Available online at www.sciencedirect.com

ScienceDirect

European Journal of Operational Research 180 (2007) 1394–1410

EUROPEAN JOURNAL OF OPERATIONAL RESEARCH

www.elsevier.com/locate/ejor

O.R. Applications

Simulation modelling and analysis of a border security system

Gökhan Çelik [a], İhsan Sabuncuoğlu [b,*]

[a] Infantry School Istanbul, Turkey

[b] Department of Industrial Engineering, Faculty of Engineering, Bilkent University, 06533 Ankara, Turkey

Received 25 February 2005; accepted 18 April 2006
Available online 11 July 2006

Abstract

Border control is vital to the security of a nation and its citizens. All countries look at measures to improve the security of their borders. But increasing security can bring a substantial financial burden. In this study, we analyze the border security problem of Turkey using a simulation approach. Our main objective is to find more efficient ways of improving border control and security along Turkey's land borders. To achieve this, we examine the structure of the border security system and its major elements, examine the relationships between performance measures, and assess the effectiveness of security elements on each system performance measure. We also look into the issues of planned changes and additional resources, and we evaluate new alternative system designs. The results of simulation experiments are analyzed by statistical methods.
© 2006 Elsevier B.V. All rights reserved.

Keywords: Military simulation; Border security

1. Introduction

Border control is vital to the security of a nation and its citizens. International terrorism, worldwide illegal immigration and refugee problems, and drug and arms smuggling are of concern to all states. Every country employs some measures to secure its borders. Since today's security systems depend on technology and personnel, efforts to increase border security will result in substantial financial costs. Hence all states try to optimize their resources while remaining effective.

The objective of this study is to identify the possible ways of increasing border control and efficiency of security along Turkey's borders. Specifically, we model the operational activities of a border company supported by a battalion and examine the existing system via simulation. First we analyze the main structure and components of the present system and to assess its effectiveness using the performance measures such as the ratio of illegal infiltrations caught, degree of controllability, and frequency of controlling. Second, we attempt to understand the relationship between security elements and performance measures. Third, we study the effect of each security element on selected performance measures and determine the degree of importance of each security element. Fourth, we identify the factors that significantly affect the performance measures and measure the

[*] Corresponding author. Tel.: +90 312 290 1262; fax: +90 312 266 4126.

E-mail addresses: celik@bilkent.edu.tr (G. Çelik), sabun@bilkent.edu.tr (İ. Sabuncuoğlu).

0377-2217/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.ejor.2006.04.040

sensitivity of the system responses to changes in the system environment. Finally, we evaluate new system design alternatives to improve system performance. In all of these stages, our aim is to find possible ways to increase border security in a cost effective manner.

Although the topic is important and vital to the security of a nation, we could not find any studies in the literature that analyzed border security systems. There are several GAO (General Accounting Office is the investigative arm of Congress in US) and CRS (Congressional Research Service) reports related to border control and security. In their CRS report (June 18, 2001), William J. Krouse (Analyst in Social Legislation; Domestic Social Policy Division) and Raphael F. Perl (Specialist in International Affairs; Foreign Affairs, Defense, and Trade Division) explain the importance of border security and propose some options to prevent illegal entry into the United States. In GAO reports, some precautions are proposed and evaluated. These include: (1) concentrating personnel and technology resources, first in the sectors having the highest level of illegal infiltration activity and moving to the areas with lesser activity, (2) making maximum use of physical barriers to deter entry along the border, (3) increasing the proportion of time border patrol agents spend on patrol, and (4) identifying the appropriate mix of technology and personnel needed to control the border.

The rest of the paper is organized as follows: In Section 2, we define the problem and its scope. In Section 3, we explain the model development process. In Section 4, we examine the system behavior, interactions between system components and performance measures; and assess the effects of each security element on the selected performance measures. In Section 5, we present the results of the experimental design to identify the significant factors. In Section 6, we compare alternatives using ranking and selection and multi-criteria decision-making procedures. Finally, we give concluding remarks and future research directions in Section 7.

2. Problem definition and system description

Turkey has 2852 km of land borders. Border troops from the Land Forces have the task of securing the borders; the General Staff approves troop organization. Each border battalion consists of three border companies and one headquarters company which both supports the activities of the border battalion commanders and provides logistical support for border companies. Border companies consist of border platoons who execute operational tasks. Border platoons (border posts) are located along the borders; they are equipped with technology and supported by personnel so that they can execute their tasks in both peace and war.

The border Security System consists of both physical barriers and a border surveillance and control system. These complementary systems can be used together or separately; the main factors affecting the use of these systems are the importance of the region, the level of threat and the nature of the terrain. Since the *Border surveillance and control system* contains all active precautions against unauthorized entry into or exit from the country, it is the core of the border security system. The main security elements of this system are border patrols, ambushes, sentries, thermal cameras and askarad. We briefly explain the elements as follows:

Border patrols: A patrol consists of three soldiers from a border platoon that watches and controls a specific section of the border. They depart according to accomplish a task from the border posts. The task occupies some time interval. Upon execution of the task they return to their respective border posts. They patrol the borders day and night.

Ambushes: An ambush is a concealed force that captures a person crossing the border illegally. Ambushes may be stationary or mobile. Stationery ambush troops are stationed at one point; mobile ambush troops work at different points at different times through the night. Ambushers work only at night.

Sentries: Sentries' main task is to watch the borders and terrain of neighbor. They are on duty during the day in watchtowers, constructed at specific observation points along the borders.

Thermal cameras: A thermal camera system is an infrared imaging system, which enables target detection, recognition and observation capabilities in all weather conditions. The passive nature of such imaging provides fully covert surveillance. They have many advantages in military usages: they are light, portable and quite; they can be repeated by one man; they are unaffected by poor field and weather conditions; they provide excellent images. Thermal cameras are used for border and port/harbor surveillance and protection of headquarters and military zones. Thermal cameras are under the control of the border company and are used only at night. Like ambushes, they can be stationary or mobile.

Askarad: Askarad, ground surveillance radar, is a new generation radar system. It is used for surveillance, target acquisition and moving target classification, precision location of targets, plotting of targets on a display, adjustment of artillery fire, guidance of small ground or airborne attack units, and helicopter navigational particularly homing. Askarads are operated both day and night and again can be stationary or mobile.

Both the thermal camera and askarad are electronic surveillance systems. The main difference between them is their range. Askarad is capable of detecting targets 4–5 times farther a way the thermal camera. All these security elements are used together to achieve the highest possible security. The problem is to use these resources in such a way that border security in fact is increased. In the next section, we discuss our approach to this problem.

3. Model development

The border security system has several stochastic elements and the military end-users want to see how the system behaves over several performance measures. The users also want the answers to several "what if" questions that arise during operation. Therefore, we use simulation as a modelling and analysis tool to study the border security problem.

The conceptual model is the first step in the simulation modelling process. At this stage, we determine the relevant elements of the system and their interrelationships (Banks et al., 1996). In practice, the border troops have many tasks beside border security, but we will focus only on this operation.

Daytime border control is not a focus of this study. When visibility is good, sentries stationed at watchtowers can see wide sections of the border, the control is almost too good. For this reason, illegal infiltrations peak at night as terrorists, smugglers, refugees and enemy forces take advantage of poor night visibility. Therefore, the full border security system operates at night as does our model. In our model, the entities are patrols, ambushes, thermal cameras, askarads, illegal infiltrations and zones. There are three main performance measures that reflect the effectiveness of the whole system. These measures are determined by consulting the army officials who plan the border control activities.

1. Degree of controllability (DOC) is the percentage of time that a zone being monitored by security elements. The border is divided into small areas or segments, are called zones. The percentage is calculated for each zone and the average of all zones is used as the performance measure.
2. Frequency of control (FOC) represents the number of time intervals that a zone is under control by security elements. The average of all zones is calculated for this performance measure.
3. Ratio of illegal infiltrations caught (ROIIC) measures the ratio of caught illegal infiltrations to the actual total number for a given zone in 1-year time period. The average of all zones is considered as the third performance measure.

For example, a particular zone is controlled successively by a border patrol and ambush for the duration of X and Y minutes, respectively. Assume also that three illegal immigrations are attempted but only one of them is caught in the total period of time Z. In this example, DOC is equal to $(X + Y)/Z$, FOC is equal to 2 (due to one patrol and one ambush) and ROIIC is equal to 1/3 (one of the three are caught).

Fig. 1 shows the input/output process of the model. Some of the input variables are random variables. The list of these random variables and their distribution functions are given in Table 1. In general, we use historical data and taken from army field manuals. Analysis of historical data suggests that an exponential distribution is suitable for modelling the arrival process of illegal infiltrations. We use a triangular distribution for the infiltration time of each type of infiltration as suggested by the literature in the absence of data. The parameters of the distributions are determined by using Border Services Instructions (KKY 118-1, 1999) and by consulting border troop commanders.

By examining the relationship between the elements of the system, we develop the logical model. As seen in Fig. 2, it starts with the movement of security elements from their locations and ends with their return to their start locations. The random arrival of illegal infiltrations is considered. The relations between these entities and events are presented in Fig. 2 to clarify the logic of the model. In this figure, departure of security elements from their locations by type and arrivals of illegal infiltrations are presented. The rest of the figure is the general flowchart model of the system. Security elements depart their locations for duty according to weather condi-

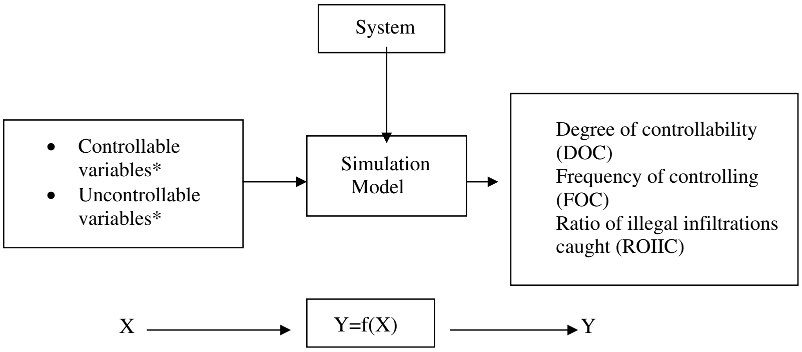

System
• Controllable variables*
• Uncontrollable variables*
Simulation Model
Degree of controllability (DOC)
Frequency of controlling (FOC)
Ratio of illegal infiltrations caught (ROIIC)
X
Y=f(X)
Y

Fig. 1. The input/output process of the model.

tions and failure conditions of high-tech devices. Meanwhile, type of duty (stationary or mobile) and duty places are determined. Then, their relations are presented according to presence of other elements in the zone or arrival of any security element while other one is already in that zone. If security elements complete their duty, they go back to their home-based locations. Otherwise, new duty places are assigned. This continues until each security element completes its duty. The logical model is coded in ARENA simulation system.

By examining the relationship between the elements of the system, we develop the logical model. As seen in Fig. 2, it starts with movement of security elements from their locations and ends with returning to their start locations. The arrivals of illegal infiltrations are considered. The relations between these entities and events are presented in Fig. 2 to clarify the logic of the model. In this figure, departure of security elements from their locations by type and arrivals of illegal infiltrations are presented. The rest of the figure is the general flowchart model of the system. Security elements leave their locations for duty according to weather conditions and failure conditions of high-tech devices.

Meanwhile, type of duty (stationary or mobile) and duty places are determined. Their relationships are given according to presence of other elements in the zone or arrival of any security element while other one is already in that zone. If security elements complete their duty, they go back to their home-based locations. Otherwise, new duty places are assigned. This continues until each security element completes its duty.

The logical model is coded in ARENA simulation system. ARENA is based on the SIMAN discrete event simulation language. In the ARENA system, entities (dynamic components of the system)

Table 1
Random variables and their distribution functions

Random variables	Distribution functions
Arrivals of illegal infiltrations	Exponential
Type of illegal infiltrations	Discrete
Infiltration time for each type of illegal infiltration	Triangular
Duty time of patrols	Triangular
Duty time of ambush, thermal camera and askarad	Triangular
Duty time before high-tech equipment failure	Uniform
Weather conditions	Discrete
Failures before and on duty	Discrete
Determination of mobile or stationary characteristics of duty	Discrete
Determination that patrols are motorized or on-foot (for each platoon)	Discrete
Determination that ambushes have night-vision device or not	Discrete
The degree of use of high-tech devices	Discrete
Determination of first points where each ambush is assigned to perform its duty	Discrete
Determination of first point where thermal camera is assigned to perform its duty	Discrete
Determination of first point where askarad is assigned to perform its duty	Discrete
Determination of next point where thermal camera will continue to perform its duty, if it is assigned as mobile	Discrete
Determination of next point where askarad will continue to perform its duty, if it is assigned as mobile	Discrete
Determination of next points where each ambush will continue to perform its duty, if it is mobile	Discrete

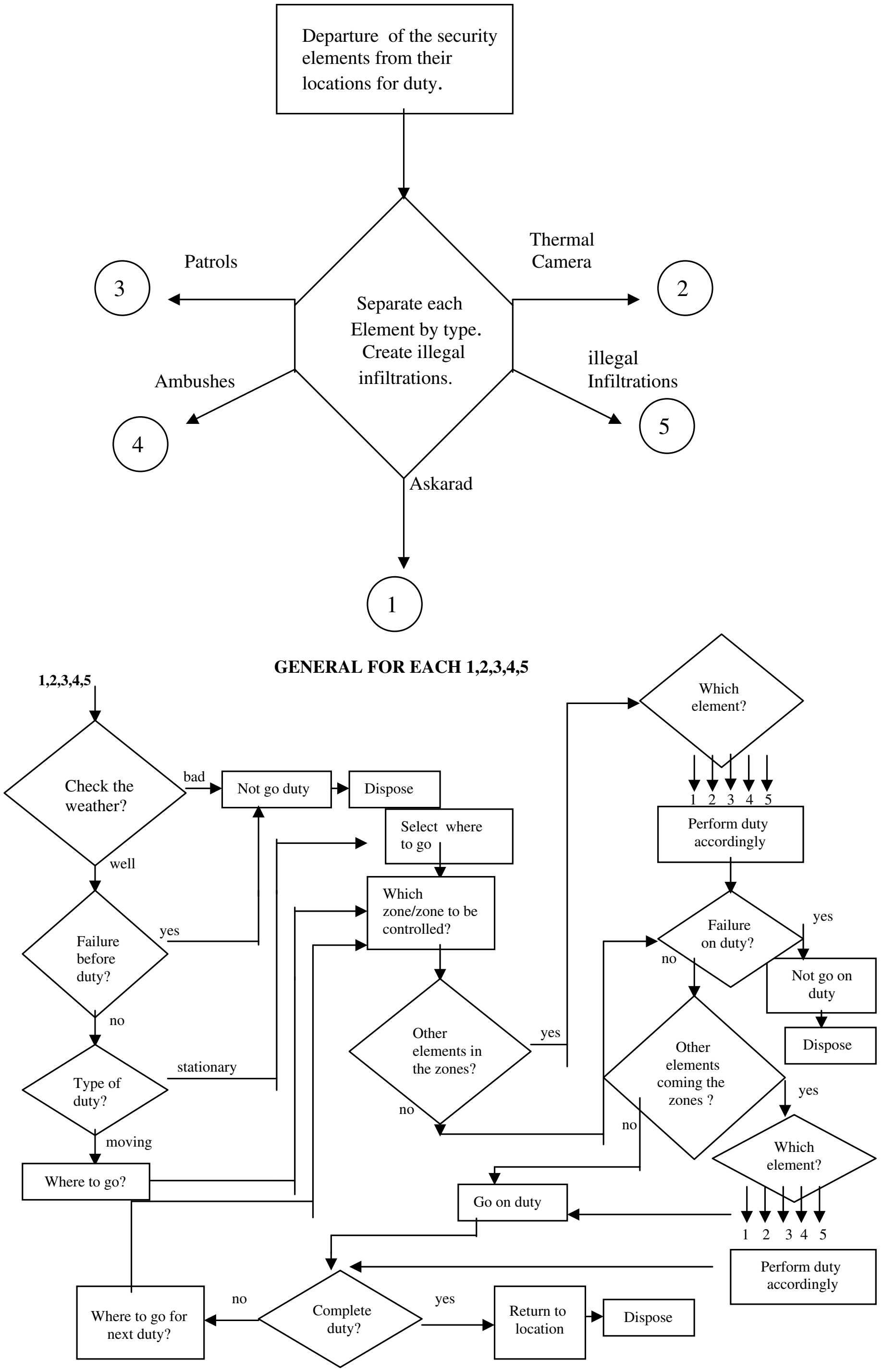


Fig. 2. The simplified flowchart of the model.

are generated to visit resources successively according to the process plan in the model operational logic. While entities are moving in the system, random events are triggered and statistics are collected. During the model execution, the state and output variables are also updated. In our implementation, we use the elements of the border security system (askarads, ambushes, etc.) to model dynamic entities and zones as the resources in the system. The statistics of three performance measures are reported as the model output.

3.1. Verification/validation of the model

We use the techniques proposed by Balcı (1998) in the validation process. For verification, we first use the Arena trace option to see if the program runs as intended. The border security system model contains four border platoons, each of which is modeled by a different subprogram. We check each subprogram individually. We also run the simulation model to test model behavior under certain conditions. Additionally, we employ an animation tool to see the consistency of the model behavior. A view of the animation page is given in Fig. 3.

In the validation process, we use the techniques in Department of Army Pamphlet 5-11 (1999). We first use Fault/Failure insertion test. This test is used to observe if abnormal behavior results from a faulty input (incorrect model component). To implement, we add a new security element that is much more effective than a thermal camera (incorrect model component). As seen in Fig. 4a, the degree of controllability jumped to 80% from 25% of thermal camera.

Secondly, we change the operation of thermal camera and askarad. In the new setting, they are positioned at one place to control limited areas (incorrect behavior of a model component). As seen in Fig. 4b, the DOC deteriorates about 30% displaying the invalid behavior of the model as expected.

We also compare the simulation results with the results of manual calculations to validate the simulation model. As seen in Fig. 5, the results of manual calculations are slightly higher than the simulation results. This is due to the fact that the same zones can be controlled simultaneously by different security elements in the real system (i.e. the effects of different elements can be overlapping). When the simulation model encounters such a situation, it takes only one of the security elements into account. On the other hand, manual calculation cannot consider such overlaps and hence it reports higher values. We also conduct a number of experiments by systematically changing the values of model input variables and parameters over the range of the input parameters. We do not observe any unexpected effect of input variables on outputs. In general the results are as expected.

4. Simulation results: Preliminary analysis

We set the sample size by adjusting simulation run-length and the number of replications. To achieve the desired accuracy (10% relative precision), we first run the simulation model for five replications for different run-lengths. We use DOC as the performance measure and calculated point and interval estimators (i.e., mean and confidence interval). The results indicate that half-length as an

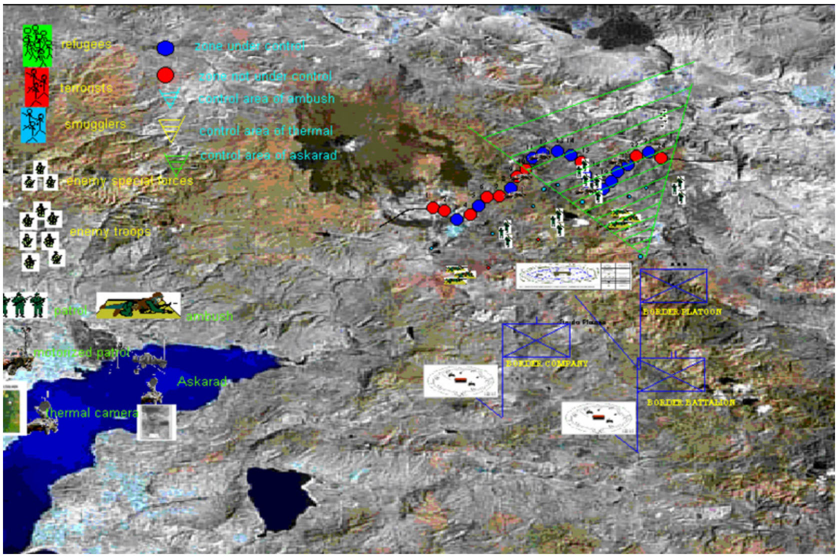


Fig. 3. An animation screen from the simulation model.

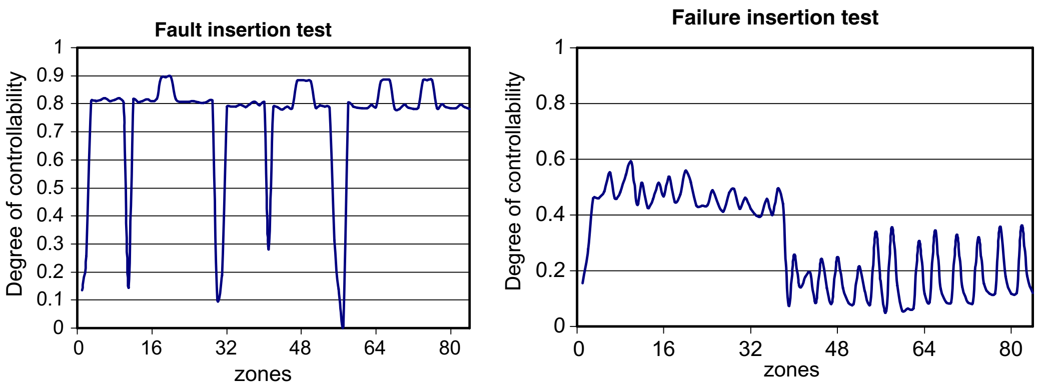


Fig. 4. Fault/failure insertion test.

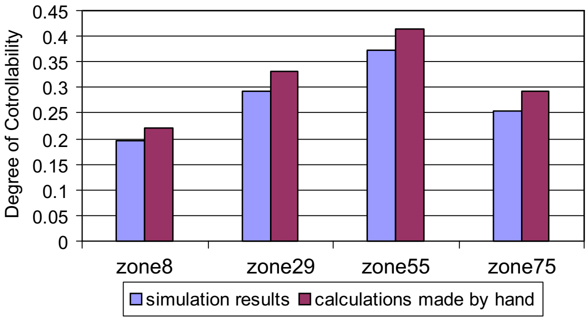


Fig. 5. Comparison of simulation model results and calculations made by hand.

indicator of the accuracy varies for different zones. Since our aim is to achieve the desired accuracy in the worst-case situation, we decided to use the half-length of a zone with the maximum half-length of all the zones for a given run-length. Fig. 6 presents the results at various run-lengths. Note that the curve gets flat after a run-length of 6-month, this means that variance of the estimator stabilizes with this sample size.

After consulting with border troop commanders to set the values of the desired precision level), we calculate number of replications required to obtain an absolute precision 0.02 (approximately 10% relative precision) for different simulation run-lengths, starting from 6-month run-length for degree of controllability. To determine sample sizes, we use the two-stage procedure suggested by Law and Kelton (1991). The results indicate that 1-year run-length and 10 replications is enough to achieve the desired accuracy. Using these sample sizes, we conduct the simulation experiments and obtain the point and interval estimators for each performance measure at various confidence levels, e.g., 90%, 95%, and 99%. When the resulting confidence intervals are actually examined, it is observed that both absolute and relative precisions for each performance measure are satisfied (Table 2).

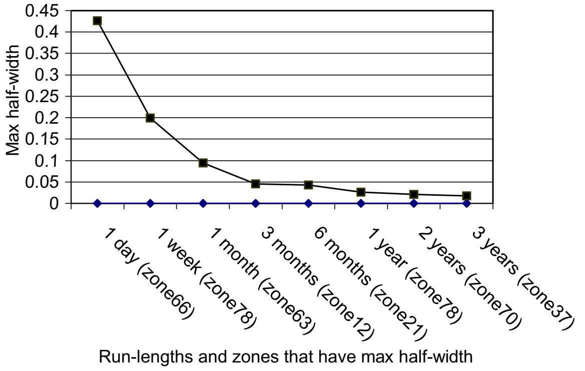


Fig. 6. Determination of run-length for degree of controllability.

4.1. Analysis of simulation results

After developing the simulation model and determining sample size, we begin to analyze system behavior for each performance. First, we examine the effects of the security elements on each perfor-

Table 2
Desired precisions

Performance measure desired precision	Degree of controllability	Frequency of controlling	Ratio of illegal infiltrations caught
Absolute precision	0.02	100	0.025
Relative precision	10%	5%	5%

mance measure. The results of the simulation experiments for DOC are given in Fig. 7a. Note that some of the zones have a higher degree of controllability than others; meaning control is not uniform along the border; this is due to variability in using security elements in the different zones. To explain the behavior of DOC, we also run the simulation model with only one security element. The distributions of DOC in this case are given in Fig. 7b–e. In general, ambush shows the most variability in DOC, since they are used only uniformly along the borders. Note also that the behavior of thermal cameras and askarad is similar and falls in between ambush and patrols. This is because thermal cameras and askarad provide security for wider piece of the border than they are stationed. Looking again at overall effects of all security elements in Fig. 7a, we note that the DOC measure is mostly affected by the ambushes. The spikes that are observed are due to the fact that zones in the neighborhood of two consecutive sections of the border can be covered twice and hence the performance improves for these zones.

Fig. 8 provides the results for FOC. Again, distribution of FOC is not uniform along the border due to the different mobility characteristics of each security element. We note that zones 25–60 have lower FOC than other zones. This difference is due to different patrol capacity; the 1st and 4th platoons have the patrol capacity for two sides (patrols on two routes simultaneously) whereas the 2nd and 3rd platoons can only patrol one side. Because the most

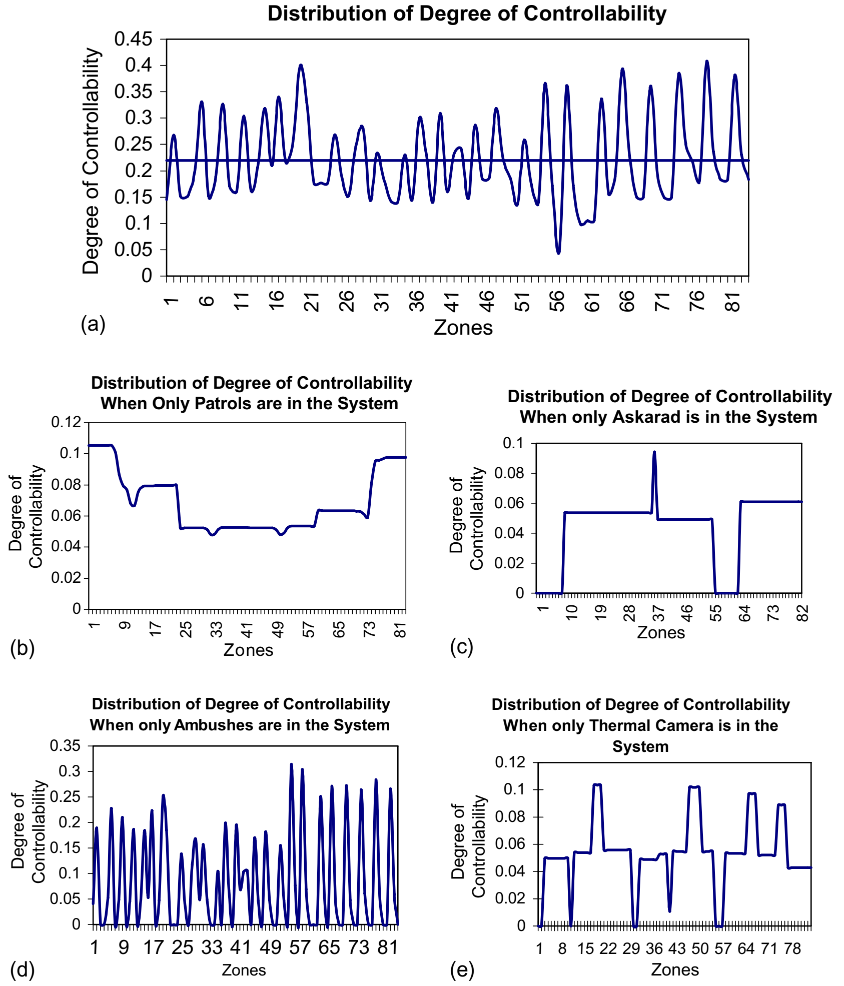


Fig. 7. Behavior of the system for degree of controllability: (a) degree of controllability (all security elements are in the system), (b) distribution of DOC (using only patrol), (c) distribution of DOC (using only askarad), (d) distribution of DOC (using only ambushes), and (e) distribution of DOC (using only thermal camera).

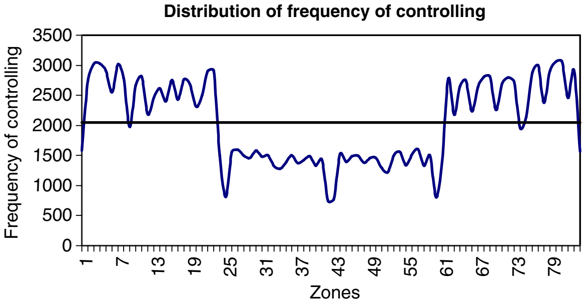


Fig. 8. Behavior of the system for frequency of controlling.

mobile security element in the system is patrols, we conclude that the FOC measure along the borderline is mostly affected by patrols.

Fig. 9 shows the behavior of the system for ROIIC. The distribution of ROIIC is a similar shape to the distribution of FOC because of the decreased patrol capacity in zones 25–60. We also compare the distributions of DOC and ROIIC and note that ROIIC is low where DOC is low. These observations raise the question of the potential relationships between DOC, FOC, and ROIIC.

4.2. Relationship between DOC, FOC and ROIIC

Looking first at DOC, FOC and ROIIC, we construct a graph that displays the results of each performance measure at each zone. As seen in Fig. 10, there is a high correlation between these two measures; ROIIC increases as DOC increases.

We also conducted simulation experiments to further study the relationship between DOC and ROIIC; this involves changing the capacity of security elements (patrols, ambushes, thermal cameras, and askarad). Fig. 11 displays the relationship between DOC, ROIIC and the costs incurred at various capacities of security elements. Here, the capacity is adjusted by a multiple of the base capacity. As expected, additional capacity of security elements improves DOC. However, the main purpose of increasing DOC is to improve ROIIC. But improvement in ROIIC is not proportional to increase in DOC. This is because some parts of the border cannot be controlled with high-tech devices (askarad, thermal cameras) due to difficult terrain. Increasing the quantity of high-tech devices, does not necessarily prevent infiltrations; beyond the appropriate number, the additional costs of high-tech devices cannot be justified. ROIIC can be maximized by stationing ambush troops at those parts of the border that cannot be monitored by high-tech devices.

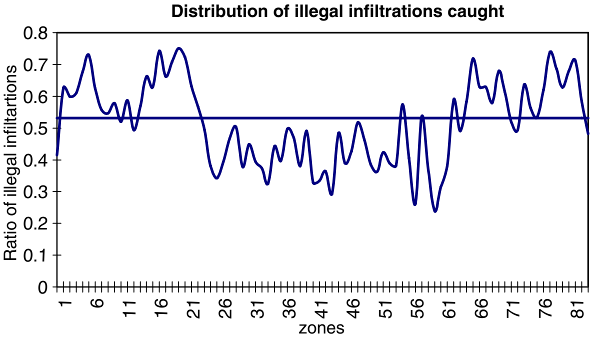


Fig. 9. Behavior of the system for ratio of illegal infiltrations caught.

Second, we examined the relationship between FOC and ROIIC by changing the capacity of patrols. As can be seen in Fig. 12, increasing the capacity of patrols improves FOC. We noted that improvement in FOC and ROIIC is not symmetrical due to the low probability of catching illegal infiltrators such as terrorist or enemy special force.

These infiltrators are well trained and can cross the border quickly in small groups. Thus, increasing the number of patrols does not necessarily prevent infiltrations. Border security planners must decide on the appropriate number of patrols, and then implement precautions such as building physical obstacles or increasing the mobility of patrol. Physical obstacles prolong time needed to infiltrate and increasing the mobility of patrols improves FOC. Both of these precautions increase ROIIC.

4.3. Analysis of the effect of each security element

One of our goals in this study is to assess the effectiveness of the security elements for each performance measure. In the military, it is important for a commander to know his troops' capabilities. Commanders of border troops want to know the capabilities of security elements for protection of borders to determine priorities for maintenance and training activities accordingly.

We run a factorial design to assess the effect of each security element. We consider four factors: patrols, ambushes, thermal camera, and askarad. As seen in Table 3, the high and low values of each element reflect whether they are present in the security system or not.

The results of ANOVA indicate that patrols are the most effective factor in ROIIC (see Fig. 13a).

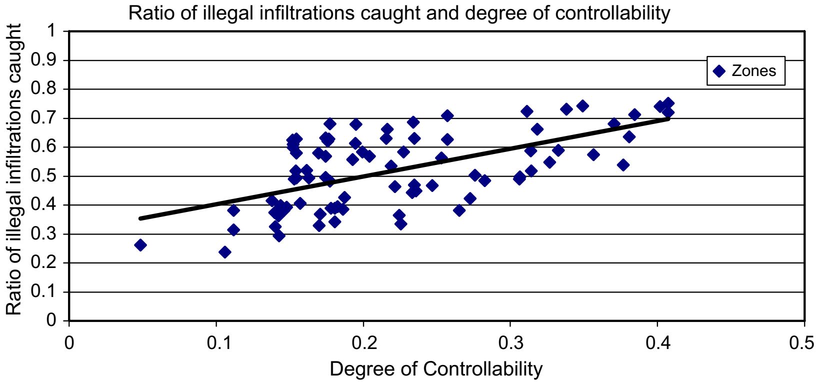


Fig. 10. Correlation between ratio of illegal infiltrations caught and degree of controllability.

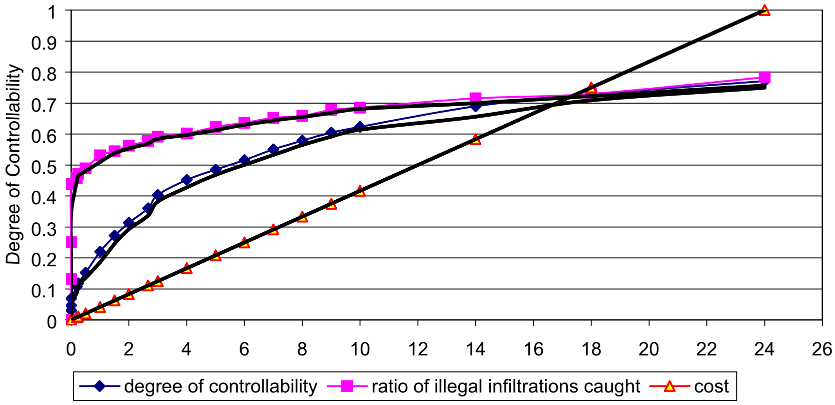


Fig. 11. Relationship between DOC, ROIIC, cost and capacity of security elements.

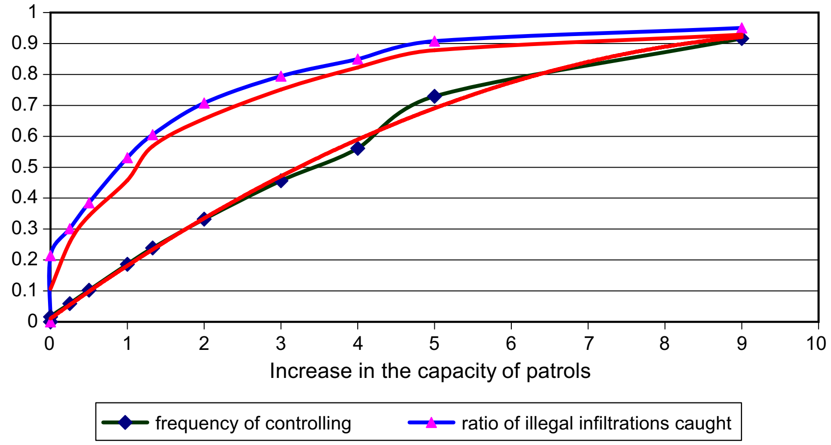


Fig. 12. Relationship between FOC, ROIIC and capacity of patrols.

Other security elements also improve ROIIC, but to a lesser degree. For DOC, each security element has the equal impact (Fig. 13b). For FOC, patrols have a big positive effect whereas the other factors (ambush, thermal camera and askarad) have negative effects.

Table 3
Factors effecting border security system

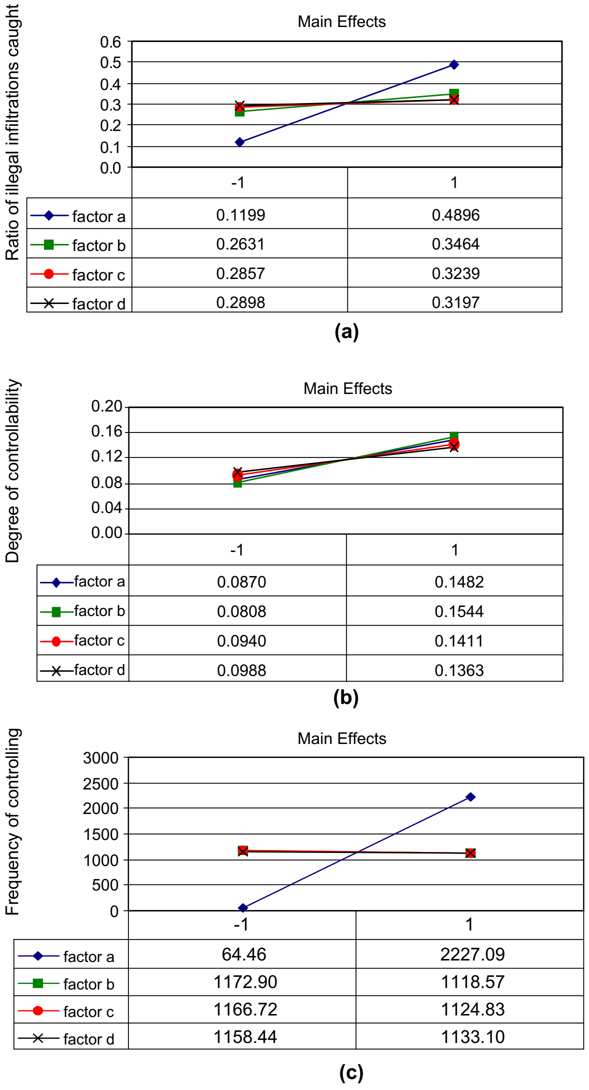
Factor	Factor description	−1	+1
a	Patrols	No patrol in the system	Patrols are typically in the system
b	Ambushes	No ambush in the system	Ambushes are typically in the system
c	Thermal camera	No thermal camera in system	Thermal camera is typically in the system
d	Askarad	No askarad in the system	Askarad is typically in the system

Note that steeper the line in Fig. 13 means that a factor has more significant effect. In the statistical analysis process, we employ the paired-*t* test to see if each security element has significant impact on the performance measures. The results indicate that each security element has significant effect on each performance measure.

5. Analysis of operating policies

In this section, we examine various operating policies related to all the security elements. The policies under consideration are: (1) the degree of use of high-tech devices, (2) the degree of use of night-vision tools, (3) whether elements are stationary or mobile, (4) the degree of use of motorized patrols, and (5) duty time of patrols. We set these factors and their levels according to Border Services Instruction KKY 118-1 (1999) and by consultation with border troop commanders.

Border Services Instruction recommends infrequent use of high-tech devices in order to extend their lifetime. Since failure of these devices is an undesired situation for commanders, some of them seldom use the devices. On the other hand, the protection of borders requires high-tech devices. The above statements are valid for night-vision tools and motorized patrols. Therefore, we set the low and high values of factors *a*, *b* and *d* according to how frequently the devices are used; factor levels indicate the probability of use of the high-tech devices or night-vision tools for duty of that day. The commander also determines whether elements will be used in a stationary or mobile form (factor *c* in Table 4); this varies with the number of critical zones and with terrain. The levels of the factor indicate the percentage of the duty that will be mobile. The maximum time that patrols can spend on bor-



(a)

(b)

(c)

Fig. 13. Main effect diagrams of security elements for each performance measure.

Table 4
Factors and levels of 2^5 factorial design

Factor	Factor description	−1	+1
a	The degree of use of high-tech devices	40%	95%
b	The degree of use of night-vision tools	25%	75%
c	Determination of stationary or mobile characteristics of duty	30%	70%
d	The degree of use of motorized patrols	15%	70%
e	Duty time of patrols	3 hours	4 hours

der control is 4 hours according to Border Services Instruction. But they can also have 3 hours patrols. The factors and their levels are given in Table 4.

We implement a full 2^5 factorial design with ten replications at each design point (factor combination) to ensure randomization. To identify significant factors and their interactions, we use ANOVA (Analysis of variance) technique and a SPSS statistical package program. First, we check two main assumptions (homogeneity of variance and normality). The results of Bartlett's test and Levene's test (Montgomery, 1992) indicate that the common variance assumption is satisfied. By plotting scatter plots of variance and residuals, and drawing histograms of residuals compared with normal, and normal probability plots of residuals, we also verified the normality assumption.

The results indicate that each main factor is significant. As seen in Fig. 14a, the degree of use of high-tech devices (factor *a*) has the greatest impact on DOC (a steeper the line means that a factor has a more significant effect). This is because the high-tech devices are used more frequently. When the high-tech devices is high, zones are under control for longer time periods and DOC increases about 28%. As seen in Fig. 14b, the degree of use of motorized patrols (factor *d*) has also the greatest effect on FOC (38%) because of their high mobility (see Fig. 14b).

Factor *d* also has a significant impact on ROIIC. This is because the improvement in FOC causes an increase in ROIIC of about 13% (Fig. 14c). When factor *a* (degree of use of high-tech devices) is at a high level, DOC increases 28% (Fig. 14a); this produces a slight improvement (5%) in ROIIC (Fig. 14c).

The magnitude and direction of the factor effects on each performance measure are given in Table 5. The results indicate that border commanders and security planners should emphasize the mobility of security elements (especially patrols). FOC improves 38% when the use of motorized patrols is at a high level; this increases ROIIC about 13%. Increasing the mobility of patrols not only improves security along the border but also deters infiltrations.

The use of high-tech devices (factor *a*) increases DOC and ROIIC 28% and 5%, respectively. Note that factor *b* (use night-vision tools) also improves DOC by 10% and ROIIC by 3%. This clearly indicates that technology has a positive impact on border security. Thus, we recommend that border commanders use high-tech devices frequently and emphasize the maintenance of these devices. We also observe that factor *e* (duty time of patrols) has some positive effects, but these are marginal: 6% for DOC and 1% for ROIIC. The other factors (use of motorized patrols and stationary vs. mobility) have little effect on DOC.

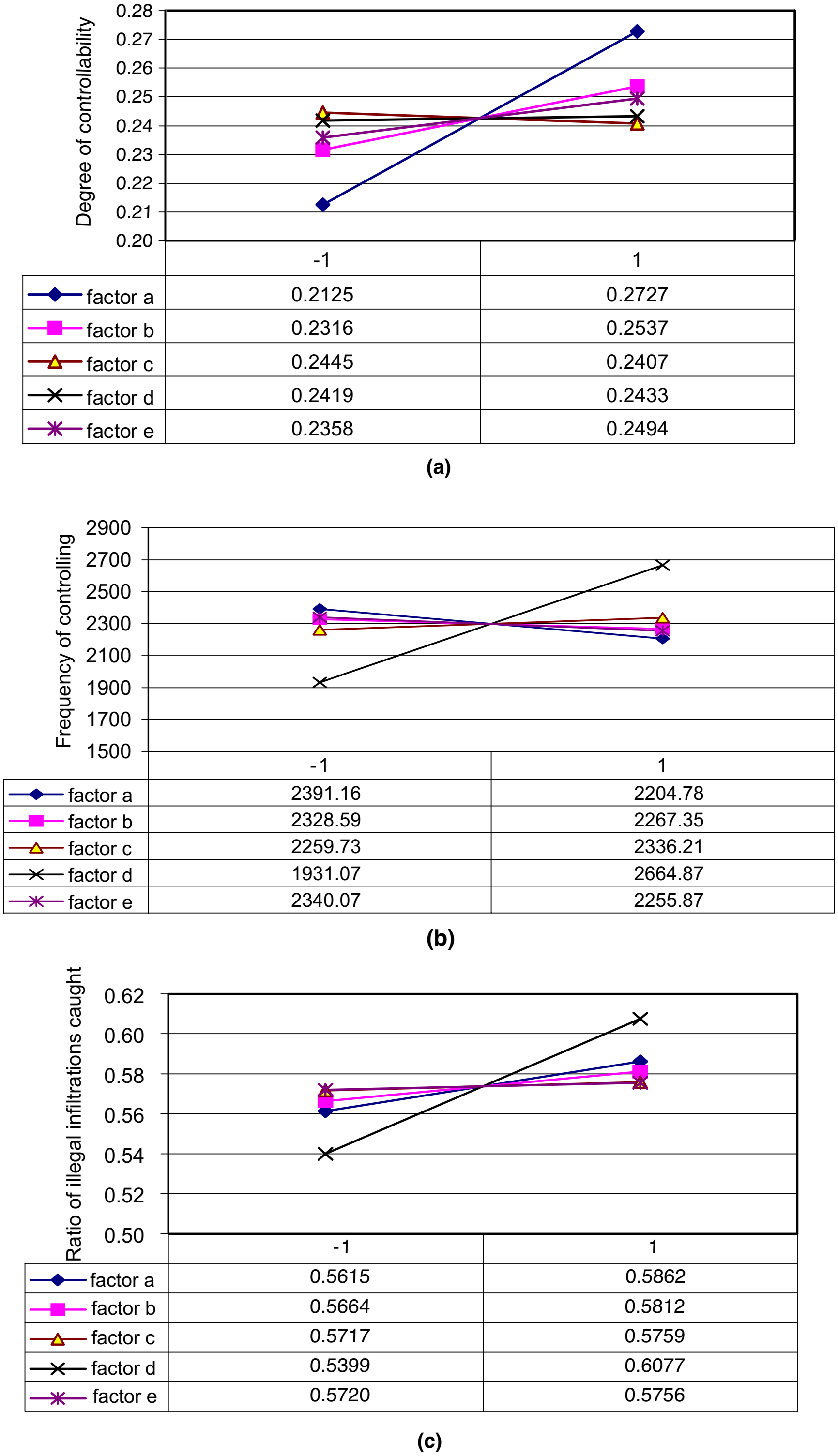
There are four significant interactions on ROIIC. These are between factors *a*–*d*, *b*–*d*, *e*–*d* and *a*–*b*–*d*–*e*. There is an interaction between factors *a* and *d* since the effect of factor *d* on ROIIC depends on the level chosen for factor *a*. When the use of high-tech devices is high, zones is monitored longer and this decreases the control of zones by patrols. Thus, the effect of factor *d* on ROIIC is less when factor *a* is at high value and the effect of factor *d* on ROIIC is greater when factor *a* is at its low value. Interactions *b*–*d* and *e*–*d* can be explained by the same reasoning.

There are two significant interactions on DOC. These are between factors *a*–*b* and *a*–*e*. These two interactions have the positive effect on DOC. The effect of factor *b* on DOC depends on the level chosen for factor *a*. When the use of high-tech devices is high, the zones will be under control longer and this increases the probability of taking the same zones under control by ambushes and patrols. Thus, the effect of factor *b* on DOC is less when factor *a* is at its high value and the effect of factor *b* on DOC is more when factor *a* is at its low value. The interaction *a*–*e* can be explained by the same reasoning. Finally, there are four significant interactions on FOC. These are between factors *a*–*c*, *a*–*b*, *b*–*c* and *b*–*e*. These interactions can be interpreted as in the case of ROIIC.

6. Alternative system designs

In this section, we propose and test new alternatives to improve system performance using ranking/selection and multi-criteria decision-making procedures. Since improvements in the border security system can be costly, we include the cost aspect in addition to the regular performance measures: DOC, FOC, and ROIIC. Specifically, we will attempt to answer the following research questions:

- If coordination is established between security elements, how much does it affect the performance measures?
- How much do additional high-tech devices affect the performance measures?



	-1	1
◆ factor a	0.2125	0.2727
■ factor b	0.2316	0.2537
△ factor c	0.2445	0.2407
× factor d	0.2419	0.2433
✳ factor e	0.2358	0.2494

(a)

	-1	1
◆ factor a	2391.16	2204.78
■ factor b	2328.59	2267.35
△ factor c	2259.73	2336.21
× factor d	1931.07	2664.87
✳ factor e	2340.07	2255.87

(b)

	-1	1
◆ factor a	0.5615	0.5862
■ factor b	0.5664	0.5812
△ factor c	0.5717	0.5759
× factor d	0.5399	0.6077
✳ factor e	0.5720	0.5756

(c)

Fig. 14. Main effect diagrams of factors for each performance measure.

- Which improvement is the best considering different criteria?
- What is the effect of high mobility of patrols on system performance?

Table 5
Effects of factors on performance measures

Performance measures	Significant factors	Improvement (%)
Degree of controllability	*a* (the degree of use of high-tech devices)	28
	b (the degree of use of night-vision tools)	10
	c (determination of stationary or mobile characteristics of duty)	−1
	d (the degree of use of motorized patrols)	1
	e (duty time of patrols)	6
Frequency of controlling	*a* (the degree of use of high-tech devices)	−8
	b (the degree of use of night-vision tools)	−3
	c (determination of stationary or mobile characteristics of duty)	4
	d (the degree of use of motorized patrols)	38
	e (duty time of patrols)	−4
Ratio of illegal infiltrations caught	*a* (the degree of use of high-tech devices)	5
	b (the degree of use of night-vision tools)	3
	c (determination of stationary or mobile characteristics of duty)	1
	d (the degree of use of motorized patrols)	13
	e (duty time of patrols)	1

The alternative systems under consideration:

1. *Benchmark system:* The existing system.
2. *A border security system in which all patrols are motorized:* In the previous section, we observed that ROIIC improves as FOC increases. We also note that FOC increases with an increase in motorized patrols.
3. *A system with one additional askarad and one additional thermal camera:* These high-tech devices make it possible to control a wider section of border.
4. *A system with coordinated security elements:* In the present system, overlaps occur when security elements monitor the same zones. We prevent these overlaps by improving coordination between security elements.
5. *A system with coordinated elements:* This is a combination of the second and the fourth alternatives.
6. *A system with coordination and one additional askarad and thermal camera.*

6.1. Evaluation of alternatives by using ranking and selection procedures

Since there are six alternatives, we have 15 pairwise comparisons of the alternatives. We apply the ranking and the Rinott selection procedure. We first determine the required number of replications for each alternative and then select the best system. The results of Rinott's procedure are summarized in Table 6.

In general, the second and the fifth alternatives are better than the others for ROIIC and FOC. A system where all patrols are motorized and coordination is established between security elements is the most effective. On the other hand, for DOC Alternative 6 is best and Alternative 3 is second. A coordinated system with extra high-tech devices provides DOC at its highest level. Even though the relative rankings of alternatives change for different performance measure, all the proposed alternatives provide better border security than the existing system (Alternative 1). This indicates that all alternatives, which improve system efficiency, should be considered by security planners.

Table 6
Results of all pair-wise comparisons and Rinott's procedure

Procedures	Performance measures	Ranking					
		1	2	3	4	5	6
All pair-wise comparisons	DOC	Alt 6	Alt 3	Alt 5	Alt 1, 2, 4		
	FOC	Alt 2, 5	Alt 1, 4	Alt 3, 6			
	ROIIC	Alt 2, 5	Alt 6	Alt 3	Alt 1, 4		
Rinott's procedure	DOC	Alt 6	Alt 3	Alt 5	Alt 4	Alt 2	Alt 1
	FOC	Alt 2	Alt 5	Alt 1	Alt 4	Alt 3	Alt 6
	ROIIC	Alt 5	Alt 2	Alt 6	Alt 3	Alt 4	Alt 1

Similarly, commanders and security planners should make coordination between security elements; as we utilize more high-tech devices, coordination becomes more important for both DOC and ROIIC.

6.2. Implementation of the geometric mean technique for multi-criteria decision-making

Since the ranking of alternatives differs for each performance measure, in this section we consider all these criteria and the cost to compare the alternatives. In this multi-criteria decision-making environment, we implement the geometric mean technique. First, we construct our hierarchy tree as seen in Fig. 15.

In the second step, we compare the alternatives for each criterion. Specifically, we construct matrices based on the simulation results (Table 7). In the third step, we form a utility matrix by taking the geometric means of each row of matrices. Meanwhile, we construct a weight matrix by taking the geometric means of each row of pair-wise comparison matrices of criteria and normalizing the results. In Tables 8 and 9, the utility matrix and weight matrix (before and after normalization) are presented.

As the last step, we take the weight powers of each alternative row in the utility matrix and calculate values for each alternative. Then we normalize the values and obtain the final ranking of alternatives as presented in Table 10.

As seen in Table 10, Alternative 5 is the best system. It shows us the importance of motorized type of patrols and coordination between security elements in the system. The fact Alternative 4 is ranked third also underscores the importance of coordination. On the other hand, alternatives that need additional high-tech devices (Alternatives 6 and 3) are not chosen because of their high costs. It is clear that if new high-tech devices are added to the sys-

Table 7
Results of each alternative for each criterion

Criteria Alternatives	Ratio of illegal infiltrations caught	Degree of controllability	Frequency of controlling	Cost[a]
1	0.53	0.21	2046.64	0.04
2	0.63	0.22	3153.56	0.055
3	0.56	0.28	1877.88	0.075
4	0.53	0.22	2045.77	0.04
5	0.63	0.22	3146.43	0.055
6	0.57	0.29	1865.71	0.075

[a] Costs of alternatives are calculated as million dollars for 1-year time period (note that costs are based on one thermal camera (0.13 million dollars), price of one askarad (0.24 million dollars) and amount of fuel needed for motorized patrols).

Table 8
Utility matrix

Alternatives	Ratio of illegal infiltrations caught	Degree of controllability	Frequency of controlling	Cost
1	0.42	0.53	0.70	2.36
2	2.50	0.57	2.80	1.07
3	0.76	2.52	0.50	0.39
4	0.48	0.62	0.70	2.37
5	2.60	0.67	2.79	1.07
6	0.97	3.03	0.50	0.39

Table 9
Weight matrix

	Ratio of illegal infiltrations caught	Degree of controllability	Frequency of controlling	Cost
Weights before normalization	1.62	0.62	0.74	1.31
Weights after normalization	0.38	0.15	0.17	0.30

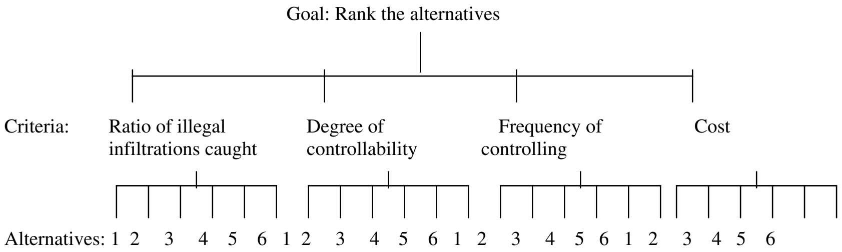

Goal: Rank the alternatives
Criteria:
Ratio of illegal infiltrations caught
Degree of controllability
Frequency of controlling
Cost
Alternatives: 1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4 5 6

Fig. 15. Hierarchy tree of alternatives and criteria.

Table 10
Ranking of alternatives

Ranking	Alternatives	Values
1	Alternative 5	0.258841
2	Alternative 2	0.249674
3	Alternative 4	0.13541
4	Alternative 1	0.126509
5	Alternative 6	0.121378
6	Alternative 3	0.108188

tem, coordination must be established between security elements.

7. Concluding remarks and future research topics

In this paper, we study the Turkish border security system via simulation to identify possible ways of increasing border control and security along the land borders. Specifically, we try to: (1) understand the behavior of the system, (2) observe the relationships between security elements and performance measures and the relationship between different performance measures, (3) find out the effect of each security element on the performance measures, (4) analyze factors that the effect the performance measures, (5) investigate system responses, when changes are made in the system or new resources are added to the system, and (6) evaluate different alternatives to improve the performance measures, using ranking-selection and multi-criteria decision-making procedures.

We analyze the outputs by using three performance measures: (1) ratio of illegal infiltrations caught, (2) degree of controllability, and (3) frequency of controlling. The main conclusions from our study are as follows:

1. DOC, FOC and ROIIC are not uniform along the border. This is due to the different use of security elements in different zones and to the varying mobility characteristics of security elements. This suggests that we can adjust DOC by the flexible use of security elements. We can also higher levels of control on the critical zones of the border. Ambushes are the most appropriate means for high-level control of critical zones. Therefore, the training of ambushes is important.
2. Patrols are the main security element in FOC. Therefore, their mobility should be increased by increasing the number of motorized patrols.
3. It is difficult to catch enemy special forces and terrorists. To improve the probability of capturing these infiltrators, these should be emphasis on building physical obstacles along the borders; these obstacles usually increase infiltration time.
4. There is a direct relation between DOC and ROIIC. But, ROIIC does not improve proportionally to DOC; it does not necessarily prevent infiltrations on the border by increasing the number of high-tech devices. We know that more high-tech devices increase DOC. Therefore, we need to identify the appropriate number of high-tech devices for each border troop and ambushes must be used for policing the zones that cannot be monitored by high-tech devices.
5. There is also a direct relation between FOC and ROIIC, but ROIIC does not improve proportional to FOC. Therefore, border security planners must identify the appropriate capacity of patrol and precautions such as increasing the mobility of patrols and building physical obstacles must be taken to maximize ROIIC. Such precautions also prevent infiltrations along the border.
6. The presence of each security element (patrols, ambushes, thermal cameras, and askarad) has a significant effect on each performance measure when compared with its absence from the system.
7. All factors have significant effects on each of the performance measures (Table 11). On the basis of these results, border troops have to use high-tech devices more frequently, increase

Table 11
Factors affecting the performance measures

Performance measures	Significant factors	Improvement[a]
Ratio of illegal infiltrations caught	*a*, *b*, *c*, *d*, *e*	5%, 3%, 1%, 13%, 1%
Degree of controllability	*a*, *b*, *c*, *d*, *e*	28%, 10%, −1%, 1%, 6%
Frequency of controlling	*a*, *b*, *c*, *d*, *e*	−8%, −3%, 4%, 38%, −4%

[a] Improvement indicates the change in performance measure when we change the factor from its low level to high level: (*a*) the degree of use of high-tech devices; (*b*) the degree of use of night-vision tools; (*c*) determination of stationary or mobile characteristics of duty; (*d*) the degree of use of motorized patrols; (*e*) duty time of patrols.

Table 12
Alternative description and ranking of alternatives

Ranking	Alternative	Alternative description	Value
1	Alternative 5	A system where coordination is established and all patrols are motorized	0.258
2	Alternative 2	A system where all patrols are motorized	0.249
3	Alternative 4	A system where coordination is established between security elements	0.136
4	Alternative 1	Benchmark system	0.126
5	Alternative 6	A system where coordination is established and one more askarad and one more thermal camera added	0.122
6	Alternative 3	A system with one more askarad and one more thermal camera	0.109

the duty time of patrols, and increase mobility of all security elements to increase the security of land borders.

8. Another way of increasing border security is to establish coordination between security elements. Coordination increases degree of controllability by preventing the monitoring of the same zones by two or more security elements at the same time.
9. When all criteria are considered. Alternative 5 is best set (Table 12).
10. Before making investments or changes in practice to increase border security, we should analyze such changes in terms of performance measures and costs for each border troop. Thus, the requirements of each border troop are evaluated more accurately leading to more useful investments.

Finally, the following topics can be investigated in future studies. First, border security should be analyzed in a situation of strained relations with a neighboring country (not war) by considering the troops located very near to borders. Second, we analyzed border security system at night; it could also be analyzed in daylight. Third, one of the main tasks of border troops is the collection of intelligence by closely watching the terrain of neighboring country; research can be conducted on this task of border troops. Finally the logistical activities and communication systems of border troops can be analyzed.

References

Balcı, O., 1998. Verification, validation, and accreditation. In: Proceedings of the 1998 Winter Simulation Conference, pp. 41–48.

Banks, J., Carson II, J.S., Nelson, B.L., 1996. Discrete Event System Simulation. Prentice-Hall, Inc., New Jersey.

Department of Army Pamphlet 5-11, 1999. Verification, validation, and accreditation of army models and simulations. Headquarters Department of the Army, Washington, DC.

Genel Kurmay Başkanlığı Kara Kuvvetleri Komutanlığı, 1999. Hudut Hizmetleri Yönergesi (KKY 118-1), Ankara (Border Services Instructions).

Law, A.M., Kelton, W.D., 1991. Simulation Modeling and Analysis, second ed. McGraw-Hill Book Company.

Montgomery, D.C., 1992. Design and Analysis of Experiments, fourth ed. John Wiley, New York.

Krouse, William, J., Perl, Raphael F., 2001. CRS (Congressional Research Service) report (June 18, 2001).

Gokhan Çelik is a captain in the Turkish Army. He received a B.S. in System Engineering from the Turkish Army Academy, and an M.S. in Industrial Engineering from Bilkent University. He has experience in infantry team and border company leadership. He now works as company commander in the Infantry School, Istanbul. He conducts research in military simulation.

Ihsan Sabuncuoğlu is Professor and Chairman of Industrial Engineering Department at Bilkent University. He received B.S. and M.S. degrees in Industrial Engineering from Middle East Technical University and a Ph.D. degree in Industrial Engineering from the Wichita State University. Prof. Sabuncuoğlu teaches and conducts research in the areas of simulation and scheduling for military and manufacturing applications. He has published papers in IIE Transactions, Decision Sciences, Interfaces, Simulation, International Journal of Production Research, International Journal of Flexible Manufacturing Systems, International Journal of Computer Integrated Manufacturing, Computers and Operations Research, European Journal of Operational Research, International Journal of Production Economics, Production Planning, Control, Journal of Operational Research Society, Journal of Intelligent Manufacturing, Computers and Industrial Engineering. He is on the Editorial Board of International Journal of Operations and Quantitative Management, Journal of Operations Management, International Journal of Computer Integrated Manufacturing, and he is associate editor of Transactions on Operational Research. He is an associate member of the Institute of Industrial Engineering and the Institute for Operations Research and the Management Science.