# A Hypergame Model for Information Security

Yadigar Imamverdiyev

***Abstract*—Game theory is one of the most powerful mathematical tools to model information security decision making. However, in game theory it is assumed that all the players have complete knowledge about each player's strategies, preferences, and decision rules used. This assumption is very strong, in reality there is often significant information asymmetry between players. In many real world situations, decision makers do not always have all the information about each player's true intentions, strategies or preferences. Consequently, they have to perceive the situation from their own points of view, and may err in their perceptions. Since the early developments of game theory attempts have been made to incorporate misperceptions in game models of either incomplete or imperfect information. However, most of these attempts are based on quantities (as probabilities, risk factors, etc.) which are too subjective in general. In this paper, we consider a special family of games of incomplete information called hypergames. Hypergame theory extends classical game theory with the ability to deal with differences in players' misperceptions. In the context of hypergames, few works have addressed the study of information security decision making. This paper presents a hypergame approach as an analysis tool in the context of information security. The proposed two level hypergame models defender's and attacker's perception of the information security situation as a series of games. Finally, we conclude and present some future work..**

***Index Terms*— information security; game theory; hypergame;**

## I. Introduction

In the modern highly networked world the cost of decisions on information security is very high as it concerns interests of many stakeholders. Therefore, such a decision must be well founded and based on a well-studied theoretical models and best practices. Game theory is a mathematical method of studying the best strategies in games and can provide valuable insights into strategic information security decisions [1].

Game theory is a convenient tool to analyze the interactions of economic agents and it was firstly applied to economy, now it is applied to military strategies, international relations, political science, and evolutionary biology and etc.

In information security area, the interactive process of the attackers and defenders is a game process. Thus, game theory can be used to predict the behavior of attacks and to support decision making.

Information security, when viewed from a game theoretic perspective, can be seen as a game comprising multiple players; the attackers (malicious users) and the defenders (network/system administrators). The benefits of quantifying information security using game-theoretic approach are enormous. Most importantly it may help network administrator to find the optimal defense strategies of a system and to calculate the expected loss associated with different defense strategies [2].

Hypergame theory extends classical game theory with the ability to deal with differences in players' misperceptions [3]. In the context of hypergames, few works have addressed the study of information security decision making. This paper presents a hypergame approach as an analysis tool in the context of information security. The proposed two level hypergame models defender's and attacker's perception of the information security situation as a series of games.

The rest of this paper is organized as follows. In the next section, we shall present an overview of application of game theory in information security. Section 3 presents limitations of game theory. In section 4, we give a brief introduction to hypergames. Finally, Section 5 presents a hypergame model between attacker and defender.

## II. Related Work: Game Theory In Information Security

Game theory is a branch of applied mathematics, exploring models of decision making under different interests of the parties (players), where each party seeks to influence the development of the situation in their own interests. Each side has its own purpose and uses some strategy that can lead to gain or losing - depending on the behavior of other players. Game theory helps to choose the best strategy in the light of the views of other participants, their resources and their possible actions.

During the game players can choose and implement a strategy from a set of different behavioral options (strategy space), in order to maximize the payoff they are receiving as an outcome of the game. In game-theoretic analysis the principle of the Nash equilibrium plays a critical role. Game in normal form is characterized by multiple participants or players, each of whom is given a set of possible strategies of behavior and the payoff function. Under the principle of Nash equilibrium rational players have strategies that form equilibrium (Nash), i.e. there is a set of strategies in which the individual player cannot increase his/her gains by changing its strategy when strategies of the other players are fixed.

There are lots of papers on the application of the game theory to information security issues. Game theory has been used to model several areas of information security like network security, intrusion detection, information warfare

Manuscript received July 15, 2013.

Yadigar Imamverdiyev is with the Institute of Information Technology of Azerbaijan National Academy of Sciences, AZ1141, B.Bahabzade 9, Baku, Azerbaijan (Phone: 994 12-510-42-53; fax: 994 12-539-61-21; e-mail: yadigar@lan.ab.az).

and security investment.

Roy et al. provide an excellent review of different approaches to game theory as it can be applied to network security [4]. Also a good overview of applications of game theory in information security can be found in [5, 6, 7].

Qu et.al. [8] presents a game theoretic model as a defense mechanism against a classic bandwidth consuming DoS/DDoS attack. The interaction between the attacker and the defender is modeled as a two-player non-zero-sum game in two attack scenarios: (i) one single attacking node for Denial of Service (DoS) and (ii) multiple attacking nodes for Distributed DoS (DDoS). The defender's challenge is to determine optimal firewall settings to block rogue traffics while allowing legitimate ones.

Modeling of intrusion detection systems (IDS) using game theory attracts more attention. In [9], Alpcan and Başar introduce a a two-person, nonzero-sum, non-cooperative game model with dynamic information where the attacker has two choices, i.e., launching an attack or doing nothing, while the defender’s choices are to trigger or not its (costly) detection scheme. Nash equilibrium solutions in closed form are obtained for specific subgames.

Patcha and Park [10] have extended the model proposed by Alpcan and Başar to include mobile ad hock networks, and have analyzed the interaction between an attacker and a host-based IDS as a dynamic two player non-cooperative game.

The same kind of attacker-defender game is studied in [11]. The number of strategies for each player is larger than two: several attack and countermeasure types are considered.

[12] presents some very similar but concrete situations of network security (information warfare) games, with specific numerical values, that also lead to simple strategy sets.

The stochastic game approach is used in [13] to model attacks directed against specific applications, against communication capacities, or against databases. [14, 15] apply stochastic game models as well, to study other specific attack scenarios, and numerically compute mixed Nash strategies. The Bayesian approach is also considered in security games, for example in [12]. The authors consider two types of attackers, namely “normal users” whose behavior is only driven by selfishness, and “malicious nodes” that intend to maximize the damage done. The defender has a priori belief about the probability of its opponent being of each type, and updates that probability as he observes the attacker`s moves. That belief is also used to determine the probability of using the detection mechanisms.

Another important domain where it is believed that game theory could be applied is the case of worm propagation [16]. In [16], the strategy of players is to choose the best quarantining strategy for the detector, while the worm chooses a scanning rate.

Besides the direct game-theoretic modelling of interactions between malicious attacks and protection strategies, game theory can be applied to economic issues of information security [17].

Kunreuther and Heal [18] recently introduced an interesting game-theoretic model for problems of interdependent security, in which a large number of players must make individual investment decisions related to security but the ultimate safety of each participant may depend in a complex way on the actions of the entire population.

## III. Limitations of Present Research

Many of the current game-theoretic security approaches are based on static games with perfect information or games with complete information [4]. However, in reality a defender often faces a dynamic game with incomplete and imperfect information against the attacker. Some of the current models involving dynamic game with incomplete and imperfect information are specific to mobile ad hoc networks [10] while others do not consider a realistic attack scenario [4].

In particular, Roy et al. [4] point out that some of the limitations of the present research are: (a) Current stochastic game models only consider perfect information and assume that the defender is always able to detect attacks; (b) Current stochastic game models assume that the state transition probabilities are fixed before the game starts and these probabilities can be computed from the domain knowledge and past statistics; (c) Current game models assume that the players’ actions are synchronous, which is not always realistic.

In usual game models it is assumed that each player knows payoff functions and set of strategies of other players. In fact, this condition is often not fulfilled. If a player does not know, payoff functions of other players, then talk about the Nash equilibrium becomes meaningless.

All the complete-knowledge games rely on accurate knowledge of the payoff functions. In real-life any player must observe and make as realistic assumptions about these payoffs (costs) as possible. If the observations about an opponent’s costs are unrealistic, a player can end up choosing a non-optimal strategy.

Since the early developments of game theory attempts have been made to incorporate misperceptions in game models of either incomplete or imperfect information. However, most of these attempts are based on quantities (as probabilities, risk factors, etc.) which are too subjective in general. In this paper, we consider a special family of games of incomplete information called hypergames. In the hypergames misperception or misunderstanding by players are explicitly assumed.

Sasaki and Kijima [19] discuss the relationships between two models of games with incomplete information, hypergames [3] and Bayesian games [20]. The authors show that any hypergame can naturally be reformulated in terms of Bayesian games in an unified way and prove that some equilibrium concepts defined for hypergames are in a sense equivalent to those for Bayesian games.

## IV. A brief introduction to hypergames

Before introducing the proposed method, we need to explain the hypergame framework.

**Definition 1. Simple hypergame**

A simple hypergame of players $p$ and $q$ is a pair of $(G_p, G_q)$.

We have $G_p = (S_p, S_{qp}, \geq_p, \geq_{qp})$ and $G_q = (S_{pq}, S_q, \geq_{pq}, \geq_q)$.

In $G_p$, $S_p$ denotes a set of strategies of $p$ while $S_{qp}$ denotes a set of strategies which the player $p$ recognizes that $q$ possesses. That is, $p$ perceives that $S_{qp}$ is the set of strategies of $q$. $\geq_p$ denotes a preference ordering on $S_p \times S_{qp}$ of $p$ while $\geq_{qp}$ is a preference ordering on $S_p \times S_{qp}$ that $p$ assumes that $q$ holds. That is, $p$ perceives that $q$'s preference ordering is $\geq_{qp}$. We define $G_q$ in a similar way.

The definition implies that each player independently perceives the problematic situation without mutual understanding. The rationality of a simple hypergame is defined as follows:

**Definition 2. Nash equilibrium of simple hypergame** For a simple hypergame ($G_p$, $G_q$) of players $p$ and $q$, $(s^{p*}, s^{qp*}) \in S_p \times S_{qp}$ is a Nash equilibrium of $G_p = (S_p, S_{qp}, \geq_p, \geq_{qp})$ if and only if we have $(\forall s^p \in S_p)(s^{p*}, s^{qp*}) \geq_p (s^p, s^{qp*})$ and $(\forall s^{qp} \in S_{qp})(s^{p*}, s^{qp*}) \geq_{qp} (s^{p*}, s^{qp})$.

This definition shows that if $(s^{p*}, s^{qp*})$ is a Nash equilibrium of $G_p$, then $p$ believes that there is no incentive for either of the players to change their strategy as long as the other does not change its strategy.

In the simple hypergame we assume no communication between the players and they make decisions completely independent based on their own subjective ($G_p$ or $G_q$).

Hypergames are analysed by using Fraser and Hipel's [21] game analysis algorithm. First a new game is constructed to represent the relative aspect of the hypergame that is to be analysed. This is achieved by taking a preference vector for each player from a game that represents their perception of the situation and combining these together to construct the new game.

Many hypergame analyses have been published, showing its use in modelling conflicts and their resolutions. Hypergame analysis methods but can be applied to military conflicts, international disputes [22], economic treaties and agreements [23], social issues [24] and etc. Hypergame approach also was applied to information warfare [25] and cybersecurity [26].

## V. A HYPERGAME MODEL

Let us consider two levels of  hypergame formally.

Game $G$ can be briefly defined as set of preference vectors of all players. Let $V_A$ be the preference vector of the Attacker, and $V_D$ – the preference vector of the Defender. Then, a game in which the Attacker and the Defender are the only players can be defined as $G = \{V_A, V_D\}$. In games with complete information players evaluate preference vectors of each other fully and adequately, therefore, they all play in the same game.

If in the two-person game, both players are playing the same game $G$, i.e. correctly estimate preference vectors of each other, then we have zero level hypergame. If at least one of the players mistakenly interprets the preference vector of another player, then there is the first level hypergame. If a player is aware of misperception of the second player, there is the second level hypergame.

Let $H^1$ denotes the first level hypergame. In this game the players are playing different games. Let $V_{ij}$ be the preference vector of player $i$ from the point of view of player $j$. Then for two players – the Attacker and the Defender – we have the following types of reflexive preference vectors:

$V_{AA}$ – preference vector of the Attacker from the point of view of the Attacker;

$V_{DA}$ – preference vector of the Defender from the point of view of the Attacker;

$V_{AD}$– preference vector of the Attacker from the point of view of the Defender;

$V_{DD}$ – preference vector of the Defender from the point of view of the Defender.

The game, played by the Attacker in the first level hypergame $H$, is denoted as $G_A = \{V_{AA}, V_{DA}\}$, and the game is played by the Defender in the same hypergame – as $G_D = \{V_{AD}, V_{DD}\}$. Accordingly, first level hypergame itself is defined as $H = \{G_A, G_D\}$.

In matrix notation the first level hypergame is shown in Table 1.

TABLE 1

THE FIRST LEVEL HYPERGAME $H^1$ IN A MATRIX FORM

| Players | Game | |
|---|---|---|
| | Attacker | Defender |
| Attacker | $V_{AA}$ | $V_{AD}$ |
| Defender | $V_{DA}$ | $V_{DD}$ |
| | $G_A$ | $G_D$ |

According to the conditions of the first level hypergame $H$, the Defender wrongly interprets preference vector of the Attacker, that is, $V_{AA} \neq V_{AD}$ is true, but the Attacker correctly estimates the preference vector of the Defender, $V_{DA} = V_{DD}$.

Even more realistic model of the analyzed situation is represented by the second level hypergame, which, as noted, occurs when one of the players knows about the misinterpretation of his position by another player.

Let $H_A^1$ denotes the first level hypergame of the Attacker and $H_S^1$ denotes the first level hypergame of the Defender. Here $H_A^1 = \{G_{AA}, G_{DA}\}$, and $H_D^1 = \{G_{AD}, G_{DD}\}$ where:

$G_{AA}$ = game $G_A = \{V_{AA}, V_{DA}\}$ from the point of view of the Attacker,

$G_{DA}$ = game $G_D = \{V_{AD}, V_{DD}\}$ from the point of view of the Attacker,

$G_{AS}$ = game $G_A = \{V_{AA}, V_{DA}\}$ from the point of view of the Defender,

$G_{SS}$ = game $G_S = \{V_{AD}, V_{DD}\}$ from the point of view of the Defender.

Table 2 shows the second level hypergame $H^2$ in a matrix form.

TABLE 2
THE SECOND LEVEL HYPERGAME $H^2$ IN A MATRIX FORM

| Players | Game | |
|---|---|---|
| | Attacker | Defender |
| Attacker | $G_{AA}$ | $G_{AD}$ |
| Defender | $G_{DA}$ | $G_{DD}$ |
| | $H_A^1$ | $H_D^1$ |

Analysing a hypergame involves analysing each of the games for stability and then comparing the results to find stable equilibriums for the hypergame. Algorithm for calculation of stable outcomes and equilibrium points in the second level hypergame $H^2$ is the following.

1. Sequentially analyze the games $G_{AA}$, $G_{AD}$, $G_{DA}$, and $G_{DD}$, by comparing corresponding preference vectors for each of them.

2. Analyze the first level hypergame $H_A^1$, taking into account information about the stability of outcomes only in the preference vectors $V_{AA}$ in the game $G_{AA}$ and $V_{DD}$ in the game $G_{DA}$. Compute the set of equilibrium points of the hypergame $H_A^1$: $E_H$ for the attacker $E_H = E_{AA} \cap E_{DA}$ (with respect to games $G_{AA}$ and $G_{DA}$).

3. Analyze the first level $H_S^1$, taking into account information about the stability of outcomes only in the preference vectors $V_{AA}$ in the game $G_{AD}$ and $V_{DD}$ in the game $G_{DD}$. Compute the set of equilibrium points of the hypergame $H_D^1$: $E_H$ for the defender $= E_{AD} \cap E_{DD}$ (with respect to games $G_{AD}$ and $G_{DD}$).

4. Analyze the second level hypergame $H^2$ as a whole, we compute the set of points of equilibrium solutions of the game, ie compute the result of the intersection of the sets of stable outcomes of the preference vector $V_{AA}$ in the game $G_{AA}$ and the preference vector $V_{DD}$ in the game $G_{DD}$: $E = E_{AA} \cap E_{DD}$ (with respect to games $G_{AA}$ and $G_{DD}$).

To show how to calculate the stability of the outcomes and the general solution of the game, we introduce some new notations and definitions.

Let a certain outcome $q$ be given. If player $A$ at a constant strategy of his opponent $D$ can make the best choice, i.e. find the outcome of a large preference weight (utility) than $q$, then $A$ has a unilateral improvement of their position. Let $UI_A$ ($UI_D$) be the set of outcomes that represent a unilateral improvement of the outcome $q$ for player $A$ [player $D$].

Let a certain outcome $q$ is given. If player $A$ at a fixed strategy of his opponent $D$ can make the best choice, ie find the outcome of a large preference weight (utility) than $q$, then $A$ has a unilateral improvement of their position. Let $UI_A(q)$ [$UI_D(q)$] is the set of outcomes that represent a unilateral improvement of the outcome $q$ for player $A$ [player $D$].

If player $A$ can make equal or worst option at a fixed strategy of the opponent's $D$, ie find the outcome of the same or smaller weight (utility) than $q$, then $A$ has the unilateral disimprovement of its position. Let $UD_A(q)$ denotes the set of outcomes representing unilateral disimprovement of the outcome $q$ for player $A$ (player $D$).

Assume that player $A$ has not a unilateral improvement of the outcome of $q$, i.e $UI_A = \varnothing$. All outcomes $q$, which satisfy this condition will be called rationally stable and denoted by the letter $r$.

Sanction is a reaction of the player in the possible improvement of the position of his opponent, which causes the latter to the outcome whose utility is less than or equal to the value of its original position.

So if the opponent knows about the possible sanctions, it would not make any sense to leave it, because if he does, the result is nothing to gain. Sanctioned position is stable for him, and he can include it in the set of expected rational solutions to the game.

Suppose player A has a non-empty set of $UI_A(q)$ for some outcome $q$. We also assume that for every $UI_A(q)$ an opponent of player $A$ – player $D$ – has its $UI_D$ or $UD_D$, whose utility for $A$ less than or equal to the utility of the outcome $q$. Then $A$ will act rationally if he/she refrains from unilateral improvement of its position in view of the possible sanctions from player $D$. Outcom $q$, whose stability for a player based on a possible sanction of his opponent will be called sequentially sanctioned and denoted by the letter $s$.

Suppose player $A$ has a non-empty set of $UI_A(q)$ for the given outcome $q$. If at one $UI_A$ of the opponent of player $A$ – player $D$ – there are no sanctions, then the outcome $q$ will be called unstable and denoted by the letter $u$.

All rational, or sequentially sanctioned outcomes for $A$ represent for him the possible solutions to the game.

It is noted by Wang, Hipel and Fraser [27] that solutions to hypergames may not necessarily be created by outcomes that are stable for all players and that it is possible that an outcome that is unstable individually for players may actually be an equilibrium for the hypergame.

## VI. A NUMERICAL EXAMPLE

For a numerical illustration of the above described approach, we use a modified version of the network security model from [9]. In Alpcan and Başar's model the attacker has two choices, i.e. launching an attack or doing nothing, while the defender's choices are to trigger or not its defense mechanism. In this study the action spaces of the players are limited only for illustrative purpose. For this purpose we also assume that actions of each player are mutually exclusive, so that it can initiate only one action at a time.

Let the attacker has two actions that he/she may take:

# 1 – Attack scenario 1;

#2 – Attack scenario 2.

Let assume that actions for the defender are the following:

# 3 – Defense Mechanism 1;

# 4 – Defense Mechanism 2;

# 5 – Defense Mechanism 3.

As noted above, hypergames are games with imperfect information. This means, at least one player has misperceptions about the game elements. Let`s assume that in this game the players have the following misperceptions:

– Players are misinterpreting the preference vectors of each other;

– The attacker is not aware about the third action available to the Defender.

The second level hypergame consists of the following four games:

– Game $G_{AA}$: The Attacker's perception of the Attacker's game;

– Game $G_{DA}$: The Attacker's perception of the Defender's game;

– Game $G_{AD}$: The Defender's perception of the Attacker's game;

– Game $G_{DD}$: The Defender's perception of the Defender's game.

From the set of actions the set of players' strategies is formed. (A strategy is any set of actions taken by a player.) The strategies of all the players together is called an outcome. The number of outcomes equals to $2^n$, where $n$ - the number of all actions available to the players. However not all of these outcomes may be feasible. Each of these actions can be performed or not performed. Therefore, in this game formally there are $2^4 = 16$ outcomes. But, given that the actions of the attacker and defender are mutually exclusive, all outcomes in which both of these actions are performed at the same time, should be excluded as practically infeasible. Also, assume that players have to take one of the actions. Therefore, in the game $G_{AA}$ ($G_{DA}$, $G_{AD}$) there are 16-12 = 4 outcomes.

The next step of the hypergame analysis is to identify the preferences of the players. We assume that both the Attacker and Defender have different utility functions for outcomes and outcomes are ordered by each player according to their individual preferences from the most preferred to least preferred (eg 4 = the most preferred; 3 = the next most preferred; 2 = the next least preferred; l = the least preferred).

We solve this numerical example using the HYPANT hypergame theory analysis tool [28]. Note that hypergame models must be written in custom HML (Hypergame Modeling Language) format by a person in order to analyze them by HYPANT.

The results of calculating of individual preference vectors and stability of outcomes for the Attacker ($A$) and Defender ($D$) in the game $G_{AA}$ are given in Table 3.

In Table 3, a sign $Y$ indicates that the corresponding action is performed, $N$ - the corresponding action is not performed. Outcomes are numbered from 1 to 4.

The preference vector indicates the players ranking of the possible outcomes. Preference vectors for the respective outcomes are given on the first row of Table 3 (for the Attacker), and on the fourth row (for the Defender).

TABLE 3
THE SECOND LEVEL HYPERGAME $G_{AA}$

| *A*'s preference vector | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| #1 | Y | N | N | Y |
| #2 | N | Y | Y | N |
| *D*'s preference vector | 4 | 2 | 3 | 1 |
| #3 | Y | N | Y | N |
| #4 | N | Y | N | Y |
| Outcome | 1 | 2 | 3 | 4 |
| Stability for *A* | *r* | *r* | *s* | *u* |
| Stability for *D* | *u* | *r* | *u* | *r* |
| Equilibriums | | *E* | | |

Below we show calculation of stability of outcomes for the Attacker:

$q = 1$; $UI_A(1) = \varnothing$. It means that the outcome $q = 1$ is rational for $A$ and it is marked with $r$.

$q = 2$; $UI_A(2) = \varnothing$. It means that the outcome $q = 2$ is rational for $A$ and it is marked with $r$.

$q = 3$; $UI_A(3) = \{1\}$. $UI_D(1) = \{4\}$. $w_D(4) = 1 \succ w_A(3) = 3$.
It means that the outcome $q = 3$ is sequentially sanctioned for $A$.

$q = 4$; $UI_A(4) = \{2\}$. $UD_D(2) = \{3\}$. $w_D(3) = 3 \succ w_A(4) = 4$.
It means that the outcome $q = 4$ is unstable for $A$.

The overall stability shows which outcomes are possible solutions to the hypergame. Equilibrium for the game $G_{AA}$ is $E_{AA}$= {{#2 Attack scenario 2, #4 Defense mechanism 2}}.

The results of games $G_{DA}$, $G_{AD}$, and $G_{DD}$ are given in Table 4, 5, 6, respectively. Note that the game $G_{DD}$ has 6 outcomes.

TABLE 4
THE SECOND LEVEL HYPERGAME $G_{DA}$

| *A*'s preference vector | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| #1 | Y | N | N | Y |
| #2 | N | Y | Y | N |
| *D*'s preference vector | 4 | 2 | 3 | 1 |
| #3 | Y | N | Y | N |
| #4 | N | Y | N | Y |
| Outcome | 1 | 2 | 3 | 4 |
| Stability for *A* | *r* | *r* | *s* | *u* |
| Stability for *D* | *u* | *r* | *u* | *r* |
| Equilibriums | | *E* | | |

Equilibrium for the game $G_{DA}$ is $E_{DA}$= {{#2 Attack scenario 1, #4 Defense mechanism 2}}.

The set of equilibrium points of the hypergame $H_A^1$ for the attacker is $E_H = E_{AA} \cap E_{DA}$ ={{#2 Attack scenario 2, #4 Defense mechanism 2}}.

TABLE 5
THE SECOND LEVEL HYPERGAME $G_{AD}$

| *A*'s preference vector | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| #1 | Y | N | N | Y |
| #2 | N | Y | Y | N |
| *D*'s preference vector | 4 | 2 | 3 | 1 |
| #3 | Y | N | Y | N |
| #4 | N | Y | N | Y |
| Outcome | 1 | 2 | 3 | 4 |
| Stability for *A* | *r* | *r* | *s* | *u* |
| Stability for *D* | *u* | *r* | *u* | *r* |
| Equilibriums | | *E* | | |

Equilibrium for game $G_{AD}$ is $E_{AD}$ = {{#2 Attack scenario 2, #4 Defense mechanism 2}}.

TABLE 6
THE SECOND LEVEL HYPERGAME $G_{DD}$

| *A*'s preference vector | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| #1 | Y | N | N | Y | N | Y |
| #2 | N | Y | Y | N | Y | N |
| D's preference vector | 6 | 5 | 4 | 3 | 1 | 2 |
| #3 | Y | Y | N | N | N | N |
| #4 | N | N | Y | N | N | Y |
| #5 | N | N | N | Y | Y | N |
| Outcome | 1 | 2 | 3 | 4 | 5 | 6 |
| Stability for *A* | *r* | *s* | *r* | *r* | *s* | *u* |
| Stability for *D* | *u* | *u* | *u* | *s* | *r* | *r* |
| Equilibriums | | | | *E* | *E* | |

Equilibriums for the game $G_{DD}$ is $E_{DD}$ = {{#1 Attack scenario 1, #5 Defense mechanism 3}, {#2 Attack scenario 2, #5 Defense mechanism 3}}.

The set of equilibrium points of the hypergame $H_D^1$ for the Defender is $E_H$ ={{#1 Attack scenario 1, #5 Defense mechanism 3}, {#2 Attack scenario 2, #5 Defense mechanism 3}}.

## VII. Conclusion

We have investigated possible usage of hypergame theory approach for developing decision making framework in information security. The proposed two level hypergame approach models defender's and attacker's perception of the information security situation as a series of games. We also have given an illustrative numerical example on deciding the best attack and defense mechanisms in the context of network security.

## References

[1] D. Fudenberg, J. Tirole, Game Theory, Massachussetts, MIT Press, 1995.

[2] K. Sallhammar, S. J. Knapskog, B. E. Helvik "Using stochastic game theory to compute the expected behavior of attackers," *International Symposium on Applications and the Internet (Saint'2005)*. Trento, Italy, 2005, pp. 102-105.

[3] P. G. Bennett, "Toward a theory of hypergames," Omega, vol. 5, no. 6, pp. 749-751, 1977.

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

[5] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, December 2011

[6] A. Singh, A. Lakhotia, A. Walenstein, "Malware antimalware games," in *Proc. 5th International Conference on Information-Warfare & Security (ICIW)*, 2010, pp. 319-327.

[7] P. Maillé, P. Reichl and B. Tuffin, "Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management," *Springer Optimization and Its Applications*, vol. 46, pp. 33-53, 2011.

[8] Q. Wu, S. Shiva, S. Roy, C. Ellis, V. Datla, "On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks," in *Proc. of the 2010 Spring Simulation Multiconference (SpringSim'10)*, Article No. 159.

[9] T. Alpcan, T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in Proc. of the 42nd Conference on Decision and Control. Maui, HI (2003), vol.3, pp. 2595-2600.

[10] A. Patcha, J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Intl Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.

[11] S. Bistarelli, M. Dall'Aglio, P. Peretti, "Strategic games on defense trees," in: Proc. of 4th Intl Workshop on Formal Aspects in Security and Trust (FAST'06), LNCS 4691, pp. 1–15, Hamilton, Ontario, Canada, 2006.

[12] J. Jormakka and J. V. E. Mölsä, "Modelling Information Warfare as a Game," *Journal of Information Warfare*, vol. 4, no. 2, pp. 12-25.

[13] K.-W. Lye and J. M. Wing, "Game strategies in network security," in *Proc. Workshop on Foundations of Computer Security*, 2002.

[14] Y. Liang, B. Li, H. Wang, "Dynamic awareness of network security situation based on stochastic game theory," in *Proc. 2nd International Conference on Software Engineering and Data Mining (SEDM)*, 2010, pp. 101-105.

[15] K. Sallhammar, B. E. Helvik, S. J. Knapskog, "A game-theoretic approach to stochastic security and dependability evaluation," in Proc. of 2nd IEEE Intl Symposium on Dependable, Autonomic and Secure Computing (DASC), 2006.

[16] A. Ganesh, D. Gunawardena, P. Jey, L. Massouli´e, J. Scott, "Efficient quarantining of scanning worms: Optimal detection and co-ordination," IEEE INFOCOM 2006. Barcelona, Spain (2006)

[17] H. Cavusoglu, S. Raghunathan, W. Yue, "Decision-theoretic and game theoretic approaches to IT security investment," J Manage Inform Syst, vol. 25, 281, 2008.

[18] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty (Special Issue on Terrorist Risks)*, vol. 26, no. 2, pp. 231-249, 2003.

[19] Y. Sasaki, K. Kijima, "Hypergames and bayesian games: A theoretical comparison of the models of games with incomplete information," *Journal of Systems Science and Complexity*, vol. 25, no. 4, pp. 720-735, 2012.

[20] Harsanyi J.C., "Games with incomplete information played by Bayesian players," *Management Science*, vol. 14, no. 3, pp. 159-182, 1967.

[21] N. M. Fraser, and K. W. Hipel, *Conict Analysis, Models and Resolutions*, Elsevier Science Publishing Co. Inc., New York, 1980.

[22] N. M. Fraser, and K. W. Hipel, "Metagame analysis of the poplar river conflict," *Journal of the Operational Research Society*, vol. 31, pp. 377-385, 1980.

[23] M. Giesen, and P. Bennett, "Aristotle's Fallacy: A Hypergame in the Oil Shipping Business," *Omega*, vol. 7, no. 4, pp. 309-320, 1979.

[24] P. G. Bennett, M. R. Dando, and R. G. Sharp, "Using hypergames to model difficult social issues: an approach to the case of soccer hooliganism," *Journal of the Operational Research Society*, vol. 31, no. 7, pp. 621-635, 1980.

[25] Kopp C., "Shannon, hypergames and information warfare," *Journal of Information Warfare*, vol. 2, no. 2, pp. 108-118, 2002.

[26] J. T. House, and G. Cybenko, "Hypergame Theory applied to Cyber Attack and Defense," *SPIE Defense and Security*, Orlando April 2010. (Proc. SPIE 7666, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IX, 766604 (May 03, 2010); doi:10.1117/12.852338)

[27] M. Wang, K. W. Hipel, and N. M. Fraser, "Modeling misperceptions in games," *Behavioral Science*, vol. 33, pp. 207–223, 1988.

[28] L. Brumley, "HYPANT: A Hypergame Analysis Tool" http://www.csse.monash.edu.au/hons/se-projects/2003/Brumley/

**Yadigar Imamverdiyev** received the MSc degree in applied mathematics from Azerbaijan State Oil Academy, Baku, Azerbaijan, in 1989, and the PhD degree in technical sciences from the Institute of Information Technology of Azerbaijan National Academy of Sciences (ANAS), Azerbaijan, in 2007. From 25.08.2011 to 25.08.2012 he was a post-doctoral researcher at Biometrics Engineering Research Center (BERC) of Yonsei University, Seoul, South Korea. Dr. Yadigar Imamverdiyev is now head of research department at the Institute of Information Technology of ANAS. His research interests include information security management, e-government security, web security, risk management, public and secret key cryptography, biometrics, speaker recognition, social networks analysis.