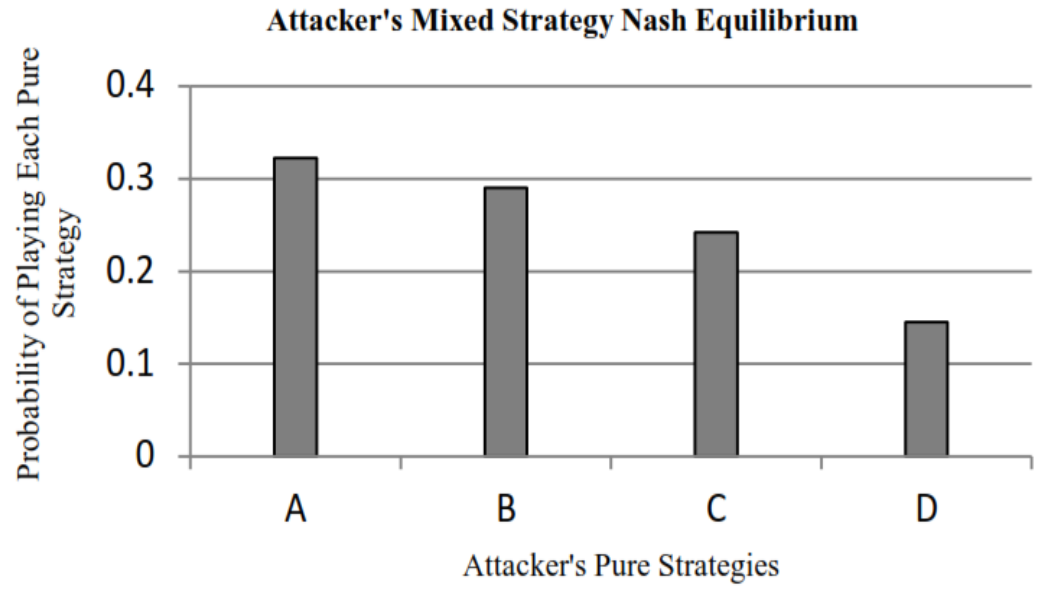

Figure 10: Attacker's mixed strategy Nash equilibrium. [23]

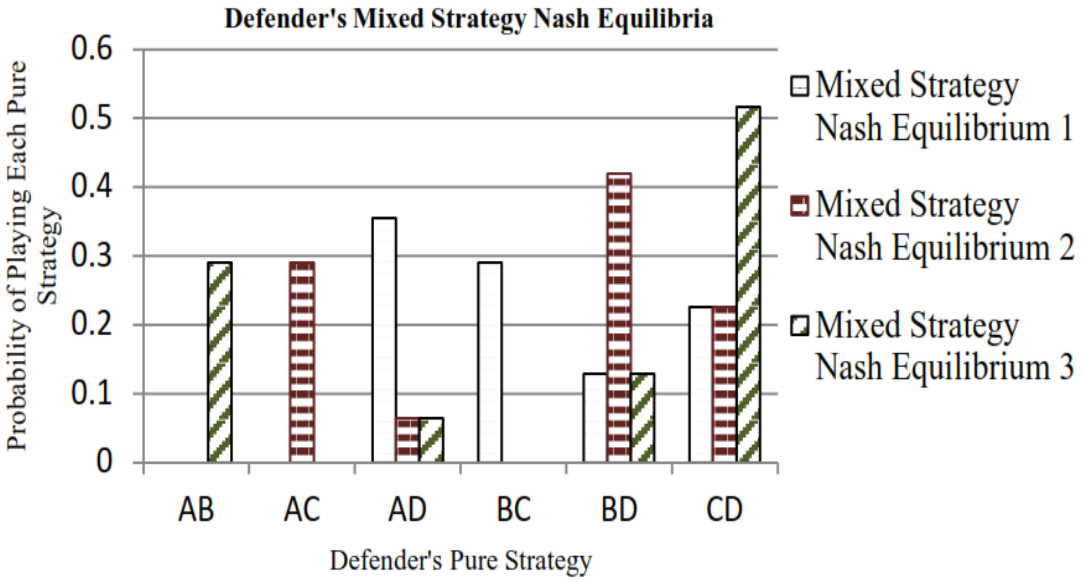

Figure 11: Defender's mixed strategy Nash equilibrium. [23]

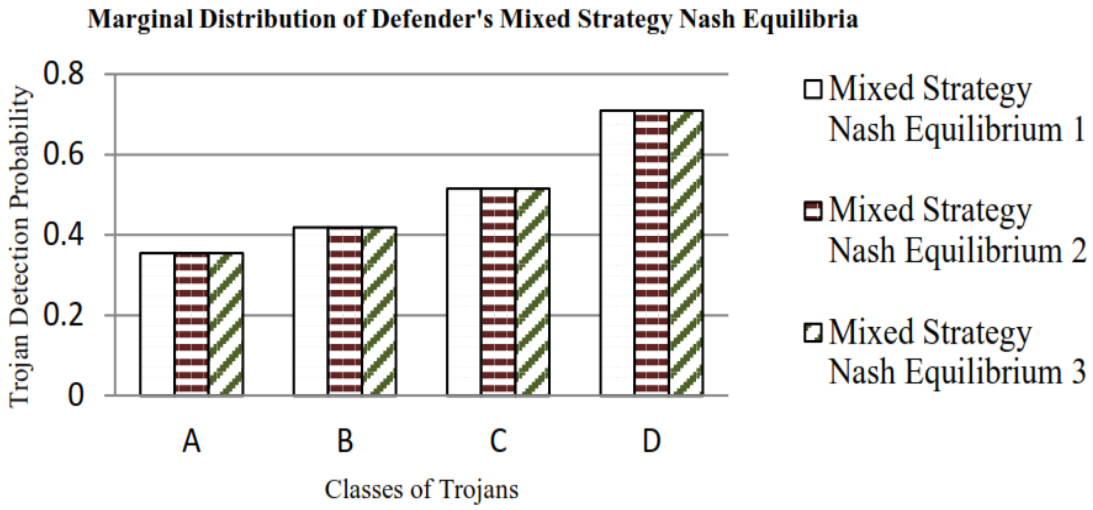

Figure 12: Marginal distribution of the defender's mixed strategy Nash equilibrium. [23]

In paper "network attack and defense game theory based on Bayes-Nash equilibrium" [29], the authors assumed the case between attacker and defender such that the strategy of defender are defending or not defending and strategies of attacker are attacking or not attacking.

The authors assumed that these cases can be described by incomplete information game and solved it by Bayes-Nash equilibrium, so that they used some formula to solve this problem such as

Defensive strategy is

$$s_1(\theta_1) = (s_{11}(\theta_1), s_{12}(\theta_1), \dots, s_{1m}(\theta_1))$$

Such that θ_i is the type set of players i

Attack strategy is

$$s_2(\theta_2) = (s_{21}(\theta_2), s_{22}(\theta_2), \dots, s_{2n}(\theta_2))$$

The risk probability is

$$q_k\left(s_{1i}(\theta_1), s_{2j}(\theta_2)\right) = 1 - p_k(s_{1i}(\theta_1), s_{2j}(\theta_2))$$

Such that p_k is the security probability and q_k is the probability that the assets that were included in the point k will be at risk due to attack, and

$$p_k = 1 - q_k$$

Since the authors assumed that there are two different levels of risk aversion of attackers, then they represented the revenue of risk aversion I and II by π_2' and π_2'' respectively, such that

$$\pi_2' = p_k - q_k\left[s_{2j}(\theta_{21}) - s_{1j}(\theta_{11})\right] * s_{2j}(\theta_{21})$$

$$\pi_2'' = q_k - p_k\left[s_{2j}(\theta_{22}) - s_{1j}(\theta_{11})\right] * s_{2j}(\theta_{22})$$

Since the authors assumed that the defender has only one type, then the expected revenue obtained by the defense party when the defender select strategy $s_{1i}(\theta_{11})$ is

$$\pi_1 = \frac{1}{3}\left\{p_k - q_k\left[s_{2j}(\theta_{21}) - s_{1i}(\theta_{11})\right] - k\right\} * \left(-s_{1i}(\theta_{11})\right) + \frac{2}{3}\left\{q_k - p_k\left[s_{2j}(\theta_{22}) - s_{1i}(\theta_{11})\right]\right\} * \left(-s_{1i}(\theta_{11})\right)$$

The equilibrium is

$$s_{1i}^*(\theta_{11}) = \frac{1}{3}\frac{6k - p_k - 2q_k}{2p_k + q_k}$$

$$s_{2j}^*(\theta_{21}) = \frac{1}{2}\frac{p_k}{q_k} + \frac{1}{6}\frac{6k - p_k - 2q_k}{2p_k + q_k}$$

$$s_{2j}^*(\theta_{22}) = \frac{1}{2}\frac{q_k}{p_k} + \frac{1}{6}\frac{6k - p_k - 2q_k}{2p_k + q_k}$$

Chapter Four

Real Model in Network Security

4.1 Stochastic Game Model

This chapter focuses on some of the important cases in this topic. So, the first section will be about case in the abstract idea of game theory.

Since the main idea in network security is the war between the attacker and the administrator, such that the network will be in normal state in other words it works by normal operations, so the administrator will work nothing but the normal check and he will explore to the vulnerability of the network, in this time malicious individual (could be competitor or a hacker whose aim is financial gain) thinking how to corrupt the network, steal data, or make financial loss to the network. When the attacker makes any kind of these attacks, it will be discovered by the administrator and he works to return the network to normal operations.

So, this model studies the actions for two players, such that one of them choses action and the other respond by his action, so for convenience, actions for both players, effect of each action on the network, and the probability of each player to decide the action will be explained.

On the other hand, the reward of the attacker will be measured by level of destruction of the network, and the costs of administrator will be measured by how much time the administrator need to return the network to normal operation. And if he has a financial loss or stolen confidential data. So, the

reward gained by attacker is not essentially equal to the cost played by administrator.

So most appropriate model in game theory to this problem is a general-sum stochastic game model. In fact, the model and cases in this chapter are clarification for the “game strategies in network security” paper [32].

Formally, a two-player stochastic game is a tuple $(S, A^1, A^2, Q, R^1, R^2, \beta)$ where

Note: the symbols that are used in this study are the same used in the paper of game strategies in network security.

$S = \{\varepsilon_1, \dots, \varepsilon_N\}$ is the state set

$A^k = \{\alpha_1^k, \dots, \alpha_{M^k}^k\}, k = 1,2, \quad M^k = |A^k|$, is the action set of player k. the action set for player k at state s is a subset of A^k, i.e., $A_s^k \subseteq A^k$ and $\bigcup_{i=1}^{N} A_{\varepsilon_i}^k = A^k$

$Q: S \times A^1 \times A^2 \times S \to [0,1]$ is the state transition function

$R^k: S \times A^1 \times A^2 \to \mathbb{R}, k = 1,2$ is the reward function of player k

$0 < \beta \leq 1$ is a discount factor which means: the future rewards to a game player.

Here in this chapter, players 1 and 2 are the attacker and the administrator, respectively.

4.2 Form of Network

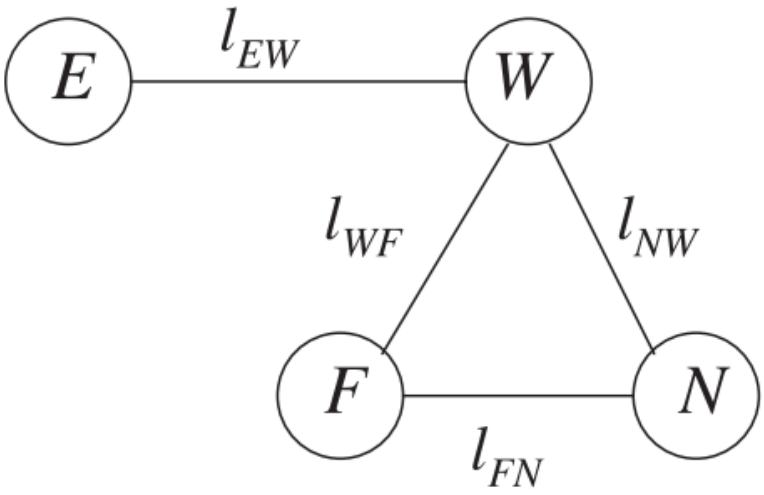

Figure 13: form of network [32]

As shown in figure 17, the model of network, contains nodes and edges. Such that nodes are the main elements in this network and it is E, W, F, N where these nodes represent a single computer, webserver, file server, and workstation, respectively. The edge in this network is the road for communication, whether this road is physical as cable or virtual as WIFI.

To solve this model, we should report the actions for both players and the effects of each action. But for convenience we will separate the action and the state for each player, and study each player alone as shown in figure 18 and figure 19.

So, the actions of attacker are

$A^1 = \{$attack httpd,

Attack ftpd,

Continue attacking,

Deface website and leave,

Install sniffer,

Run DOS virus,

Crack file server root password,

Crack workstation root password,

Capture data,

Shutdown network,

$\emptyset\}$

Such that $\emptyset$ is inaction

Actions for administrator is

$A^2 = \{$remove compromised account and restart httpd,

Restore website and remove compromised account,

Remove viruses and compromised account,

Install sniffer detector,

Remove sniffer detector,

Remove compromised account and restart ftpd,

Remove compromised account sniffer,

$\emptyset\}$

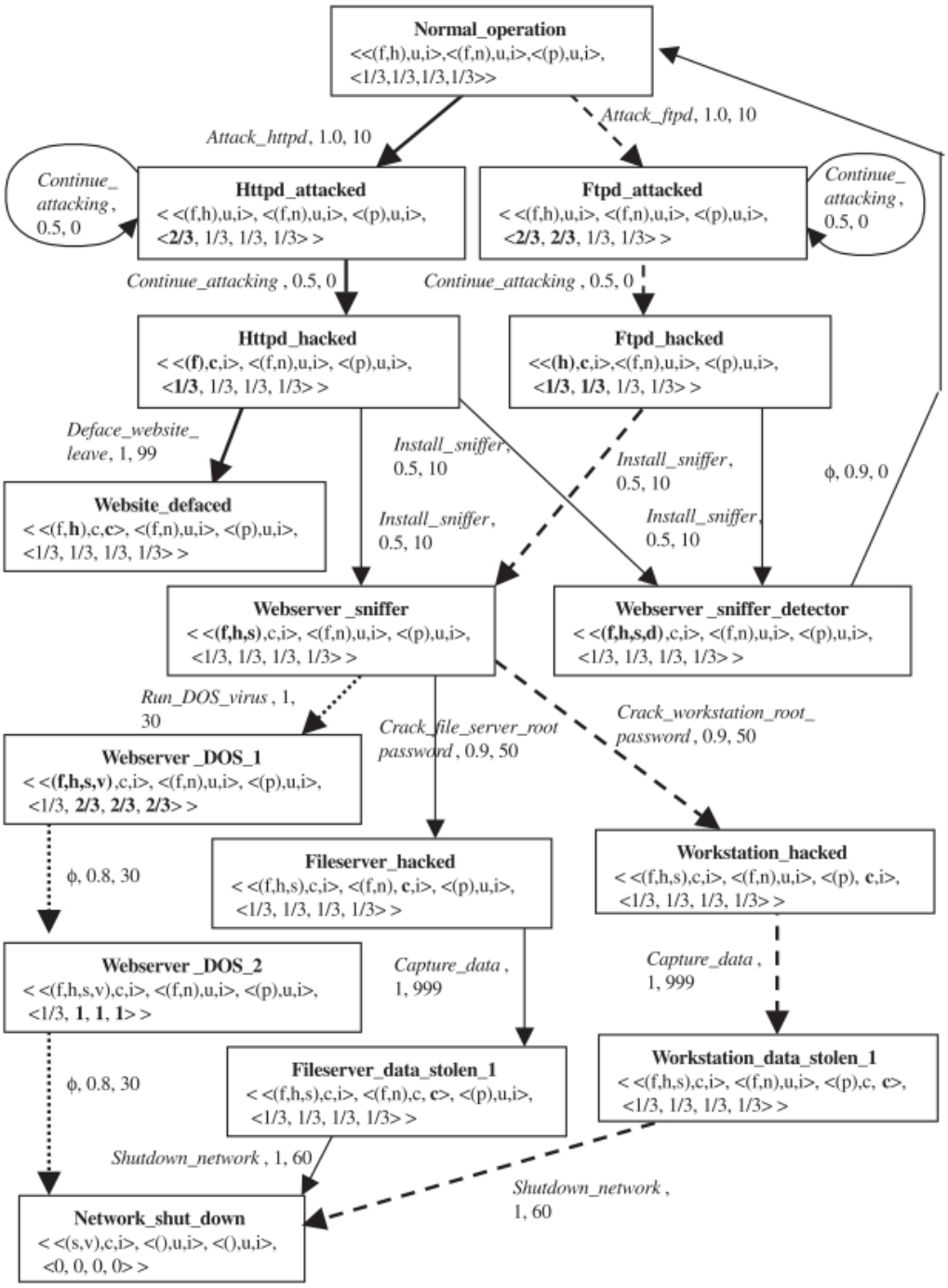

Figure 14: actions for attacker [32]

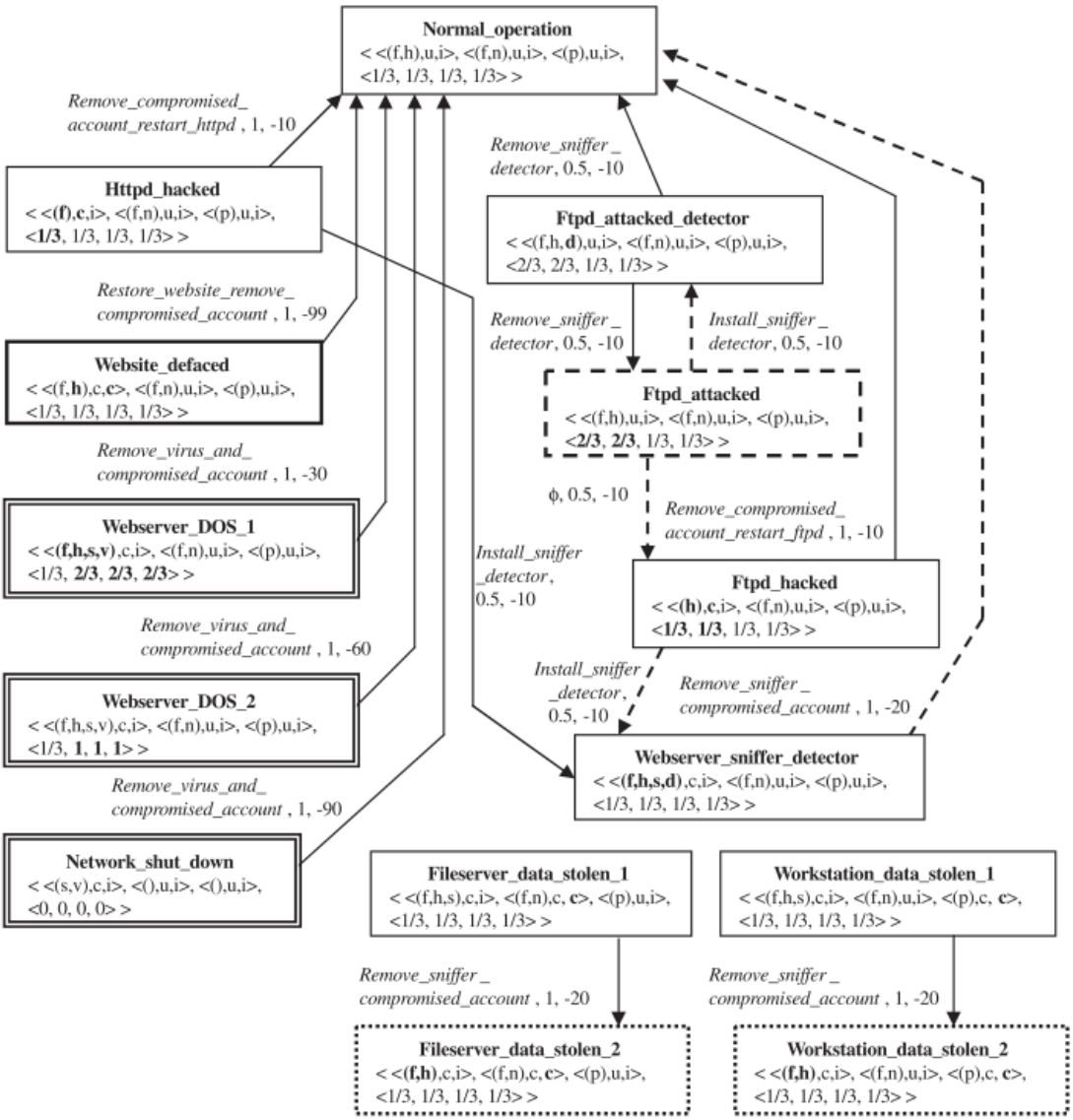

Figure 15: actions for administrator [32]

Each row of boxes in these figures represent state in this model, and all of actions in each state represent a subset of A^1 or A^2. To explain this, in the state "normal operation" in figure 14, the attacker can take many of actions.

$A^1_{normal\ operation}$ ={attack httpd, attack ftpd, ∅}

Each player in any state has many actions to take to make network transition to another state, so when the player wants to transfer from one state to another, he needs to choose an action from available actions in this state, this action ensure transition to new state by probability value, and it achieves to this player a value of reward or costs. For example, when attacker exists in state "httpd hacked" in figure 14, and he decided transition to another state, he has several options, which are {deface website and leave, install sniffer}. If he decided to choose "deface website and leave" he will deface website by probability equal "1" and reward equal "99", and if he decided to choose "install sniffer" he will arrive either to "webserver sniffer" by "0.5" probability and reward "10" or to "webserver sniffer detector" by "0.5" probability and reward "10" too. So, we can say prob (website defaced: httpd hacked, deface website and leave) =1.

4.3 Nash Equilibrium.

Nash equilibrium is a concept in game theory that represent a solution for the model that ensure equilibrium between players, such that it achieve to each player maximum benefit or reward he can get or minimum loss he incurs.

This concept was used in many models of the game theory, also it can be used here in this model - general sum stochastic game model-, and the main idea in these concepts as it was represented in the first chapter in are explained as follow:

Let me be player 1 in the game, I will say if me and the other player used the optimal strategy (as the Nash equilibrium represent it) that ensure to me benefits greater than or equal for benefits that I will have if I used any other strategy and the other player used the optimal strategy. So, both players decided to choose an optimal strategy. So, let we put this idea in mathematical form [34]

$$v^1(\pi_*^1, \pi_*^2) \geq v^1(\pi^1, \pi_*^2), \forall \pi^1 \in \boldsymbol{\Omega^M} \quad \boldsymbol{and}$$

$$v^2(\pi_*^1, \pi_*^2) \geq v^2\left(\pi_*^1, \pi^2\right), \forall \pi^2 \in \boldsymbol{\Omega^{M^2}}$$

Such that

$\pi^k: S \rightarrow \boldsymbol{\Omega}^{M^k}$ is a stationary strategy for player k

Stationary strategy meaning is that the rule of choosing an action is the same in every stage

And $\pi^k(s)$ is the vector $\left[\pi^k(s, \alpha_1) \ldots \ \pi^k(s, \alpha_{M^k})\right]^T$

Where $\pi^k(s, \alpha\ \ )$ is the probability that player k will take action α in state s

And $v^k\left(\pi^1, \pi^2\right)$ is the value vector of the game for player k when both players play their stationary strategies π^1 and π^2

where$v^k_{\pi^1,\pi^2}(s) = E_{\pi^1,\pi^2}\{\sum_{h=0}^{H}(\beta)^h r^k_{t+h}: s_t = s\}$

where the expectation operator $E_{\pi^1,\pi^2}\{.\}$ Is used to mean that player k plays π^k

And $r_{t+h}^k = \pi^1(s_{t+h})^T R^k(s_{t+h})\pi^2(s_{t+h})\ for\ h \geq 0$

And $\boldsymbol{\Omega}^n = \{p \in \mathbb{R}^n : \sum_{i=1}^n p_i = 1, p_i \geq 0\}$ be the set of probability vectors of length n

In fact, there are two types of stochastic game model; infinite-horizon game and finite-horizon game. Here we used infinite-horizon game, so let H=∞ and $\beta < 1$.

To find the stationary equilibrium for this model we should use the non-linear programming [34]

$$\min_{u^1,u^2,\sigma^1,\sigma^2} 1^T[u^k - R^k(\sigma^1,\sigma^2) - \beta p(\sigma^1,\sigma^2)u^k], \quad k = 1,2$$

Subject to

$$R^1(\varepsilon_i)\sigma^2(\varepsilon_i) + \beta T(\varepsilon_i, u')\sigma^2(\varepsilon_i) \leq u'(\varepsilon_i), \quad i = 1, \dots, N$$

$$\sigma^1(\varepsilon_i)^T R^2(\varepsilon_i) + \beta\sigma^1(\varepsilon_i)^T T(\varepsilon_i, u^2) \leq u^2(\varepsilon^i)1^T, \quad i = 1, \dots, N$$

Where $u^k \in \mathbb{R}^N$

$$\sigma^k \in \Omega^{M^k}$$

$R^k(\sigma^1,\sigma^2)$ is the vector $[\sigma^1(\varepsilon_1)^T R^k(\varepsilon_1)\sigma^2(\varepsilon_1)$ ... $\sigma^1(\varepsilon_N)^T R^k(\varepsilon_N)\sigma^2(\varepsilon_N)]$. It contains the rewards for each state when the players play σ^1 and σ^2

$p(\sigma^1,\sigma^2)$ is a state transition probability matrix $\left[\sigma^1(s)^T[p(s' : s, a^1, a^2)]_{a^1\in A^1, a^2\in A^2}\sigma^2(s)\right]_{s,s'\in S}$. This matrix is the stochastic matrix for a Markov chain induced by the strategy pair (σ^1,σ^2).

$T(s,u)$ is the matrix $[[p(\varepsilon_1 : s, a^1, a^2) \dots p(\varepsilon_N : s, a^1, a^2)]^T u^T]_{a^1 \in A^1, a^2 \in A^2}$, where u is an arbitrary value vector.

So $T(s,u)$ represents future rewards from the next state

4.4 static game models

In this section I will review the ideas about static game models. In [30] the researchers considered the conflict between the attacker and the monitoring nodes in the network, and they considered the actions for the attacker to be (attack, or not attack) and the actions for the node of the network is (monitor, or not monitor), and it concluded the payoffs as the following tables.

Table 10: Payoff matrices for the defender and its opponent when the opponent node is a malicious node [30]

	Monitor	Not monitor
Attack	$(1-2\alpha)\omega - \mathrm{c_a}, (2\alpha-1)\omega - \mathrm{c_m}$	$\omega - c_a, -\omega$
Not attack	$0, -\beta\omega - c_m$	0,0

Table 11: Payoff matrices for the defender and its opponent when the opponent node is a regular node [30]

	Monitor	Not monitor
Not attack	$0, -\beta\omega - c_m$	0,0

where:

ω is the security value of the defender?

c_a and c_m denote the cost to the attacker of making an attack, and the cost to the defender of keeping the monitoring system activated.

1− α denotes the false negative rate or missing attacks rate.

β represents the false alarm rate.

Then they derived some of functions to find the best strategies, such that.

$$p_E = \begin{cases} p_{E1} = argmax_{0\le p\le 1} \left\{ \begin{matrix} p.\left[\begin{matrix} q_E\big((1-2\alpha)\omega - c_a\big) \\ +(1-q_E)(\omega - c_a) \end{matrix} \right] \\ +(1-p)[q_E.0 + (1-q_E).0] \end{matrix} \right\} \\ p_{E2} = 0 \end{cases} \begin{matrix} if\ the\ opponent\ is\ malicious \\ if\ the\ opponent\ is\ regular \end{matrix}$$

$$q_E = argmax_{0\le q\le 1} \left\{ \begin{matrix} \mu_0 \left[\begin{matrix} q\left[\begin{matrix} p_{E1}\big((2\alpha-1)\omega - c_m\big) \\ +(1-p_{E1})(-\beta\omega - c_m) \end{matrix} \right] \\ +(1-q)[p_{E1}(-\omega) + (1-p_{E1}).0] \end{matrix} \right] \\ +(1-\mu_0)\left[\begin{matrix} q[(1-p_{E2})(-\beta\omega - c_m)] \\ +(1-q)[(1-p_{E2}).0] \end{matrix} \right] \end{matrix} \right\}$$

$$(p_E, q_E) = \begin{cases} (p^*, q^*) if\ \mu_0 > \dfrac{(1+\beta)\omega + c_m}{(2\alpha+\beta-1)\omega} \\ (\bar{p}, 0) \quad if\ \mu_0 < \dfrac{(1+\beta)\omega + c_m}{(2\alpha+\beta-1)\omega} \end{cases}$$

Where $p^* = \begin{cases} \frac{\beta\omega + c_m}{(2\alpha+\beta)\omega\mu_0} & if\ the\ opponent\ is\ malicious\ node \\ 0 & if\ the\ opponent\ is\ a\ regular\ node \end{cases}$

,$q^* = \frac{\omega - c_a}{2\alpha\omega}$, and $\bar{p} = \begin{cases} 1 & if\ the\ opponent\ is\ malicious \\ 0 & if\ the\ opponent\ is\ regular \end{cases}$

$$\mu_j\big(\theta_i \big| a_i(t_k), h_i^j(t_k)\big) = \frac{\mu_j\big(\theta_i \big| h_i^j(t_k)\big) P\big(a_i(t_k) \big| \theta_i, h_i^j(t_k)\big)}{\sum_{\bar{\theta}_i} \mu_j\big(\bar{\theta}_i \big| h_i^j(t_k)\big) P\big(a_i(t_k) \big| \bar{\theta}_i, h_i^j(t_k)\big)}$$

Where:

μ_0: the strategies of the opponent and the defender can be represented by a tuple (p, q).

p represents the probability that the opponent plays attack.

q represents the probability that the defender plays monitoring.

(p_E, q_E) is the Bayesian equilibrium.

Nodes j and i denotes the defender and it opponents, respectively.

$a_i(t_k)$ represents the action of player i at stage t_k.

$h_i^j(t_k)$ is the history actions of node i observed by node j from stage t_0 to stage t_{k-1}.

$P\left(a_i(t_k)\middle|\theta_i, h_i^j(t_k)\right)$ represents the probability that $a_i(t_k)$ is observed at stage t_k under the condition that the type of the opponent (node i) is θ_i and that the defender (node j)'s observation $h_i^j(t_k)$ on θ_i the history actions of the opponent (node i).

$\mu_j\left(\theta_i\middle|a_i(t_k), h_i^j(t_k)\right)$ represents the probability as the update inference of node j that the type of node i is θ_i under the condition that the observed history actions of node i is $h_i^j(t_k)$ and the action of node i at stage t_k is $a_i(t_k)$.

4.5 Internet of Things and How to Develop it?

Another important case in this topic is about using game theory in the internet of things (IoT). According to “Green Fog Planning for Optimal Internet-of-Thing Task Scheduling” paper “The important of this topic come from this topic is modern, and the scientific giving is renewed. Moreover, the IoT used is spread in many fields of life. It is predicted that more than 50

billion of terminals and devices, such as smartphones, tablets, wearable devices, etc., will be connected to the Internet in 2020, which will generate as much as two Exabytes daily IoT data with features of volume, velocity, and variety" [18]

On the other hand, and for this importance, the attackers are targeting this field actively. So, the protection became very important, thus game theory turn is useful.

We will take a quick look in the paper "A Game Theory Collaborative Security Detection Method for Internet of Things Systems" [49]

This paper assumed that is N nodes (things or objects), and each node "N" are exchanged information with his neighbors "N_i". On the other hand, the attacker looking for the best aims and the best vulnerabilities. Here begin the games nodes wants to prevents attack and decreasing the losses, and the attackers want to increase the profit.

This paper assumed that the system makes alarm on node i when attacks occur, this process is denoted by x_i for $i = 1, \dots, N$. on the other hand, the paper supposes that x_i are gaussian white noises with zero mean under normal conditions and they are mutually independent.

To collaborative security detection, the paper defines two events $H_0$and $H_1$by $\{H_0: a = 0\}$ and $\{H_1: a \neq 0\}$, and make the following testing hypothesis.

$$\frac{1}{N}\sum_{i=1}^{N} x_i \underset{H_0}{\overset{H_1}{\gtrless}} \delta^c$$

Through working on the data of the mathematical model, and through derivation, the paper came up with the decision function at each node.

$$x_i(m) = c_{ii}x_i(m-1) + \sum_{j\in N_i} c_{ij}x_j(m-1)$$

Where the symbols used as in paper.

Then, this paper built on the previous result to find the best response or the Nash equilibrium to this model.

This study will not focus on the details of this model, because our focus is poured on presenting how to use game theory in the application of network security. Speaking about network security model details need to have co-writer of this study who is specialized in network security.

In any case this paper depends on Nash equilibrium to solve this problem and finally it explains case studies, such that distributed denial of service (DDoS).

What I want to say, is that the security in the IoT is very important field because it is very spread today and it became used in vital facilities, for example, oilrigs and military facilities.

On the other hand, Fog became a very important field in cyber which is now used in the IoT.

Offshore oilrigs generate 500 GB of data weekly, commercial jets generate 10 TB for every 30 minutes of flight [12], where any delay in terms of milliseconds affects these facilities. So instead of transferring the data to the cloud, it is transferred now to miniature cloud in the same facility where the things are.

As a conclusion, the security of the fog of the internet of things became a crucial thing to be done, because of its need to human life, and so research should be concentrating on using game theory in making the best use of the security of this field.

Conclusion

As a result, to this study, the implementation of game theory in the field of network security was very useful. The survey that was done and presented in this thesis shows that the chances to have better defending strategies against the hacker's attacks are higher, and the losses are decreased by making the algorithms of network security much powerful with the aid of this theory.

Game theory models that represent the conflict between the administrator and the hacker were presented in this study, the equilibrium of these models was clarified and the application of game theory on many cases of network security has been illustrated such as: wiretap channel, IC infection check, denial of service problem solution… also the information warfare was studied in general, and the application of game theory in the field of securing the internet of things and the fog was elaborated.

Although the results of implementing game theory in the field of network security are mesmerizing, it is still used in its basic form, so it is recommended that the researchers make a lot of effort in this field to produce much more effective algorithms using this powerful tool (game theory), especially if we know that game theory is not used in some of the important fields yet such as the security of the fog, it is needless to say that this field of research isn't covered yet and it has a lot of potential.

References

[1] R. Antoon, **Network security 1 and 2 companion guide**. Pearson Education India, 2006.

[2] M. Ara, H. Reboredo, S. A. M. Ghanem, and M. R. D. Rodrigues**, *"A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer*," in 2012 IEEE International Conference on Communication Systems (ICCS),** 2012, pp. 60–64.

[3] F. M. Aziz, L. Li, J. S. Shamma, and G. L. Stüber, ***"Resilience of LTE eNode B against smart jammer in infinite-horizon asymmetric repeated zero-sum game*," Phys. Commun.,** vol. 39, p. 100989, 2020.

[4] S. G. Babajanyan, A. E. Allahverdyan, and K. H. Cheong, ***"Energy and entropy: Path from game theory to statistical mechanics,"*** **Phys. Rev. Res.,** vol. 2, no. 4, p. 43055, 2020.

[5] T. Basar***, "The Gaussian test channel with an intelligent jammer,"*** **IEEE Trans. Inf. Theory**, vol. 29, no. 1, *pp. 152–157, 1983.*

[6] R. Bragg, "Mark and Strassberg, Keith.**"," Netw. Secur. Complet. Ref.,** 2004.

[7] S. Buchegger and T. Alpcan, ***"Security games for vehicular networks*," in 2008 46th Annual Allerton Conference on Communication, Control, and Computing,** 2008, pp. 244–251.

[8] J. E. Canavan, **Fundamentals of network security**. Artech House, 2001.

[9] F. Carmichael, **A guide to game theory**. Pearson Education, 2005.

[10] T. Choi, A. Taleizadeh, and X. Yue, **"Game theory applications in production research in the sharing and circular economy era."** Taylor & Francis, 2020.

[11] M. Ciampa, ***Security+ guide to network security fundamentals*.** Cengage Learning, 2012.

[12] Cisco Systems, **"Fog Computing and the Internet of Things: Extend the Cloud to Where the Things** Are," 2015.

[13] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, S. S. Lyengar, ***"Game theory for cyber security and privacy,"*** **ACM Comput. Surv.,** vol. 50, no. 2, pp. 1–37, 2017.

[14] J. Eatwell, M. Milgate, and P. Newman, **Game theory**. Springer, 1989.

[15] I. Englander, ***"The Architecture of Computer Hardware, System Software, and Networking,"*** **An Inf. Technol. Approach,** p. 11, 2009.

[16] B. A. Forouzan and D. Mukhopadhyay, **Cryptography and network security (Sie).** McGraw-Hill Education, 2011.

[17] V. D. Gllgor, ***"On denial-of-service in computer networks,"*** **in 1986 IEEE Second International Conference on Data Engineering,** 1986, pp. 608–617.

[18] Z. He, Y. Zhang, B. Tak, and L. Peng, ***"Green Fog Planning for Optimal Internet-of-Thing Task Scheduling,"*** **IEEE Access,** vol. 8,

pp. 1224–1234, 2019.

[19] G. Hoglund and J. Butler, *Rootkits:* **subverting the Windows kernel.** Addison-Wesley Professional, 2006.

[20] K. Horák, Q. Zhu, and B. Bošanský, ***"Manipulating adversary's belief: A dynamic game approach to deception by design for proactive network security,"*** **in International Conference on Decision and Game Theory for Security,** 2017, pp. 273–294.

[21] H. B. Hubboub, ***"Denial of service attack in wireless sensor networks,"*** **Denial Serv. Attack Wirel. Sens. Networks**, 2010.

[22] M. O. Jackson, ***"A brief introduction to the basics of game theory,"*** **Available SSRN 1968579,** 2011.

[23] C. A. Kamhoua, H. Zhao, M. Rodriguez, and K. A. Kwiat, ***"A game-theoretic approach for testing for hardware trojans,"*** **IEEE Trans. Multi-Scale Comput. Syst.,** vol. 2, no. 3, pp. 199–210, 2016.

[24] T. Karthy, S. Vaishnavi, and A. Barath, ***"Game Theory in Military Decision: An Anecdote,"*** **in IOP Conference Series: Materials Science and Engineering,** 2020, vol. 912, no. 6, p. 62043.

[25] J. Katz, ***"Bridging game theory and cryptography: Recent results and future directions,"*** **in Theory of Cryptography Conference,** 2008, pp. 251–272.

[26] S. Kramer and J. C. Bradfield, ***"A general definition of malware,"*** **J. Comput. Virol.,** vol. 6, no. 2, pp. 105–114, 2010.

[27] C. B. Lee, C. Roedel, and E. Silenok, ***"Detection and characterization of port scan attacks,"*** **Univeristy California, Dep. Comput. Sci. Eng.**, 2003.

[28] X. Liang and Y. Xiao, ***"Game theory for network security,"*** **IEEE Commun. Surv. Tutorials,** vol. 15, no. 1, pp. 472–486, 2012.

[29] L. Liu, C. Huang, Y. Fang, and Z. Wang, **"Network Attack and Defense Game Theory Based on Bayes-Nash Equilibrium,"** 2019.

[30] Y. Liu, C. Comaniciu, and H. Man, **"A bayesian game approach for intrusion detection in wireless ad hoc networks,"** In Proc. 2006 workshop on Game theory for communications and networks, 2006.

[31] Y. Li, S. Qiao, Y. Deng, and J. Wu, ***"Stackelberg game in critical infrastructures from a network science perspective,"*** **Phys. A Stat. Mech. its Appl.,** vol. 521, pp. 705–714, 2019.

[32] K. Lye and J. M. Wing, ***"Game strategies in network security,"*** **Int. J. Inf. Secur.,** vol. 4, no. 1–2, pp. 71–86, 2005.

[33] S. Moothedath, D. Sahabandu, J. Allen, A. Clark, L. Bushnell, W. Lee, R. Poovendran, ***"Dynamic Information Flow Tracking for Detection of Advanced Persistent Threats: A Stochastic Game Approach,"*** **arXiv Prepr. arXiv***2006.12327*, 2020.

[34] R. B. Myerson, ***Game theory.*** **Harvard university press**, 2013.

[35] J. F. Nash Jr, "**John Forbes Nash, Jr**.," **Marian. Cook, comp. Math. An outer view Inn. world, Princet. Univ. Press. Princet.,** pp. 42–43,

2009.

[36] M. J. Osborne**,** ***An introduction to game theory*****, vol. 3, no. 3. Oxford university press New York**, 2004.

[37] P. G. Palafox-Alcantar, D. V. L. Hunt, and C. D. F. Rogers, ***"The complementary use of game theory for the circular economy: A review of waste management decision-making methods in civil engineering,"*** **Waste Manag., vol**. 102, pp. 598–612, 2020.

[38] I. Park, ***"Two-Level Game and Politics of the United States–North Korea Negotiation,"*** **Korean J. Def. Anal.,** vol. 32, no. 3, pp. 437–456, 2020.

[39] E. Rasmusen, ***Games and information: An introduction to game theory,*** no. 519.3/R22g. Blackwell Oxford, 1989.

[40] T. Robertazzi, ***Basics of computer networking*****. Springer Science & Business Media**, 2011.

[41] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, ***"A survey of game theory as applied to network security,"*** **in 2010 43rd Hawaii International Conference on System Sciences,** 2010, pp. 1–10.

[42] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Hjorungnes, ***"Physical layer security: Coalitional games for distributed cooperation,"*** **in 2009 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks,** 2009, pp. 1–8.

[43] S. Shen, H. Ma, E. Fan, K. Hu, S. Yu, J. Liu, Q. Cao, ***"A non-***

cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," **J. Netw. Comput. Appl.,** vol. 91, pp. 26–35, 2017.

[44] R. Shimonski, **CEH v9: Certified Ethical Hacker Version 9 Study Guide.** John Wiley & Sons, 2016.

[45] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, ***"A game theoretic defence framework against DoS/DDoS cyber attacks,"*** **Comput. Secur.,** vol. 38, pp. 39–50, 2013.

[46] T. M. Thomas and D. Stoddard, ***Network Security First-Step: NETWORK SECURITY FIRST ST_p2*****. Cisco Press**, 2011.

[47] X. Wang, D. Jia, S. Gao, C. Xia, X. Li, and Z. Wang, "***Vaccination behavior by coupling the epidemic spreading with the human decision under the game theory,"*** **Appl. Math. Comput.,** vol. 380, p. 125232, 2020.

[48] Z. G. Wang, Y. Lu, and X. Li, "**Optimal network defense strategy selection based on Bayesian game," Int. J. Secur. Networks**, vol. 15, no. 2, pp. 67–77, 2020.

[49] H. Wu and W. Wang, ***"A game theory based collaborative security detection method for Internet of Things systems,"*** **IEEE Trans. Inf. Forensics Secur.,** vol. 13, no. 6, pp. 1432–1445, 2018.

[50] J. Yang, B. Jiang, Z. Lv, and K. K. R. Choo, ***"A task scheduling algorithm considering game theory designed for energy management***

in cloud computing," **Futur. Gener. Comput. Syst.,** vol. 105, pp. 985–992, 2020.

[51] Q. Yan, F. R. Yu, Q. Gong, and J. Li, ***"Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges,"*** **IEEE Commun. Surv. tutorials,** vol. 18, no. 1, pp. 602–622, 2015.

Websites:

[52] T. Bell ‹***"csoonline‹" 12 4 2018*** *].Online .[Available:*

https://www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html] [Accessed 2020 /11 /29]

[53] M. Levine, and J. Date ‹***"abcnews‹"*** 9 /7 /2015. Online .[Available:

https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731] .[Accessed 2020 /11/ 29]

[54] wikipedia, ***"wikipedia,"*** 27 /10 /2020. [Online]. Available:

https://en.wikipedia.org/wiki/Hannibal. [Accessed 29 /11 /2020].

[55] wired.com ‹***"wired.com‹"*** 23 11 1999. [Online] .[Available:

https://www.wired.com/1999/11/cracker-launches-attack-on-nasa] . [Accessed 2020 11 29]

جامعة النجاح الوطنية

كلية الدراسات العليا

النمذجة الرياضية لنظرية اللعبة وتطبيقاتها في أمن الشبكات

إعداد

حمزة سليم حسن حرزالله

إشراف

أ.د. ناجي قطناني

قدمت هذه الأطروحة استكمالاً لمتطلبات الحصول على درجة الماجستير في الرياضيات المحوسبة بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين

2021

النمذجة الرياضية لنظرية اللعبة وتطبيقاتها في أمن الشبكات

إعداد

حمزة سليم حسن حرزالله

إشراف

أ.د. ناجي قطناني

الملخص

كنتيجة لهذه الدراسة، فإننا نجد أن تطبيق نظرية الألعاب في مجال أمن الشبكات مفيدًا جدًا. يُظهر البحث الذي تم إجراؤه وتقديمه في هذه الأطروحة أن فرص الحصول على استراتيجيات دفاعية أفضل ضد هجمات المتسللين ستكون أعلى باستخدام نظرية اللعبة، ويتم تقليل الخسائر عن طريق جعل خوارزميات أمان الشبكة قوية جدًا بمساعدة هذه النظرية.

تم عرض نماذج نظرية الألعاب التي تمثل الصراع بين المسؤول عن الشبكة والهاكر في هذه الدراسة، وتم توضيح توازن هذه النماذج، كما تم توضيح تطبيق نظرية اللعبة على العديد من حالات أمان الشبكة مثل: قناة التنصت على المكالمات الهاتفية، والتحقق من عدوى شرائح IC ، حل مشكلة رفض الخدمة... كما تمت دراسة حرب المعلومات بشكل عام، وتم تطوير تطبيق نظرية الألعاب في مجال تأمين إنترنت الأشياء وانترنت الأشياء الضبابي.

على الرغم من أن نتائج تطبيق نظرية الألعاب في مجال أمن الشبكات مذهلة، إلا أنها لا تزال مستخدمة في شكلها الأساسي، لذلك يوصى بأن يبذل الباحثون الكثير من الجهد في هذا المجال لإنتاج خوارزميات أكثر فاعلية باستخدام هذه الأداة القوية (نظرية اللعبة)، خاصة إذا علمنا أن نظرية الألعاب لم يتم استخدامها في بعض المجالات المهمة حتى الآن مثل أمان الانترنت الضبابي، فلا داعي للقول إن هذا المجال من البحث لم يتم تغطيته بعد ولديه الكثير من الإمكانات.