"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

A QUANTITATIVE STOCHASTIC MODEL FOR AVIATION SECURITY

Catalin CIOACA*, Marian OANA*, Florin Cătălin OLTEANU**

*Faculty of Aeronautical Management, "Henri Coanda" Air Force Academy, Brasov, Romania
**Economic Engineering and Manufacturing Systems Department, Transilvania University of Brasov, Romania

Abstract: *This paper provides a quantitative analysis of the risks of terrorism in aviation security system using mathematical device. The aim of analysis is to support effective the underlying decision process in conflict situations that may occur due to terrorist threats in aviation system. To obtain a model more suitable and real of the phenomenon, it were adopted the instruments offered by the mathematical theory of discrete Markov processes and game theory, the results constitute a systematic risk assessment effectively against such attacks. To demonstrate de approach, a simple example of a terrorist attack against a passengers aircraft is modelled and analyzed.*

Keywords: *aviation security, game theory, Markov chain, conflict situations*

1. INTRODUCTION

The security of aviation system has traditionally been expressed in a qualitative manner. Qualitative risk analysis involves considering each risk in a purely descriptive way, to imagine various characteristics of the risk and the effects that these could have on the aviation system.

In the aftermath of the 9/11/2001, it has been considered that the threats against the aviation system are real and multiple, and in this context the civil aircraft could be the target of terrorist attacks conducted with air defence systems.

In contrast to failure, attack may not always be well characterized by models of a random nature. Thus, the probabilistic methods for quantifying the operational security of aviation systems provide a more accurate model of the terrorists' expected behaviour, which can be used to assign more realistic transitions probabilities in the stochastic models.

In this paper, a game theoretic method is used for analyzing the aviation security, where the interactions between a terrorist and the aircraft are modelled as a two-player stochastic game.

Also, for the mathematical description of the attack, viewed as a phenomenon that takes place in stages and determines the system passing through several states, Markov chain theory is used.

2. THE STOCHASTIC MODEL

2.1 Related work

System failure is a concept that denotes the system's inability to deliver its services, in the security community it calls *security breach.* A security breach might be caused by normal usage operation, but more likely by *intentional attack* upon the system.

Considered physical system can only be found in a multitude of states S and can change state at discrete moments $t_1, t_2, \ldots, t_n$.

$$S=\{S_1, S_2, \ldots, S_m\} \qquad (1)$$

If the probability of moving to a state when a state θ ($t_k<\theta<t_{k+1}$) to a state S_i depends on S_j in which the system is at a time t ($t_{k-1}< t<t_k$), then the system evolution is described by a discrete – time Markov chain [1].

Exemplifying every intermediate point of attack, depending on the success (A_{i+1}) or failure (A_{i-1}), the attacker has the opportunity either to cancel the attack (safety system), or continue it (A_i).

On the other hand, the system has the ability to detect the attack and change to safety system, which would lead to the attackers impossibility to continue the attack (figure 1).

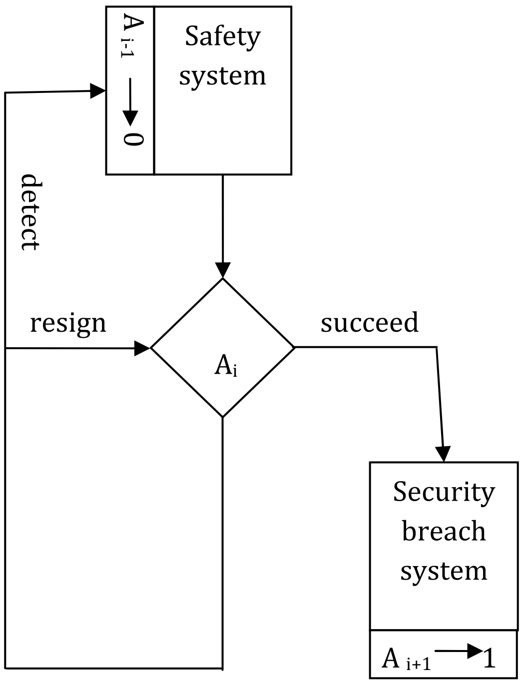

Fig.1 Terrorist attack against aviation system described as state changes

For each of the states of the associated crowd A crossing probabilities $P_{ij}(t, \theta)$ can be arranged in the shape of a square matrix:

$$P_{ij} = \| P_{ij}(t, \theta) \| \qquad (2)$$

where each element satisfies the relations:

$$\begin{cases} \sum_{A_j \in A} P_{ij}(t,\theta) = 1, A_i \in A, \ \forall \ (t,\theta), t \prec \theta \\ 0 \le P_{ij}(t,\theta) \le 1, \ \ A_i, A_j \in A, \ \ \forall \ (t,\theta) \end{cases} \qquad (3)$$

Also, the likehood of passage in any state of the system can be calculated if the initial distribution is known and also the transition probabilities at different times [2].

$$P_{rs} = P_{rk} \times P_{ks} = \left\| \sum_{A_j \in A} P_{ij}(r,k) \times P_{jl}(k,s) \right\| \ \forall \ A_i, A_j \in A \qquad (4)$$

If the evolution of the system was developed by the moments 1, 2,..., n, then the relation (4) becomes:

$$P_n = P_0 \times P_{0,1} \times P_{1,2} \times \ldots \times P_{n-1,n} \qquad (5)$$

where P_0 is the initial distribution [3].

2.2 Quantification of an attack

This is a simple example to illustrate the possible use of the theory previously presented.

Suppose that a passenger plane enters the path to large landing area with a low risk of terrorist attack. The aircraft has both active countermeasures system (DIRCM), as well as passive (chaff & flares) against attacks with portable surface to air missiles (MANPADS).

A terrorist cell is ready to attack aircraft with such a system, once the aircraft will enter the complex possibilities of antiaircraft action. The number of missiles available is 3.

The attacker considers that in order to predict the outcome of his attack (figure 2), the aircraft can be found after the attack in one of the possible states [4,5].

- S_1 – the aircraft lands safely (the rocket did not reach target due to limited knowledge of terrorist missile operating system);
- S_2 –the aircraft is damaged but can land in emergency terms;
- S_3 – the aircraft was destroyed.

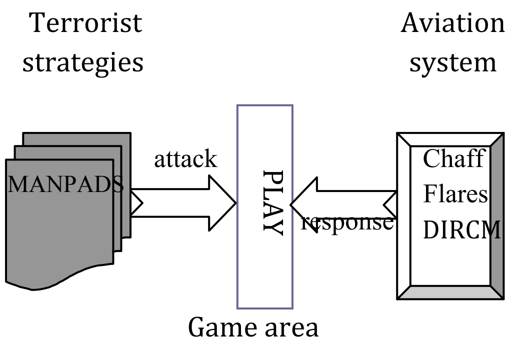

Fig. 2 The interactions between a terrorist and the aircraft modeled as a two-player game

We consider the initial state of the aircraft (before the first missile launch) with the distribution:

$$P_0 = (1,0,0) \qquad (6)$$

The probabilities of transition from one state to another are expressed by the values

$$P_{0,1} = \begin{array}{c} \\ \\ \\ \end{array}\begin{array}{ccc} S_1 & S_2 & S_3 \\ \hline 0,2 & 0,5 & 0,3 \\ 0 & 0,6 & 0,4 \\ 0 & 0 & 1 \end{array}\begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \end{array} \qquad (7)$$

Stochastic matrix P can be interpreted as representing the aircraft's chances of moving from one state to another, and these transitions are irreversible.

The evolution of the system changes with the times depending on which rockets are launched. So, it must calculate the vector P_3 which will consist of probabilities that the system (aircraft) is in the three states after missile launch:

$$P_1 = (1 \;\; 0 \;\; 0) \bullet \begin{pmatrix} 0,2 & 0,5 & 0,3 \\ 0 & 0,6 & 0,4 \\ 0 & 0 & 1 \end{pmatrix} = (0,2 \;\; 0,5 \;\; 0,3) \qquad (8)$$

P_1 shows that after the first missile launch system has a good chance to be in state S_2.

For P_2 we obtain:

$$P_2 = (0,2 \;\; 0,5 \;\; 0,3) \bullet \begin{pmatrix} 0,2 & 0,5 & 0,3 \\ 0 & 0,6 & 0,4 \\ 0 & 0 & 1 \end{pmatrix} = (0,04 \;\; 0,4 \;\; 0,56) \qquad (9)$$

In this case, the system will most likely find in the state S_3, therefore, the terrorist attack can be successful using only two missiles in total.

Finally, for P_3 we get:

$$P_3 = (0,008 \quad 0,242 \quad 0,732) \qquad (10)$$

This calculation shows that the determination of terrorists to attack aircraft with three missiles is established, although it can get close to accomplishing the mission at a rate of 60% using only 2 missiles.

3. THE GAME MODEL

Game theory is not a new concept in the field of aviation security system. The gain of using a game theoretic approach is that it may help stakeholders from aviation (airliners, industries, government, and so on) to find the optimal solution (technical and strategical) for the aircraft to become more secure, to ensure best possible protection against advanced air defense devices, and a higher survival rate as in the case of a terrorist attack.

Regard each terrorist attack, which may cause a transition in the stochastic model as an action in a game, then the interactions between the attacker and the system can be modeled as a two-player game, as illustrated in figure 2 [6].

The game consists of:

- the two players: N={1,2}={attacker, system};
- the strategy spaces of players: S_k,k=1,2,…,n, where S_k is the set of all available strategies to player k;
- the payoff function of player: V_k:S→R, k=1,2,…,n.

Let X and Y crowds pure strategies of the two players (A, B), where $X \in S_1$, $Y \in S_2$, and be $x \in X$ and $y \in Y$ pure strategies chosen by two players [7,8].

If each player has a finite number of pure strategies, meaning $X = (x_1,\ldots,x_m)$ and $Y = (y_1,\ldots,y_n)$, than the game can be represented by the matrix:

$$V = \begin{Vmatrix} v_{11} & v_{12} & .. & v_{1n} \\ v_{21} & v_{22} & .. & v_{2n} \\ .. & .. & .. & .. \\ v_{m1} & v_{m2} & .. & v_{mn} \end{Vmatrix} \tag{11}$$

In most cases the terrorist does not know exactly the possibility that the attack is countered by the system, game theory says that he should assume that his opponent is aware of the game that tries to minimize the gain expected by the attacker [9].

If player A chooses strategy x_i, must expect the player to respond to that strategy B which corresponds to the lowest gain, y_j strategy that is determined by:

$$\alpha_i = \min v_{ij} \tag{12}$$

Armed with m pure strategies, player A will seek to maximize earnings:

$$\alpha = \max \alpha_i = \max_i \min_j v_{ij} \tag{13}$$

After a similar reasoning, player B will apply one of the strategies that did not lose more than β, where:

$$\beta = \min \beta_j = \min_j \max_i v_{ij} \tag{14}$$

Using the example from the previous chapter, the gain matrix may be made depending on shooting conditions (training drawer, weather, etc.) and use of protective measures (assets, liabilities, none) of the aircraft:

V=

	y_1	y_2	y_3
x_1	v_{11}	v_{12}	v_{13}
x_2	v_{21}	v_{22}	v_{23}
x_3	v_{31}	v_{32}	v_{33}

=

	act.	*pass.*	*no*
1R	**0,1**	**0,2**	**0,3**
2R	**0,2**	**0,4**	**0,5**
3R	**0,3**	**0,5**	**0,7**

(15)

Lower values of α and superior β of the game are:

$$\alpha = V = \beta = 0{,}3 \tag{16}$$

meaning the strategy x_3 for the A player and the y_1 strategy for the B player are optimal strategies.

Thus, the conflicting parties must understand that if you do not meet up maxmin strategies, namely minmax they may lose more.

In the example shown, player A must necessarily choose x_3 strategy, any strategy chosen in the hope of winning more can be prevented by player B.

It is assumed that both players know the game matrix and that they choose a certain strategy, based on the premise that their opponent is at least as good at it and will do everything to prevent him from achieving his goal.

4. CONCLUSIONS AND FURTHER WORK

Even if the model presented is quite simple, it could be a start for extended approach that includes more than one type of attack and there are more than two possible ways to reach the safety system state.

In drawing up the mathematical model of the game does not always stand out as not optimal strategies. Even if both players know the rules, they do not know the consequences of selected strategies.

Also, game theory shows that in cases where the attacker does not know the probability of being countered by the system, abandoning the strategy would result in loss of warranty minmax expected earnings, which would be contrary to the logical behavior. A "one-shot game" with a minmax solution in such cases may be more appropriate for modeling the expected behavior of attackers.

The theoretical model presented in this paper offers a realistic scenario of what could happen today in the aviation security system, even if they require further research, including validation of the used data.

REFERENCES

1. Tudorache, P., Modelul lanturilor Markov la studiul actiunilor de lupta. *AFT Journal.* Issue 1 (2006).
2. Grad, V., *Cercetarea operationala in domeniul militar.* Bucuresti: Sylvi Publishing House (2000).
3. Hampu, A., *Cercetari operationale si modelarea sistemelor militare.* Sibiu: ATU Publishing House (1999).
4. Lye, K., Wing, K.S., Game strategies in network security. *Proceeding of 15th IEEE Computer Security Foundations Workshop* (2002).
5. Wang, D., Madan, B.B., Trivedi, K.S., Security analysis of sitar instruction tolerance system. *ACM SSRS'03* (2003).
6. Sallhammar, K., *Stochastic Models for Combined Security and Dependability Evaluation.* Source [online]. Available: http://www. ntnu.diva-portal.org (December, 2010).
7. Stahl, S., *A Gentle Introduction in Game Theory.* American Mathematical Society (1991).
8. Stevens, F., Courtney, T., Model based validation of an intrusion-tolerant information system. *Proceeding of the 23rd Symposium on Reliable Distributed Systems* (2004).
9. Rosu, A., *Teoria jocurilor strategice.* Bucuresti: Military Publishing House (1967).