A Hypergame Model for Information Security

Yadigar Imamverdiyev*

* Azerbaijan National Academy of Sciences, Institute of Information Technology, AZ1141, 9 B.Vahabzade, Baku, Azerbaijan

e-mail: yadigar@lan.ab.az

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.) that are very difficult to compute in real world applications. 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. The proposed two level hypergame models defender's and attacker's perception of the information security situation can be considered as a series of games.

Keywords- Information security; decision-making; game theory; hypergame.

1. 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. 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 can be considered as a series of games.

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

2. Game Theory in Information Security: Limitations

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 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 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].

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 about the attacker. Some of the current models involving dynamic game with incomplete and imperfect information are specific to mobile ad hoc networks [8] 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 the payoff functions of other players, then talking 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 with 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 very difficult to compute with acceptable accuracy in practice. 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 [9] discuss the relationships between two models of games with incomplete information, hypergames [3] and Bayesian games [10]. 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.

Many hypergame analyses have been published, showing its use in modeling conflicts and their resolutions. Hypergame analysis methods but can be applied to military conflicts, international disputes [12], economic treaties and agreements [13], social issues [14] and etc. Hypergame approach also was applied to information warfare [15] and cybersecurity [16].

3. A Brief Introduction to Hypergames

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

An *n*-person non-cooperative game is defined by $G = (S_1, S_2,...,S_n; v_1, v_2, ..., v_n)$, with player set $N = (1, 2, 3,..., n)$. S_i is player i's strategy set and v_i is player i's preference function for each $i \in N$. For the given set of players and the individual strategy sets, an outcome is defined by $s = (s_1, s_2, s_3,..., s_n)$, with $s_i \in S_i$ being the strategy chosen by player i. The set of all outcomes are then defined by $S = S_1 \times S_2 \times S_3 \times ... \times S_n$.

If all the outcomes are ranked in order according to a player's payoffs by writing the most preferred outcome on the left and least preferred on the right, then a preference vector (PV) is formed for the player and denoted by V_i. Consequently, a game can be represented by a set of PVs: $G = \{V_1, V_2, \ldots, V_n\}$.

In a zero-level hypergame, there are no misperceptions, each player is represented by only one PV, and all the players are playing the same game: $H^0 = G = \{V_1, V_2,...,V_n\}$.

In a first-level hypergame, at least one of the players has misperception about PVs of other players. Suppose V_i is the true PV for player i, and V_{ij} is player j's interpretation of player i's PV. Misperception occurs if $V_{ij} \neq V_i$, that is, player j incorrectly interprets i's PV. As a result of misperception the game played by player j will be different from the one played by player i. The first-level hypergame model is formulated as

$$H^1 = \{H_1^0, H_2^0,...,H_i^0,...,H_n^0\} \quad (\exists i, j \in N : H_i^0 \neq H_j^0)$$

$$= \left\{ \begin{bmatrix} V_1 \\ V_{21} \\ \vdots \\ V_{i1} \\ \vdots \\ V_{n1} \end{bmatrix} \begin{bmatrix} V_{12} \\ V_2 \\ \vdots \\ V_{i2} \\ \vdots \\ V_{n2} \end{bmatrix} \cdots \begin{bmatrix} V_{i1} \\ V_{2i} \\ \vdots \\ V_i \\ \vdots \\ V_{ni} \end{bmatrix} \cdots \begin{bmatrix} V_{1n} \\ V_{2n} \\ \vdots \\ V_{in} \\ \vdots \\ V_n \end{bmatrix} \right\}$$

$\exists i, j \in N : V_{ij} \neq V_i$.

The definition of a 1-level hypergame can be extended to high-level hypergames, where some of the players have access to some additional information that allow them to form perceptions about other players' beliefs, other players' perceptions about themselves, and so on.

In a second-level hypergame, at least one of the players is aware that they are playing different games and would therefore perceive what the other players' game is. This can be interpreted as the players playing different first-level hypergames, resulting in a second-level hypergame:

$$H^2 = \{H_1^1, H_2^1,..., H_i^1,..., H_n^1\}$$

$$\forall i \in N, \quad \exists i, j \in N : H_i^1 \neq H_j^1;$$

$$= \left\{ \begin{bmatrix} H_1^0 \\ H_{21}^0 \\ \cdots \\ H_{n1}^0 \end{bmatrix} \begin{bmatrix} H_{12}^0 \\ H_2^0 \\ \cdots \\ H_{n2}^0 \end{bmatrix} \cdots \begin{bmatrix} H_{1n}^0 \\ H_{2n}^0 \\ \cdots \\ H_n^0 \end{bmatrix} \right\},$$

where $H_{ji}^0 = [V_{1ji}, V_{2ji},..., V_{kji},..., V_{nji}]$, $\forall k \in N_{ji}, \forall j \in N_i, \forall i \in N.$

V_{kji} describes what player i believes with regard to how player j interprets k's intentions, $i \neq j \neq k,$ and $i, j, k \in N.$

An Lth-level hypergame consists of n individual games, where at least one of the individual games is different from the others, and the highest order of expectation involved in the

individual games is L. A formal definition of an Lth-level hypergame model is given below [17]:

$$H^L = \{H_1^{L-1}, H_2^{L-1}, ..., H_n^{L-1}\},$$
$$L = 1,2,3,..., \exists i, j \in N : H_i^{L-1} \neq H_j^{L-1}.$$

4. A Hypergame Model for Information Security

In this section we are going to introduce a hypergame model to represent attacker-defender strategic interaction that apply to most information security problems in general. Let us consider two levels of hypergame formally.

As noted above, a game G can be briefly defined as a 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 perceived by 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 perceived by the Attacker;
- V_{DA} – preference vector of the Defender perceived by the Attacker;
- V_{AD}– preference vector of the Attacker perceived by the Defender;
- V_{DD} – preference vector of the Defender perceived by the Defender.

The game, played by the Attacker in the first-level hypergame H^1, 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 $H^1 = \{G_A, G_D\}$.

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^1, 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_D^1 denotes the first-level hypergame of the Defender. Here $H_A^1 = \{G_{AA}, G_{DA}\}$, and $H_D^1 = \{G_{AD}, G_{DD}\}$.

The second-level hypergame $H^2 = \{H_A^1, H_D^1\}$ 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.

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

Analyzing a hypergame involves analyzing 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_A for the attacker $E_A = E_{AA} \bigcap E_{DA}$ (with respect to games G_{AA} and G_{DA}).

3. Analyze the first-level H_D^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_D for the defender $E_D = E_{AD} \bigcap E_{DD}$ (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}: $E = E_{AA} \bigcap E_{DD}$ (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 q is an outcome. If player A at a fixed 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 $UI_A(q)$ is the set of outcomes that represent a unilateral improvement of the outcome q for player A.

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 element in $UI_A(q)$ 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 [17] that solutions to hypergames may not necessarily be created by outcomes that are stable for all players

and it is possible that an outcome that is unstable individually for players may actually be an equilibrium for the hypergame.

5. A Numerical Example

For a numerical illustration of the above described approach, we use a sample attacker defender game from [18] where defender tries to protect assets and attacker targets them. 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.

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 [19]. 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 calculations 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 $E_A = E_{AA} \bigcap E_{DA}$={{#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}}.

6. 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.

Acknowledgements

Author would like to thank anonymous reviewers for their useful comments which have greatly improved the manuscript.

References

[1]. D. Fudenberg, and J. Tirole. *Game theory*. MIT Press/Massachussetts, 1995.

[2]. K. Sallhammar, S. J. Knapskog, and 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, pp. 102-105, Jan. 31 2005-Feb. 4 2005.

[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, pp.1-10, 5-8 Jan. 2010.

[5]. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, "Game theory meets network security and privacy", *ACM Computing Surveys*, Vol. 45, No. 3, Article 25, June 2013.

[6]. A. Singh, A. Lakhotia, and A. Walenstein, "Malware antimalware games," *Proc. 5th International Conference on Information-Warfare & Security (ICIW)*, Ohio, USA, pp. 319-327, 8-9 April 2010.

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

[9]. 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, August 2012.

[10]. Harsanyi J.C., "Games with incomplete information played by Bayesian players", *Management Science*, Vol. 14, No. 3, pp. 159-182, November 1967.

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

[12]. N. M. Fraser and K. W. Hipel, "Metagame analysis of the Poplar River conflict", *Journal of the Operational Research Society*, Vol. 31, No. 5, pp. 377-385, 1980. DOI: 10.1057/jors.1980.70

[13]. M. Giesen, and P. Bennett, "Aristotle's fallacy: A hypergame in the oil shipping business", *Omega*, Vol. 7, No. 4, pp. 309-320, 1979.

[14]. 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, July 1980.

[15]. Kopp C., "Shannon, hypergames and information warfare", *Journal of Information Warfare*, Vol. 2, No. 2, pp. 108-118, 2002.

[16]. J. T. House and G. Cybenko, "Hypergame theory applied to cyber attack and defense", *Proceedings of the SPIE*, Vol. 7666, Article id. 766604, 11 pp., May 03, 2010. doi:10.1117/12.852338.

[17]. M. Wang, K. W. Hipel, and N. M. Fraser, "Modeling misperceptions in games", *Behavioral Science*, Vol. 33, No. 3, pp. 207–223, July 1988.

[18]. T. Alpcan, T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," *42nd Conference on Decision and Control*. Maui, HI, 2003, vol.3, pp. 2595-2600, 9-12 December 2003.

[19]. L. Brumley, "HYPANT: A Hypergame Analysis Tool". http://www.csse.monash.edu.au/hons/se-projects/2003/Brumley/ Latest Access Time for the website is 11 November 2013.