A Spatial Model against Air based Terrorist Attacks

Abouzar Ramezani*, MohammadReza Malek**

*, Malek Ashtar University of Technology, Tehran, Iran, abouzar.ramezani@gmail.com
** GIS Department, Faculty of Geodesy and Geomatic Engineering K.N.Toosi university of technology, Tehran, Iran, mrmalek@kntu.ac.ir

Abstract. As terrorist groups has undoubtedly acquired some missiles, preparing a spatial framework for analysis of such threats is of great importance for countries. Intelligent air based threats are considered as the main elements of the terrorist attacks that damage the critical infrastructures. Air defence systems playing a strategic and decisive role in defense networks require smart management and operational mechanisms to countermeasure the threats and risks, both quickly and decisively. The spread of terrorist groups, security around the world, have been threatened and should think over to reduce the vulnerability and increase the safety of critical infrastructure. Infrastructure safety management needs to consider all parameters that affect the vulnerability of infrastructure. To exploration the nature of each factor that effect vulnerability of infrastructure against airborne threat and the relation between factors will lead to the creation of a spatial framework. Our suggested spatial model facilitates the analysis, planning and decision-making in relation to reduce the vulnerability of infrastructure. To evaluate the efficiency of developed framework a method proposed to reduce vulnerability of infrastructures and to banish airborne threats equipped with GPS and INS.

Keywords. Spatial Model, Vulnerability, Airborne Threats, Infrastructure, Terrorism

1. Introduction

After the September11th terrorist attacks, worldwide focus on preventing and curbing terrorist activities is highly accelerated [1]. The total number of deaths caused by terrorism has been increased by 80 percent when compared to the figure in the prior year [2]. Terrorist groups have now achieved a variety of weapons, ammunition and equipment, and they have the capability to damage and destroy targets by their members without entering any official ground conflicts.

One of the most important factors that can curb terrorist threats is to identify their targeting areas. Lessons learned from the past support the idea that the terrorist objectives are to break the will of the people and weaken the state power, both militarily and economically, and their strategy is to destroy the centers of gravity, thereby focusing on bombing and destruction of the crucial infrastructures [2, 3].

LBS 2016
13th Conference on Location-Based Services
Vienna, 14–16 November 2016

Published in "Proceedings of the 13th International Conference on Location-Based Services", edited by Georg Gartner and Haosheng Huang, LBS 2016, 14-16 November 2016, Vienna, Austria.

Many studies in different countries have investigated the vulnerability of critical infrastructures against terrorist threats. The need for a framework that provides decision making in the field of security and risk is widely recognized. In this context, some studies have been carried out, one of which is a decision framework for safety and risk management [4]. Research conducted recently has been in the field of protective proceeding to reduce risk. A framework has been developed for managing a rapid response in the face of threats against oil and natural gas fields [5]. A risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructures was developed in 2009 [6]. This decision support framework considers threat scenarios and probabilities, value of human life, physical damage, indirect damage, risk reduction and protective measure costs. Probabilistic terrorism risk assessments that quantify the costs and benefits are conducted for three items of infrastructure using representative cost and vulnerability data. Based on our knowledge, no work has addressed spatial framework for vulnerability assessment due to air based threats. One of the issues not resolved yet is introducing various strategies to reduce the vulnerability of infrastructures for which such a methodology could be proposed.

2. The principles of spatial framework

The aim of developing spatial framework is providing the ability of make different model to assessment vulnerability of infrastructure against airborne threats based on effective indicators, in order to understand, explain or predict the behavior of airborne threats and infrastructure. Our model is designed in such a way to reflect the fact that they embody certain aspects of the real world. After testing model a better understanding of vulnerability achieved.

In the developed spatial framework, there are four main objects that should be considered. These include passive defense object (D_p), active defense object (D_A), target object (T), and threat object (T_h). The relationship between objects are destruction (Des), deviation (Dev), protection (Pro), capturing information (Cap).

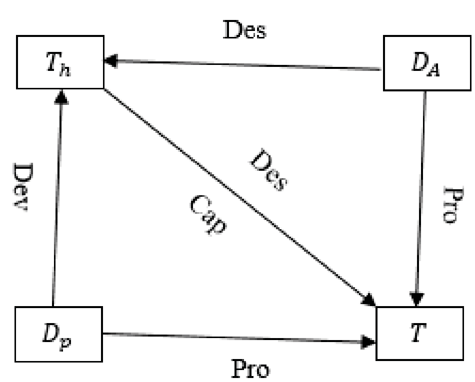

Figure 1. Relations between framework objects

A spatial framework for vulnerability analysis of infrastructure due to airborne threats as part of the general framework is developed. This framework has four main objects including airborne threat, infrastructure, radar system and misleading. Airborne threats as subset of the original threatened object are one of the main factors that damages infrastructure, which infrastructures are considered as a key element of life of a country. Radar detection systems as a protective operator have been deployed in many strategic areas of the country to identify airborne threats and avoid hitting to critical infrastructure. Jammers as passive operator protect and reduce the vulnerability of the infrastructure by disrupt the performance of threats.

Each of framework objects has properties that effect vulnerability analyzing of infrastructure. The Fig. 2 shows the properties of framework objects. Airborne threats for capturing information act like a dynamic spatiotemporal conical object. Properties include navigation error, start and end points of motion, movement restrictions and data about the volume, height and beam angle are specified. In this type of airborne threat behavior information capture by sensors and volume properties are determined by sensor resolution. Airborne threats for destructing infrastructures operate like a dynamic spatiotemporal point object, and its properties are specified. Radar system operation is like a dynamic in time spherical object and characteristics including position, horizontal and vertical coverage angle should be identified. Jammers operate like a conical static object and characteristics include beam angle and height are determined by this equipment.

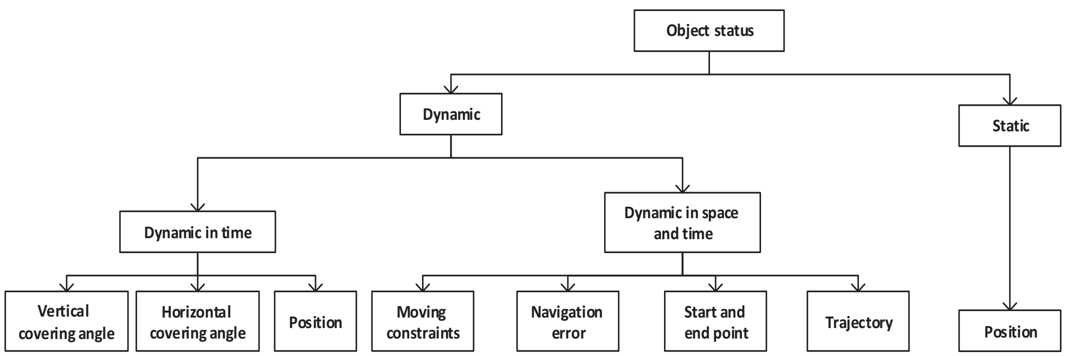

Figure 2. The properties of object status

Infrastructure behaves differently against threats. If terrorist want to capture information, infrastructure act such as a 3dimensional planar object. Whenever threats act as destructor, infrastructure act such as a 2 dimensional planar object. For a two-dimensional planar object, radius of vulnerability must be identified.

After determining the type of objects, affecting functions in vulnerabilities of infrastructure against airborne threats will be determined for each of the objects. For example, explosion functions of threat, vulnerability functions related to infrastructure and other functions of objects are specified. After determining the effective functions of each objects, framework provide the possibility to define different scenarios for vulnerability analysis.

3. Framework evaluation

For evaluating spatial framework, a model for analysis and reducing vulnerability of infrastructure is extracted and implemented. Fig. 3 shows implementation of the most probable path of airborne threats so that is would not be visible to radar object and the best location for deploying jammers. By identifying the vulnerability radius of infrastructure and the accuracy of the INS, locations of jammers could be estimated. By considering the explosion threat outside the vulnerability radius of the infrastructure, jammers should be positioned at a distance of 146.26 kilometers, or more with respect to infrastructure.

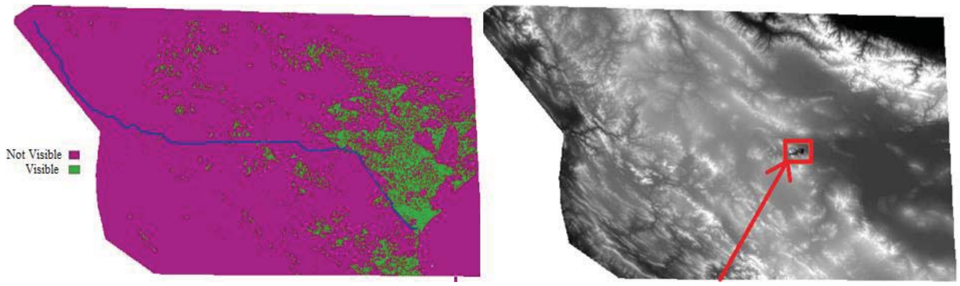

Figure 3. Implementing the most probable path of the threat by considering radar coverage

Fig. 4 shows the locations of the misleading in the three-dimensional view. As can be seen, the threat is moving in route and not visible to radar detection object.

At present, the focus is on the deployment of jammers near the infrastructure. Due to the high power of these jammers, they are identified by attackers and are, therefore, destroyed by the attackers. Another weakness of these systems is that the time of disturbance is short and against the high accuracy of inertial navigation system, thereby lowering the vulnerability degree of the infrastructure against new threats.

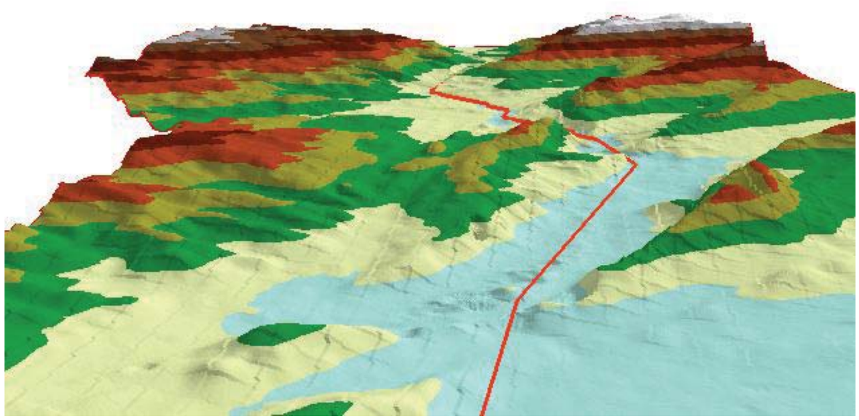

Figure 4. The three dimensional view of jammer position

By assuming that the jammers are not detected and the conventional model is employed, by establishing the high power jammer for 50 kilometers disturbances, the comparative results are shown in Table 1.

Table 1: Comparing the proposed model with the conventional model

The extent of damage	The distance between threat and target	Model
1%	1577	Proposed model
87%	183	Conventional model

4. Conclusions

A spatial framework for vulnerability Analysis against airborne threats is one of the basic needs of administrators, planners and stakeholders of infrastructures. Due to the increase in the number of terrorist groups and their access to military equipment, managers require a framework that can consider all the parameters that affect the vulnerability of infrastructures and employ measures to counter the threats. In this research, all factors influencing vulnerability of infrastructures were identified and a spatial framework was developed for the design and modeling of different scenarios. For evaluating spatial framework, a model for analysis and reducing vulnerability of infrastructure is extracted and implemented. In this model, the most probable paths of access to infrastructure were identified, and then the radius of the vulnerability of the infrastructure was calculated; in the final step, the optimum location of jammers was selected. Using the developed framework, different scenarios for analyzing vulnerability of infrastructure could be examined.

References

[1] M.G. Stewart, Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure, International Journal of Critical Infrastructure Protection 3(1) (2010) 29-40.

[2] Global Terrorism Index, Measuring and Understanding impact of terrorism,institute for economics and peace, Sydney, 2015.

[3] M.G. Stewart, Cost effectiveness of risk mitigation strategies for protection of buildings against terrorist attack. Journal of Performance of Constructed Facilities, 22(2) (2008) 115-120.

[4] L. Twisdale, R. Sues, F. Lavelle, Reliability-based design methods for protective structures, Structural safety, 15(1) (1994) 17-33.

[5] M.G. Jaatun, E. Albrechtsen, M.B. Line, I.A.Tondel, O.H. Longva, A framework for incident response management in the petroleum industry. International Journal of Critical Infrastructure Protection, 2(1) (2009) 26-37.

[6] M.R. Driels, Weaponeering: Conventional weapon system effectiveness. American Institute of Aeronautics and Astronautics, Virginia, 2004.