Modelling Information Warfare as a Game

Jorma Jormakka[1] and Jarmo V. E. Mölsä[2]

[1]*Department of Technology*
National Defence College
P.O. Box 7, FI-00861 Helsinki, Finland
E-mail: jorma.jormakka@mil.fi

[2]*Communications Laboratory*
Helsinki University of Technology
P.O. Box 3000, FI-02015 HUT, Finland
E-mail: jarmo.molsa@tkk.fi

Abstract
Game theory is one of the possible ways to study information warfare with mathematical models. This paper presents four example games which illustrate the different requirements for an effective playing strategy in information warfare. These games study, how a bold playing strategy can lead to domination, how a mixed playing strategy can reduce domination, how it can be useful to play a dominating strategy only part of the time, and how excessive domination can lead to rebels where all playing parties lose. This paper also describes meta-strategies whose goal is to modify the perceived costs and conditions of a game. This kind of perception management is closely related to the Observe-Orient-Decide-Act (OODA) loop.

Keywords: *Information warfare, game theory, OODA-loop.*

Introduction

This paper presents four example games for modelling information warfare. With the help of game theory, the possibility for achieving and maintaining a dominating position in different kinds of information warfare cases is investigated. In general, the purpose of mathematical modelling of information warfare is to produce a quantitative evaluation of an attack or a defence strategy. This paper concentrates on finding quantitative answers in describing the most effective strategies for certain information warfare scenarios. In information warfare the fundamental weapon and target is information, while the main goal is information superiority (Hutchinson and Warren, 2001). An important issue here is the possibility to modify the enemy's perception of costs and conditions related to warfare. These perception management issues are closely related to the Observe-Orient-Decide-Act (OODA) loop which describes the decision process and its dependence on timely and correct observations (Boyd, 1996). The OODA-loop emphasizes the orientation phase which is responsible for analysing and interpreting the different observations to find out the most useful decision.

The structure of this paper is the following. First an overview of game theory is given. Then some general observations about modelling information warfare as a game are described. The first game in this paper shows the benefit of bold strategies in asymmetric warfare. The second game indicates the benefits of using mixed defence strategies for mitigating the dominance of a stronger party. The third game analyses the optimal disturbance strategy, when a dominator wants to prevent the usage of a communication network. The fourth game

ISSN 1445-3312 print/ISSN 1445-3347 online

points out that excessive dominance can result in rebels which cause massive costs to all playing parties. All these four games are dependent on correct perceptions of costs and other conditions of the game. The next section describes how meta-strategies can be used to modify the costs and conditions perceived by an enemy. Finally, some related work is described and the conclusions are given.

An Overview of Game Theory

This section describes the most important issues in game theory to make it easier to understand the games defined later in this paper. For an extensive introduction to game theory see, for example, Gibbons (1992). Game theory treats multi-person decision problems as games where each player chooses such decisions which result in the best possible payoff for himself/herself, regarding the most probable decisions of the other players. All players are thus expected to be rational, i.e. they want to maximize payoffs. It is not possible to predict the outcome of a play if some players are irrational. Actually, it should be common knowledge that all the players are rational: all the players know that all the players are rational, and that all the players know that all the players know that all the players are rational, and so on.

The (normal-form) representation of an n-player game G specifies the players of the game, the strategies for each player, and the payoff function for each player:

$$G = \{S_1,\ldots,S_n;u_1,\ldots,u_n\}.$$

Here, S_i denotes the set of strategies available to the player i, $1 \le i \le n$. A strategy $s_i \in S_i$ is one complete plan of action for a game. The payoff for the player i is defined by the function $u_i(s_1,\ldots,s_n)$, where s_j, $1 \le j \le n$, is the strategy chosen by the player j.

Games are generally divided into static and dynamic games. A static game is a simultaneous-move game, and all players choose their strategies simultaneously without knowing what strategies other players have chosen. A dynamic game is a sequential-move game, and players choose their strategies in sequence. Static games can be combined in a dynamic fashion, and a repeated game is one example of this.

Games can have different properties. In a cooperative game players try to maximize the joint payoff, but in a non-cooperative game all players concentrate only on maximizing their own payoff. In warfare, however, there is no cooperation. In a game of complete information the payoff function of all players is common knowledge, but in a game of incomplete information at least one player is not sure about the payoff function of another player. In a game of perfect information a player with the move knows the full history of the game played so far (i.e. what strategies other players have chosen), but in a game of imperfect information at least one player with the move does not know the full history of the game.

The strategies in S_i are the *pure* strategies for the player i. If player i has M different pure strategies ($S_i = \{s_{i1},\ldots,s_{iM}\}$) then a mixed strategy for player i is a probability distribution $p_i = (p_{i1},\ldots,p_{iM})$, where $0 \le p_{im} \le 1$ for $m = 1,\ldots,M$ and $p_{i1} + \cdots + p_{iM} = 1$. A mixed strategy indicates one player's uncertainty about what another player will do. A pure strategy s_{im} can be represented as a mixed strategy by setting p_{im} to 1 (and the remaining terms in the probability distribution being 0).

The expected payoff v_i for player i in an n-player static game $G = \{S_1,\ldots,S_n;u_1,\ldots,u_n\}$, when player j $(1 \le j \le n)$ plays the mixed strategy p_j, is the following:

$$v_i(p_1,\ldots,p_n) = \sum_{m_1=1}^{M_1}\cdots\sum_{m_n=1}^{M_n}\left[\prod_{k=1}^{n} p_{km_k}\right] u_i(s_{1m_1},\ldots,s_{nm_n}), \quad (1)$$

where M_j is the number of pure strategies available to the player j. For a two-player case (1) is

$$v_1(p_1,p_2) = \sum_{m_1=1}^{M_1}\sum_{m_2=1}^{M_2} p_{1m_1}\, p_{2m_2}\, u_1(s_{1m_1}, s_{2m_2}). \quad (2)$$

When modelling decision problems with game theory it is often possible to identify one or more equilibrium conditions which define a strategically stable prediction of the outcome of a play. In an equilibrium condition no player has interest to change his decision, because this would only result in a lower benefit for the player changing his/her decision. In an n-player static game $G = \{S_1,\ldots,S_n;u_1,\ldots,u_n\}$ of complete information the mixed strategies $(p_1^*,\ldots,p_n^*)$ are a Nash equilibrium if, for each player i, p_i^* is player i's best response to the mixed strategies specified for the other players. In other words, p_i^* solves

$$\max_{p_i} v_i(p_1^*,\ldots,p_{i-1}^*,p_i,p_{i+1}^*,\ldots,p_n^*)$$

for any player i, $1 \le i \le n$. A Nash equilibrium provides a local maximum value for v_i, $1 \le i \le n$. Single-player strategy changes are thus not useful at a Nash equilibrium, because any two Nash equilibriums (provided they exist) must differ in the strategies of at least two players. So, to change the outcome of a game from one Nash equilibrium to another, at least two players must change their strategies at the same time. It has been shown that there exists at least one Nash equilibrium, possibly involving mixed strategies, for any normal-form static game with a finite number of players and strategies. If a game has exactly one Nash equilibrium, it is the unique solution to the game. Game theory cannot necessarily predict the outcome of a game, if there are more than one Nash equilibriums for the game. Especially, when a game has multiple Nash equilibriums with conflicting payoffs, this game can have an outcome which is not a Nash equilibrium.

Credibility is a central issue in dynamic, sequential-move games. Only credible threats or promises can have an effect on how a game proceeds. In the context of warfare we will concentrate on threats instead of promises. In a two-player game, one player can threat to change his/her strategy, if the other player does not act as required by the stronger player. If the threat is not accepted, the play will end up in another Nash equilibrium which provides a worse outcome for the player not accepting the threat. Credible threats about future behaviour can thus have an influence on current behaviour.

The concept of a Nash equilibrium describes the possible outcomes of a static game of complete information, but there are stronger equilibrium concepts for more complicated (richer) types of games. For example, a dynamic game of complete information may have many Nash equilibriums, but only sub-game perfect Nash equilibriums do not involve non-credible threats or promises.

An example of a dynamic game is a repeated game $G(T)$, where a static game G of complete information (the stage game) is repeated T times. The outcome of a single stage of this

dynamic game can, however, differ from the Nash equilibriums of the basic static stage game. If the stage game G has multiple Nash equilibriums, a sub-game perfect outcome of $G(t)$ at a single stage t, $t < T$, is not necessarily a Nash equilibrium of G, when credible threats about the future behaviour are involved.

Information Warfare as a Game

A natural setting for modelling information warfare is to have a game with two players: an attacker and a defender. All players are expected to be rational here. The payoff for an attacker is the damage to a victim. As a starting point for the forthcoming games, we will first give some possible scenarios for information warfare:

1. An army with high technology attacks an opponent's Command, Control, Communication, and Intelligence (C^3I) system and tries to disable it at the beginning of a strategic strike. In addition to hacker warfare methods, this kind of an attack can include many other methods, like physical destruction, disabling of sensors, electronic warfare, and so on. The goal of all of these attack methods is to cause loss of information and delays in the OODA-loop which causes wrong decisions to be taken (Kopp, 2002).
2. A group of attackers carries out a massive attack against a critical information technology infrastructure of a society with easily available tools, such as Denial of Service (DoS) tools, viruses, worms, Trojans, and password crackers. The goal is to produce chaos, economic losses, and psychological effects.
3. A group of terrorists carries out a targeted, well-planned, and coordinated attack using precision weapons, such as new viruses, worms, and DoS tools. The attack aims in bringing down important organizations and sabotaging business operations. This kind of attack needs information of the target before the attack can be made, and the time of the attack is likely to be carefully chosen. The goal of a targeted attack is to cause economic losses, to influence willingness to fight, or to support other actions, like terrorist operations.
4. A group of attackers carries out long-term information warfare to cause economic losses and slow down technical development.

All these scenarios involve more than one manifestations of information warfare: command-and-control (C^2), intelligence-based, electronic, psychological, hacker, economic, and cyber warfare (Libicki, 1995). Each game here concentrates on a single manifestation of information warfare.

Attack and defence strategies must not be too unspecific. Only one strategy should be possible to play at a time, and there should be a limited amount of clearly different strategies. Otherwise the outcome of a game would be unknown, if several strategies can be played at the same time. The players of the games in this paper can only choose one strategy at a time.

Terrorist Game: Bold Strategy Can Result in Domination

The first game in this paper is the terrorist game. Terrorism can be combined with many information warfare methods.

The main contribution of this game is to show that in a game with more than one conflicting Nash equilibriums can only end up in domination. In asymmetric warfare at least one of the players is expected to be in a weaker position than the other players.

The terrorist game is a two-player static game of complete information, where both players are rational. Terrorists (T) capture hostages and threaten to blow up the hostages if the requirements of the terrorists are not accepted. The government (G) proposes that terrorists should surrender and be put to jail. Both players have two strategies p_1 and p_2. The strategy p_1 means accepting what the other player suggests: terrorists surrender or the government accepts the requirements (e.g. pays the ransom). The strategy p_2 means rejecting what the other player suggests (terrorists kill the hostages or the government rejects to negotiate). The payoffs are the following:

- If both players play p_1, both players get -1: G accepts requirements, T surrenders and is put to jail but gets benefit from the accepted requirements.
- If both players play p_2, both players get -10: G rejects, T kills hostages and terrorists themselves.
- If player T plays p_1 and player G plays p_2, T gets -5 and G gets 0: G rejects, T surrenders and is put to jail.
- If player Tplays p_2 and player Gplays p_1, T gets 1 and G gets -5: T gets free with accepted requirements, hostages released.

Let us assume T plays the mixed strategy $(p_T p_1, (1-p_T)p_2)$, where $0 \le p_T \le 1$. This means that T plays p_1 with the probability of p_T, and p_2 with the probability of $(1-p_T)$. G plays the mixed strategy $(p_G p_1, (1-p_G)p_2)$, where $0 \le p_G \le 1$. The expected payoff v_T for T is according to (2)

$$\begin{aligned} v_T &= -p_T p_G - 10(1-p_T)(1-p_G) - 5p_T(1-p_G) + (1-p_T)p_G \\ &= p_T(5-7p_G) - 10 + 11p_G, \end{aligned}$$

and the expected payoff v_G for G is

$$\begin{aligned} v_G &= -p_T p_G - 10(1-p_T)(1-p_G) + 0p_T(1-p_G) - 5(1-p_T)p_G \\ &= p_G(5-6p_T) - 10 + 10p_T. \end{aligned}$$

The Nash equilibrium points (p_T, p_G) for this game are calculated by analysing the best-response correspondences $p_T^*(p_G)$ (the value of p_T which maximizes $v_T(p_G)$) and $p_G^*(p_T)$ (the value of p_G which maximizes $v_G(p_T)$). These correspondences describe, how the own optimal mixed strategy selection probability depends on the opponents probability. First we identify the pure strategy Nash equilibriums ($p_j = 0 \vee p_j = 1,\ j \in \{T, G\}$):

$p_T^*(0) = 1$ and $p_G^*(1) = 0$: Nash equilibrium point is (1,0)

$p_T^*(1) = 0$ and $p_G^*(0) = 1$: Nash equilibrium point is (0,1)

The possible Nash equilibriums involving mixed strategies can be found by differentiating the payoff functions:

$$\frac{\partial v_T}{\partial p_T} = 5 - 7p_G = 0 \Rightarrow p_G = \frac{5}{7},$$

$$\frac{\partial v_G}{\partial p_G} = 5 - 6p_T = 0 \Rightarrow p_T = \frac{5}{6}.$$

The Nash equilibriums are thus the following points: $(p_T, p_G) \in \left\{(1,0),(0,1),(\frac{5}{6},\frac{5}{7})\right\}$. These points reflect the intersection points of the best-response correspondences shown in the Fig. 1. The payoffs (v_T, v_G) at the equilibrium points are: $(-5,0),(1,-5),(-\frac{15}{7},-\frac{10}{6})$.

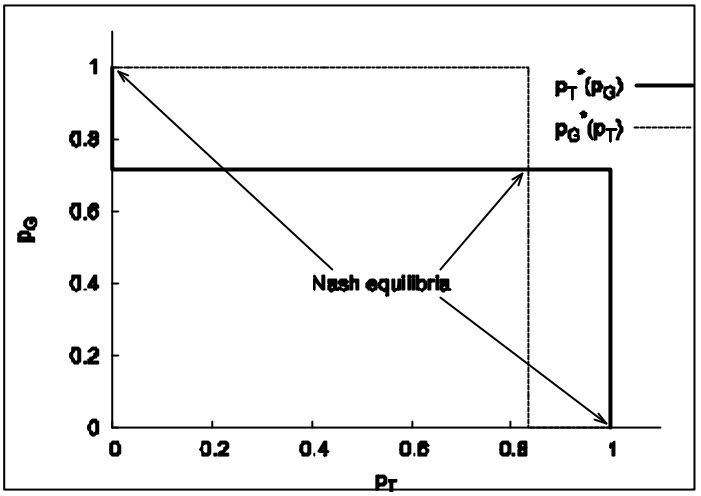

Figure 1: The intersections of the best-response correspondences are the Nash equilibriums.

The two Nash equilibrium points with pure strategies (p_1, p_2) and (p_2, p_1) give the best payoffs for v_G and v_T, respectively. Thus, the third equilibrium point is not in interest for neither player. As such, however, these results do not yet provide any unique solution to this static game. A bold strategy (as defined in gambling theory in Dubins, 1965) can, however, result in a unique solution in the long term when the static terrorist game is repeated.

Let us assume, that G is bold and always plays p_2. G states that it will not negotiate with T. Player T may not believe that G will play boldly, and T may try p_2 for finitely many times, but if G sticks on to playing p_2, T will eventually finish with a finite negative gain and T will have to start playing p_1 in order to minimize the losses. This familiar real-life game can only end up in domination, where T accepts that G always plays p_2 and will accept losing on this game, or in blowing up the hostages and terrorists. Then rational player T must always play p_1. A bold rational player always wins over the less bold rational player in the long term when the terrorist game is repeated. This can be formulated as the following Proposition 1.

Proposition 1. Let $G = \{S_1,\ldots,S_n;u_1,\ldots,u_n\}$ be a non-cooperative n-player static game which is repeated. S_i is the set of strategies and u_i is the payoff function of the player i. Let the set $E \neq \varnothing$ of Nash equilibriums satisfy the following two criteria:

1. There are players i and j and two equilibrium points $x, y \in \mathrm{E}$ such that $u_i(x) \geq u_i(z)$ and $u_j(y) \geq u_j(z)$ for any $z \in \mathrm{E}$. Thus, there is no unique solution to this static game because it is not possible for players i and j to achieve the best possible payoff at the same time. This is a typical case, for example, in asymmetric warfare.
2. Let the strategy of the player i in x be x_i and the strategy of the player j in y be y_j. Let z be the outcome of the static game. If $z \in \mathrm{E}$ and the strategy of the player i is x_i,

then $z = x$, and if the strategy of the player j is y_j, $z = y$. In other words, if the game ends up in a Nash equilibrium, then only either of the players i and j will get the maximum payoff.

The repeated game can only end up to the player i dominating the player j, or the player j dominating the player i, or both i and j being dominated by some player k, or to a point outside E. A point outside E will result, for example, if players i and j both insist on playing their best-response strategy.

Proof. This proposition does not say anything that is not already known from Nash equilibrium points, but it is given because of the conclusions we can draw from it. If the solution is not one of the equilibrium points, some player has a reason to change his strategy. Thus the players try to get to a solution, which is in the set E. As the player i is rational and the game is non-cooperative, he will try to get the best gain and force others to play $x = (x_1,...,x_n)$. He can only play x_i, but the only equilibrium point where his strategy is x_i, is x. Thus, the other rational players can only play the strategy they play in x. If the player i succeeds, he will dominate over j. If some other player succeeds, he will dominate over i. The last possibility is that the result is not an equilibrium point, which happens, for example, if neither player i nor player j accept domination. In this case player i will choose x_i and player j will choose y_j, but due to conflicting Nash equilibriums this combination will result in an outcome which is not in the set E. □

Domination strategy seems acceptable in the repeated terrorist game, but in general the acceptability of the solution depends on what side one is. The cause for asymmetric warfare is often domination in the first place. Domination strategies are not necessarily stable. When the cost of accepting domination is on the same range as the estimated cost of fighting against it, we should expect a crisis to appear.

Evildoer Game: Mixed Defence Strategies Can Reduce Domination

The second game in this paper is the evildoer game. In this game an evil hacker tries to attack and compromise a victim network or host. This can be seen as a relevant (sub)goal for many forms of information warfare, especially for C^2, hacker, and cyber warfare.

The main contribution of this game is to show that using mixed defence strategies can result in better tolerance against dominative attack strategies, when no generic defence strategy is available.

The evildoer game is a static game with complete information, where both players are rational. There are two players, an attacker A and a victim B. The goal of the attacker is to cause damage to the victim by crashing hosts, installing malicious software, getting remote access with root-privileges, causing Denial-of-Service, and so on. To achieve the goal, the attack must find a primary attack which cannot be directly detected (e.g., no fingerprint available for a new exploit). The attacker has two strategies p_{A1} and p_{A2}, where p_{A1} means overloading the victim with many secondary attacks at the same time with the primary attack to cause delays in the OODA-loop of the victim and make the detection of the primary attack more difficult. The strategy p_{A2} means trying only the primary attack. The victim also has two strategies p_{B1} and p_{B2}, where p_{B1} means detecting and alerting on all suspicious network

traffic, but some of this traffic may have to allowed to pass through due to the high probability of false alarms. p_{B2} means detecting and blocking only the most important attacks. As the primary attack will succeed initially, the victim may, however, be able to detect the attack afterwards with a delay by paying attention to the available alerts. The payoffs u_A and u_B for the attacker and the victim, respectively, are the following:

- $u_A(p_{A1}, p_{B1}) = 4$ and $u_B(p_{A1}, p_{B1}) = -5$: the victim does not detect the primary attack at all, because the victim is overloaded by the large amount of alerts from the secondary attacks.
- $u_A(p_{A1}, p_{B2}) = 3$ and $u_B(p_{A1}, p_{B2}) = -2$: the victim does not detect the primary attack, but some of the secondary attacks may cause alerts. These alerts can be used as an indication about a larger attack, and signs about intrusions into important hosts can be searched more carefully. There is a low probability for identifying the successful primary attack.
- $u_A(p_{A2}, p_{B1}) = -10$ and $u_B(p_{A2}, p_{B1}) = 20$: the victim detects all suspicious network traffic. As there is only a low volume of alerts, the victim has time to analyse all data carefully, and the intrusion is detected after a delay.
- $u_A(p_{A2}, p_{B2}) = 30$ and $u_B(p_{A2}, p_{B2}) = -20$: the victim does not detect the primary attack.

Let us assume that the attacker plays the mixed strategy $(pp_{A1}, (1-p)p_{A2})$, where $0 \le p \le 1$, and that the victim plays the mixed strategy $(qp_{B1}, (1-q)p_{B2})$, where $0 \le q \le 1$. The expected payoff v_A for A is according to (2)

$$v_A = p(5q-2) + 5 - 4q,$$

and the expected payoff v_B for B is

$$v_B = q(2-5p) - 3 + p.$$

The best response correspondences $p^*(q)$ and $q^*(p)$ for the attacker and the victim, respectively, have one intersection at $p = 2/5$ and $q = 2/5$, which is the unique mixed strategy Nash equilibrium for this evildoer game. The evildoer game has thus a unique outcome.

This result has the following effect on the selection of attack and defence strategies. If a specific defence strategy is not generic, but instead works well only against a specific attack strategy, then changing the defence strategy more or less randomly results in better tolerance against the dominative attack strategies. The attacker has thus more difficulties in dominating a victim when the victim is using mixed defence strategies.

In this specific evildoer game the attacker should overload the victim in 40 % of the attacks, and use only a single primary attack mechanism in 60 % of the attacks. The victim, on the other hand, should try to detect all possible suspicious network behaviour 40 % of the time, and concentrate only on detecting and blocking the major attacks 60 % of the time. The mixed strategy Nash equilibrium reflects the mutual uncertainty about the other player's strategy.

Vandal game: Domination Can Have a Limited Time Span

The third game in this paper is the vandal game. In this game a vandal tries to disturb the usage of a communication network, for example, by initiating a flooding Denial of Service (DoS) attack overloading the target network or by jamming a wireless network.

The main contribution of this game is to show that domination can have a limited time span. If the victim network is unusable for a too long time, legitimate users will start using another

network for communication purposes. This new network is selected so that the vandal cannot disturb it, at least not with the same attack methods.

The vandal game is an n-player static game of complete knowledge, where all the players are rational. In this game all the players are using the services of a communication network. The player V is the vandal who does not maximize his gain from having good service with low costs, but instead maximizes the harm to other users. The player L_j, $2 \le j \le n$, is a legitimate user of the network. All legitimate users are identical. In total there are thus n players. All the players have two strategies p_1 and p_2, where p_1 means using the network, and p_2 means being idle. If the vandal is using the network, then the network is expected to be overloaded and cannot be used for legitimate purposes. The payoffs for the vandal and the legitimate user are the following:

- If V plays p_2, V will get 0.
- If V plays p_1, V will get m, if there are m legitimate users playing p_1.
- If L_j, $2 \le j \le n$, plays p_2, L_j will get 0.
- If V plays p_2 and L_j, $2 \le j \le n$, plays p_1, L_j will get 1.
- If V plays p_1 and L_j, $2 \le j \le n$, plays p_1, L_j will get -1.

Let us assume that the player V plays the mixed strategy $(p_1 p_1, (1-p_1)p_2)$, and that the player L_j, $2 \le j \le n$, plays a mixed strategy $(p_L p_1, (1-p_L)p_2)$, where $0 \le p_L \le 1$. The expected payoff v_V for the vandal is

$$v_V = (n-1)\, p_1 p_L,$$

and the expected payoff v_{L_j} for the legitimate user L_j is

$$v_{L_j} = -p_1 p_L + (1-p_1)p_L = p_L(1-2p_1).$$

We can concentrate on analysing the best-response correspondences between the vandal and only one legitimate user, because all legitimate users are here expected to behave in a similar fashion. This results in a two-dimensional presentation for the best-response correspondences $p_1^*(p_L)$ and $p_L^*(p_1)$, and they do not have only a single intersection point, but, instead, an infinite set of intersection points, because the correspondences overlap partially. The Nash equilibriums for this vandal game are thus the following: When p_1 is in the range $[\frac{1}{2}..1]$, p_L is 0, and the expected payoff is 0 for all players.

The solution of the game is that the vandal cannot win since the other players stop using the service. Initially, of course, there will be a loss for the legitimate users because network service is not available, but the legitimate users will find another communication mechanism.

When studied as a dynamic game, the vandal should not always play p_1 because legitimate users will stop using the communication network. If the vandal plays p_1 only part of the time (here less than 50% of the time), he can gain. An important question is, how often to play p_1 so that legitimate users will not stop using the communication network.

Rebel game: Extreme Domination Can Result in Rebellions

Let us look at a game like the terrorist game, which has several Nash equilibrium points and which therefore leads to a dominating solution if played repeatedly with a bold strategy. In this rebel game the dominating solution is expected to cause extremely high costs to the weaker party. These high costs will eventually be seen unbearable by the weaker party which will eventually start to rebel.

The main contribution of this game is to show that it is useful for a dominating party to prevent extremely high costs for the weaker party. Otherwise the weaker party may start to rebel which will result in substantial costs to the dominating party.

If a game with high costs to the weaker party is played several times, we do not know the outcome. The purpose of the rebel game is to suggest a way to treat such games and to propose a solution concept. If the game is played up to some finite finishing time and the players optimize their strategies up to the finishing time then the game can be treated as a single step game with all the outcomes up to the finishing time and with all strategies which are sequences of one step strategies. Such a game has at least one Nash equilibrium point. This, however, is not a realistic solution since the players cannot calculate strategies up to the finishing time and cannot assume the opponent is calculating strategies up to the finishing time and playing rationally, unless the finishing time is only few steps ahead. For instance, if there are two players and each has two strategies in one step, then after 25 steps there are two to power fifty outcomes. Using a computer for numerical evaluation of such a game approaches the computing limit, and memory demands are reached even earlier.

Analytic solutions can be used to give probability distributions for the gains or losses of the players in n steps even for a large n, provided that the model is sufficiently simple. Let us briefly describe one such method, the generating function method. Let users A and B have strategies $p_{1A}, p_{2A}, p_{1B}, p_{2B}$, which they play with probabilities $p_{1A}, p_{2A}, p_{1B}, p_{2B}$ respectively. Let s_{n,q_A,q_B,r_A,r_B} denote the probability of A having cost r_A and B having cost r_B after a sequence of moves where A has played p_{2A} q_A times and B has played p_{2B} q_B times in n steps. The order of playing the strategies has an importance to the costs, and s_{n,q_A,q_B,r_A,r_B} is the sum of probabilities over all possible orderings of playing the strategies. There is the recursion equation:

$$s_{n,q_A,q_B,r_A,r_B} = \sum_{i=1}^{2}\sum_{j=1}^{2} p_{iA}\, p_{jB}\, s_{n-1,q_A+1-i,q_B+1-j,r_A+f_A(i,j),r_B+f_B(i,j)} \qquad (3)$$

The functions $f_A(i,j)$ and $f_B(i,j)$ are the losses of A and B on one step. We can solve it individually for A and B. In the case of A, the cost of B is not of interest, thus we must solve an equation of the general type

$$s_{n,q_1,\ldots,q_K,r} = s_{n-1,q_1,\ldots,q_K,r} + \sum_j p_{n-1,q_1,\ldots,q_j+c_i,\ldots q_K,\, f_j(r,q_j,n)}\, s_{n-1,q_1,\ldots,\, q_j+c_j,\ldots,\, f_j(r,q_j,n)}\,. \qquad (4)$$

In the generating function method (Jormakka, 2003) we try to find a function

$$G_n(u,v) = G_n(u_1,\ldots,u_K,r) = \sum_{k=0}^{\infty} s_{n,q_1,\ldots,q_K,r} \prod_j u_j^{\,y_j(k,n,q_1,\ldots q_K,r)}\, v^{x(k,n,q_1,\ldots q_K,r)}$$

with some functions y_j, x_j such that the recursion equation is changed to the form

$$G_n(u,v) = \left(1 + \sum_j g_j(n-1,u,v)\right) G_{n-1}(u,v) + B_{n-1}(u,v) \quad (5)$$

The function $B_{n-1}(u,v)$ describes the contribution of the boundaries. Notice, that $g_j(n-1,u,v)$ is not always a function, can also be a linear operator. The equation for the generating function is solved and $G_n(u,v)$ is expanded into a power series out of which the probabilities are extracted. The form of the solution for s_{n,q_A,q_B,r_A,r_B} is typically a partition with some restrictions. Partitions are also slow to evaluate numerically, but in many cases one can find limits or bounds which can be effectively evaluated. We will not go into the mathematical details of the method here. The theory is explained in (Jormakka, 2003).

When the probabilities are solved we can draw a few conclusions. If a single step game with domination is played *n* times, the probability of player's cost exceeding a given limit can be obtained from the probabilities s_{n,q_A,q_B,r_A,r_B}. Assuming that a player has set a maximum limit to tolerable losses, this gives the probability of a player starting to play irrationally in the single step game for fighting against an intolerable situation. The game has been named the rebel game because there is an easy periodic solution where *A* plays a dominating strategy and causes *B* losses of value *R* on each step. Assuming that *B* has the limit *M* for tolerable costs, he is likely to rebel after *n=M/R* steps. Assuming that this rebellion incidence levels the costs of *B* and *A* to zero and *A* again starts playing the dominating strategy, we have a periodic sequence of rebels.

In the periodic solution *B* plays irrationally on some steps and therefore it is not a good rational solution. We may have the following rational solutions:

1) The immediate costs to *B* are so high, that he can play only one strategy in each step. That is, the immediate cost of one step exceeds *M*. Then it is rational for *B* to accept all the time the domination strategy played by *A*.
2) *A* does not play a domination strategy, but instead he plays a mixed fair strategy. Then *B*'s losses never grow to *M* and his rational behavior on the single step game is also rational in the multi-step game. This requires *A* to be cooperative.
3) *A* and *B* play strategies, which are almost rational on the single step game but still never lead to intolerable losses to either player. Then the players are almost non-cooperative.

The third solution seems intuitively to be a possible solution concept for this kind of a game. The players are almost rational and non-cooperative on each single step. They do not optimize moves over any sequence of steps, which is realistic. Their motivation is to avoid intolerable losses and the strategy should guarantee it. A rather simple mathematical model guaranteeing that the probability of losses higher than *M* are impossible can be made by multiplying the probabilities by $(r_j - M_j)$, where *j=A,B*, and scaling the equation correspondingly by c_n so that probabilities sum to one:

$$s_{n,q_A,q_B,r_A,r_B} = \sum_j c_{n-1}(r_A - M_A)(r_B - M_B)\, p_{iA} p_{jB} s_{n-1,q_A+1-i,q_B+1-j,r_A+f_A(i,j),r_B+f_B(i,j)} \quad (6)$$

There is a natural connection with the rebel game and asymmetric information warfare. In asymmetric warfare one of the parties is often a group of people who feel for some reason having suffered intolerable damage and is ready for acts looking irrational if the whole history

is not considered. Domination strategy is not the solution as the rebel game shows. It seems impossible to impose so high costs on one step that the solution 1) be realistic. The solution 2) makes little sense to A. Probably balancing between the extremes as in 3) is the only practical solution. Applied in information warfare, we should conclude that neither high penalties nor going along with demands of cyber warriors is a working solution. The goal should be to remove the possibility of intolerable losses to either side. Mathematical models typically give only insight, but in this case there may be a chance for rough estimation of the time before irrational playing behavior happens and how much weaker should a strategy be of a dominating strategy in order to bring a stable solution.

Meta-Strategies: Modifying Observations and Orientation of the Enemy

A widely used model for describing the decision processes in warfare is the OODA-loop (Boyd, 1996). The one who is able to get inside the opponent's OODA-loop will control, how fast the opponent is able to react to new situations and also, what decisions the opponent is making. This is information superiority, and the essential goal for information warfare.

Here we will shortly describe how it is possible to model the modification of the opponent's OODA-loop as a game of information warfare. All the complete-knowledge games described so far 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. In the OODA-loop language this is expressed as making a wrong decision.

To combine game theory and the OODA-loop we can end up in a meta-strategy which defines how to affect the strategy selection process (decision process) of the enemy. The primary goal of this kind of a meta-strategy is to make threats look credible, i.e. lure the opponent to make wrong observations about the costs of the attacker. If an opponent believes some threats from an attacker, this opponent will play according to these false observations, and the attacker is allowed to enter at least partially inside the OODA-loop of the opponent. As a result, the quality and speed of the opponent's decisions will be decreased.

In a complete knowledge game with realistic payoff functions the possible results of an information warfare game are mostly known in advance. Only choosing a suitable meta-strategy will make it possible to modify these pre-determined results.

Related work

Hacker warfare, which is one manifestation of information warfare, can be modelled by using attack trees (Cohen, 1998; Schneier, 2000). Attack tree modelling is a method similar to using risk trees in risk assessment. An attack tree classifies different attack types, and defines a risk for each attack type to be the product of the associated probability and the cost of a successful attack. It seems, however, impossible to assign probabilities to various attack types. It is naturally possible to estimate the probabilities of particular attack types using some large set of analysed cases, but such probabilities do not predict the situation in special cases. The success probability of using an exploit is strongly time dependent: a vulnerability is first known only to a few, then public scripts exploiting this vulnerability will be available, and finally the associated security patch will be installed on most vulnerable computers and the exploit will no longer be useful. This time dependency associated with lack of knowledge makes building and updating a detailed attack tree practically impossible. Thus, an attack tree grows big with too many unknown probabilities, like in Cohen (1998).

In the area of network security, game theory has been used to model misbehaviour and selfishness in ad hoc networks (Michiardi, 2003; Urpi, 2003). Penetration into a computer system has been studied with the help of game theory in Sallhammar (2004).

Conclusions

This paper used game theory to model four different information warfare cases. The results from these games indicated that different strategies are effective in achieving and maintaining a dominating position in the long term when a single step game is repeated many times.

In the terrorist game, which has two conflicting results, a bold strategy was required to force an enemy to believe that a player will not accept any threats. In the evildoer game it was shown that mixed strategies can mitigate the dominative position of the attacker, especially when any defence strategy is effective only against a specific attack strategy. Changing the defence strategy somehow randomly will increase the probability of mitigating attacks. In the vandal game, where there is no cost for carrying out a DoS attack, an attacker should overload a network only part of the time, so that the defender will not stop using a network completely. Finally, the rebel game indicated that causing excessive damages to a weaker party can result in rebellions where both parties will suffer large damages. Maintaining a dominating position requires the stronger player to limit the long term costs to the weaker party. If the weaker party feels that it has suffered too much there will be little difference how much it will lose the next time. Here, understanding the history of the play is required to treat actions as rational in the sense of game theory.

In a dynamic game, such as a repeated game, only credible threats can have an effect on current behaviour. This fact can be exploited in meta-strategies, which try to modify the opponent's observations and perceptions of the payoff functions and strategies in the game. This perception management is closely related to the OODA-loop. Meta-strategies are one possibility for getting inside the opponent's OODA-loop, and controlling the observations and orientations, and the resulting decision process as a whole.

References

Boyd, J. R. (1996). *The Essence of Winning and Losing,* Presentation slides, January, 1996

Cohen, F. et al. (1998). *A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses: A Cause and Effect Model and Some Analysis based on That Model,* Sandia National Laboratories.

Dubins, L. and Savage, L. (1965). *How to Gamble if You Must; Inequalities for Stochastic Processes,* McGraw-Hill.

Gibbons, R. (1992). *A Primer in Game Theory,* Pearson Education, Essex, UK.

Hutchinson, W. and Warren, M. (2001). Principles of Information Warfare. *Journal of Information Warfare,* **1**(1): 1-6.

Jormakka, J. (2003). *Combinatorial Decision Theory with Applications in Hacker Warfare Modelling*, Technical Report (preprint), Department of Technology, National Defence College, Helsinki, Finland. Publication Series, **1**(12).

Kopp, C. (2002). Shannon, Hypergames and Information Warfare. *Journal of Information Warfare,* **2**(2): 108-118.

Libicki M. (1995). *What is Information Warfare?* National Defense University.

Michiardi, P. and Molva, R. (2003). A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad hoc Networks. In: *Proceedings of the WiOpt'03 workshop,* March, 2003, Sophia-Antipolis, France.

Sallhammar, K. and Knapskog S. J. (2004). Using Game Theory in Stochastic Models for Quantifying Security. In *Proceedings of the Ninth Nordic Workshop on Secure IT Systems,* November, 2004, Espoo, Finland.

Schneier, B. (2000). *Secrets & Lies*, Wiley, New York.

Urpi, A. and Bonuccelli, M. and Giordano, S. (2003). Modelling cooperation in mobile ad hoc networks: a formal description of selfishness. In: *Proceedings of the WiOpt'03 workshop,* March, 2003, Sophia-Antipolis, France.