A Model the Process of Overcoming Multizone Protection Stationary Object by an Intruder

G. KONOPACKI
gkonopacki@wat.edu.pl

Institute of Computer and Information Systems
Faculty of Cybernetics, Military University of Technology
Kaliskiego Str. 2, 00-908 Warsaw, Poland

The article examines a model of the process to overcome multi-zone protection for a stationary object (buildings, together with the adjacent area) by a determined passive intruder, which means the intruder is not affecting the active protection system (for both equipment and people) and not intending to stop the action before achieving a protected object. As a tool for describing the actions the intruder was proposed a process of Markov class CD, whose character is presented in the form of analytical equations Chapman – Kolmogorov. The article presents a solution to this system and discusses its practical usefulness.

Keywords: protection of objects, modeling, the process of Markov.

1. Introduction

The need to ensure the safety of various objects, especially the importance of military, political, financial, is becoming more common and already existing results from evolution and the occurrence of new threats due to the brutalization of the methods attackers use and an increase the value of the damage. Thus, it became a standard to equip objects in a more or less complex system of protection, so called. protection systems of objects. Usually, they combine two elements working together: the technical system and physical protection, in which the crucial link is the person.

Nowadays, the rapid development of the technical system is subject to a particular security system, which does not detract from a person of decisive importance in providing effective protection, as he/she makes final decisions based on the reaction of the technical system. Nevertheless, the electronics and computer science play a significant role in the protection systems of objects. The observation area is carried out using CCTV cameras and object access control is controlled by computer systems, because they are actually only capable of uniformly continuous and reliable operation in various climatic conditions at different times of the day and year. With well-developed multimedia technology, it is possible to visualize data and events in the security system and protected objects.

An undeniable advantage of such systems is that they can also be equipped with elements of artificial intelligence, used to analyze data on the state of the protected object, and, most importantly, to detect, locate, and often neutralize the actions of an intruder, that is violating a protection zone of the protected object. The requirements of modern computer security systems are extremely high. Their fulfilment can guarantee only systems having the following properties:

- high technical reliability
- reaction to the materialization of credibility (the implementation) the risks, in particular the reliability of detection and location of the intruder, a threat to the protected object
- a minimum level of occurrence of states of a false alarm and false peace
- ease of signals verification generated by the system
- ease of use
- resistance to sabotage and being destroyed.

Advanced computer security systems offer the possibility of developing proposals for decision in the event of specific threats. It is very important that the realization of risks (particularly for high intensity) may cause different reactions of the person responsible for taking decisions and actions in the event of abnormal signalling facility. Thus, the system offers staff assistance in the form of "hints" of activities, forcing their specific sequence, documenting decisions and actions, and recalls the actions necessary, but have not yet taken.

In cases where the implementation of a local hazard is mild, this aspect of the system is not so very important. While the realization of the risks over a large area, with their high intensity, requires rapid decision making during the coordination of activities aimed at neutralizing the effects of the implementation and/or managing the rescue operation. In such situation, large amounts of data come to management positions that require their rapid interpretation and treatment through decisions.

An equally important factor as the efficiency and effectiveness of technical security is the reaction of appropriate services generated by the alarm system. Therefore, the security system equipped with a reliable and efficient installation of signalling and notification, and a competent person to respond to the occurrence of hazards provide proper security of the protected object. Construction of computer systems for the protection of buildings must take into account the principles, which show that this system must [Niezabitowska 2010]:

- be closely tailored to the specifics of the protected object and its protected value. This usually determines that equal security systems is not created for two different protected objects, even if characterized by very similar properties, since the same details to facilitate security systems are able to be overcome relatively quickly which, in turn, would result in futility to continue their use
- include an appropriate set of technical devices (sensors, cameras, lights, analyzers), to ensure providers identify when the materialization of risks
- be flexible, that is designed for easy expansion and changes resulting from changes in the protected object and technical development of protective devices, and from changes in intruder techniques and activities used by the tools used for active conservation measures applied against the object
- provide certainty that the predetermined probability of materialization are detected signs of danger (e.g. intruder detection) in such intensity that they can give rise to legitimate concern about the impact on the protected object. Thus, it is clear that if the status of the security object can be expected to reduce, it must also change the security system itself.

There is another expectation directed at the security systems associated with their ”intelligence”. Modern computer security systems must provide protection to develop proposals for decision support for identification of the realization of a particular type of threat. Thus, understood as ”intelligence” artificial intelligence would be used primarily to recognize the state of a ”false alarm” and ”false peace”, the identification of individuals according to their somatic characteristics such as fingerprints, bones, skulls, DNA and other individuating characteristics between individuals and the identification of adverse, or other desired states and events. The use of artificial intelligence, because of its cost, should occur in such cases where the intensity necessary to observe the events is so high that physical protection (people) cannot guarantee a sufficiently high probability of identifying emerging signs of abnormalities or risk realization

Reliability of security systems are strongly associated with the immune system on the prevalence of ”false alarms” and ”false peace”. A false alarm occurs when the protected object and system security measures are not subject to the security system intruder alarm signals. This condition can be caused by defective functioning of technical elements of the system or − at the technically efficient system − occurrence of adverse random events (e.g. storm, accidental activation barrier). False peace − a phenomenon far more dangerous than a false alarm − occurs when there is actual penetration of a protected object or its environment by an intruder, while the security system for various reasons does not respond.

The principal tasks of the vast majority of security systems, objects are oriented to prevent an attacker (sniffer) on the area immediately adjacent to the protected object, and for his intrusion into the area − its location as quickly as possible, secretive surveillance and eventual neutralization.

2. A Model

2.1. The Assumptions

A formal proposal to approach the problem of overcoming the multi-zone intruder protection area of the object will be presented next. This problem will be dealt with using the following assumptions:

1. The area protected facility (facility protection area) creates a number of concentrically located relative to the object

of the protection zones. Protection zones are disjoint and adjacent closed areas, armed with various physical and technical measures, which is another inconvenience for an intruder on the way to a protected object. Examples of protection zones for the object may be [Nowak 2007]:

- *the first zone of protection* − building a fence that can be equipped with sensors that detect attempts by his clambered sufficient safety, or performance of the grid intersection of sap
- *the second zone of protection* − the area of land between the fence and building wall
- *the third zone of protection* − the technical elements of signaling the presence of an intruder at the wall of an object or attempts of overcoming by him external insurances of security of objects
- *the fourth protection zone* − inside the object.

2. Overcoming the security zones by the intruder begins to break the protective barrier of the outer zone of the protected area, then move to the next zone, located directly to the property protected. The way to overcome the protected area depends on the skills and preparation of the intruder and the organization of the protection zones, which means that the following scenarios are possible:
   - intruder leaves the protected area at the break of the outer barrier (first) zone of protection (an accidental intruder or hearing the security system of the protected object)
   - intruder, not paying attention to whether it was detected, possibly overcomes the simplest way (in the shortest time) the protection zone, until they reach the protected object
   - intruder defeats the zone of delay resulting from the search path of transition to the next zone and the possible withdrawal of the zone immediately preceding that in which it is located, to leave the protected area without reaching the protected object
   - intruder moves as before with the fact that he/she can ”jump” (e.g. with the use of means of transport), individually or collectively forward some or all zones, but does not intend to leave the protected area before reaching the protected object (intruder determined).

The intruder waiting in the protection zone can last for a stretch of time, which is the realization of a random variable with distribution depending on the preparation of the intruder, his/her strategy for overcoming the protected area and protection zones to organize, while the transition between zones of protection occurs without loss of time (at $t = 0$).

Due to the practical aspects, this will be processed on a model, which takes into account the conservation area to overcome the object by a determined intruder, i.e., one that is determined to achieve the protected object.

2.2. The Formulation of the Problem

It is assumed that the facility protection area consists of a finite number of $n \in N$ protection zones. Let $S_i, (i = 0,1,2,...,n)$ mean protection zone number i, where S_0 means outer protection zone, while S_n denotes the last zone, near the protected object.

Based on the verbal description of the process of overcoming the facility protection area by the intruder suggests the following formal model based on stochastic process of the CD class (continuous parameter, discrete states) in which the parameter will be the time for a set of states − a collection of protection zones. A graphic illustration of this process is illustrated in Figure 1, which adopted the following designations:

- $\lambda_{i,j}(t)$ – intensity of the transition intruder from the protection zone S_i to zone S_j $(i < j)$
- $\eta_i(t)$ – intensity of the immediate transition of the intruder from the protection zone S_i to zone S_n
- $\mu_{j,i}(t)$ – intensity gradually withdrawing intruder from the protection zone S_j to zone S_i $(i < j$ and $i \neq j)$
- $\xi_i(t)$ – intensity of the immediate withdrawal of the intruder from protection zone S_i to zone S_0 $(i \neq n$ and $i \neq 0)$
- $\mu_{i,i}(t)$ – intensity of an intruder waiting in zone S_i, where:

$$\begin{cases} \mu_{i,i}(t)=1-\left(\eta_i(t)+\xi_i(t)+\sum\limits_{k=i+1}^{n}\lambda_{i,k}(t)+\right. \\ \left.+\sum\limits_{k=0}^{i-1}\mu_{i,k}(t)\right), \qquad i=0,1,\ldots,n\text{-}1, \\ \mu_{n,n}(t)=0. \end{cases} \tag{1}$$

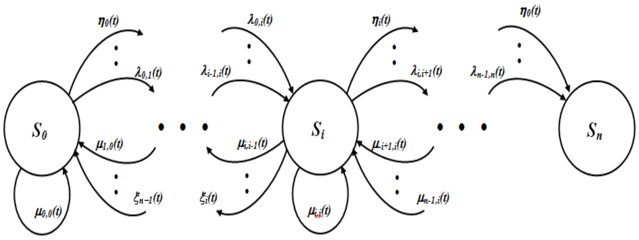

Fig. 1. Graphical presentation of the process of overcoming the multi-zone protection area for the object by an intruder

Examining the process of overcoming the protection area of the object can be treated as a homogeneous Markov process with continuous and discrete parameters in the states. Parameter in this process is time, while the states − as had already been said − the zone of protection. Thus, this process can be presented in the following system of Chapman − Kolmogorov equations:

$$\begin{cases} p_i'(t)=-\left(\sum\limits_{k=0}^{i-1}\mu_{i,kt}(t)+\sum\limits_{k=i+1}^{n}\lambda_{i,k}(t)+\eta_i(t)+\xi_i(t)\right)\cdot \\ \cdot\, p_i(t)+\sum\limits_{k=0}^{i-1}\lambda_{k,i}(t)\cdot p_k(t)+ \\ +\sum\limits_{k=i+1}^{n-1}\mu_{k,i}(t)\cdot p_k(t), \quad i=0,1,\ldots,n-1, \\ p_n'(t)=\sum\limits_{k=0}^{n-1}\left(\lambda_{k,n}(t)+\eta_k(t)\right)\cdot p_k(t), \\ i=n. \end{cases} \tag{2}$$

Determination of probabilities $p_n(t), p_{n-1}(t),\ldots, p_0(t)$, finding the intruder in zone $S_i, (i=0,1,2,\ldots,n)$ requires the solution of this system of equations with the initial conditions defining the probability of finding the intruder in any protection zone. In the general case, the solution of the Chapman − Kolmogorov equations can be very difficult in an analytical way. In such cases, approximate methods are used, using the properties of the process.

In practice, simpler options are used to overcome the facility security area issue by the intruder. This simplified model will be presented below.

2.3. Simplified Model

Model simplified treated further illustrates the often encountered case of the intruder only nudge forward, whose aim is to achieve as soon as possible the protected object. Thus, this process will be only characterized with intensities of transitions between adjacent states, showing the successive zones of protection, the protected object coming closer and the intensities go from any state to the state of the imaging area directly adjacent to the protected object. In the present model of the process, it is assumed that the intensity of the transitions between states are constant (not time-dependent), and that

:

$$\begin{aligned} &\eta_i>0, \quad i=0,1,\ldots,n-1, \\ &\lambda_{i,i+1}>0, \ i=0,1,\ldots,n-1, \\ &\mu_{i+1,i}=0, \ i=n-2,\ldots,1,0, \\ &\varepsilon_i=0, \quad i=n-1,\ldots,1,0. \end{aligned} \tag{3}$$

Graphical interpretation of the simplified model to overcome the multi-zone protection area by the intruder object is shown in Figure 2.

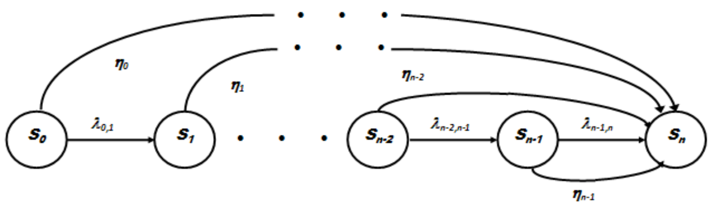

Fig. 2. Graphical presentation of a simplified model of the process of overcoming the multi-zone protection area for the object by an intruder

The stochastic process under consideration can be described by the following system of equations of Chapman − Kolmogorov [Gichman & Skorochod 1968, Norris 1977, Stefanko 2000]:

$$\begin{cases} p_0'(t)=-(\eta_n+\lambda_{0,1})\cdot p_0(t), \\ \quad i=0, \\ p_i'(t)=-(\eta_i+\lambda_{i,i+1})\cdot p_i(t)+\lambda_{i-1,i}\cdot p_{i-1}(t), \\ \quad i=1,2,\ldots,n\text{-}1, \\ p_n'(t)=\sum\limits_{k=0}^{n-1}(\lambda_{k,n}+\eta_k)\cdot p_k(t), \\ \quad i=n. \end{cases} \tag{4}$$

It is assumed that

$$\alpha_i=\eta_i+\lambda_{i,i+1}, \qquad i=0,1,2,\ldots,n-1. \tag{5}$$

With the numerical values set the intensity of transitions between zones of protection can be met with two cases:

- values a_i are different
- not all values a_i are different.

Next, consider the first variant. In the case of the second variant, shown on a method of solving the equations (4) it will be possible to use. At $t_0 = 0$ the intruder can be located in any zone of protection S_i, $(i = 0,1,2,...,n)$ with a probability p_i, $(i = 0,1,2,...,n)$. Therefore, the system of differential equations (4) is solved with the following initial conditions (Cauchy):

$$p_i(t_0) = p_i, \qquad i = 0,1,2,...,n-1, \qquad \sum_{i=0}^{n} p_i = 1. \tag{6}$$

Applying the Laplace transformation to equations (4) is obtained [Stewart 1994]:

$$p_i(s) = \frac{1}{s+\alpha_i}\left(p_i + \sum_{k=0}^{i-1} p_k \prod_{j=k}^{i-1} \frac{\lambda_{j,j+1}}{s+\alpha_j} \right), \tag{7}$$

$i = 0,1,2,...,n-1$.

Applying the appropriate transformations to the system of equations (7) is replaced by the following equations:

$$p_i(s) = \sum_{j=0}^{i} A_{ij} \frac{1}{s+\alpha_j}, i = 0,1,2,...,n-1, \tag{8}$$

where:

$$A_{ij} = \sum_{k=0}^{j} p_k \frac{\prod_{\substack{m=k \\ m\neq i}}^{i} \lambda_{m,m+1}}{\prod_{\substack{l=k \\ l\neq j}}^{i} (\alpha_l - \alpha_j)}. \tag{9}$$

Applying inverse Laplace transformation to equations (8) the following is obtained:

$$p_i(t) = \sum_{j=0}^{i} A_{ij} \cdot e^{-\alpha_j t}, \ i = 0,1,2,...,n-1. \tag{10}$$

Probability $P(t)$ that the intruder will not get in the zone closest to the protected object is equal to:

$$P(t) = \sum_{i=0}^{n-1} p_i(t). \tag{11}$$

Given the expressions (9) and (10) in (11) we finally obtain:

$$P(t) = \sum_{i=0}^{n-1} B_{in} \cdot e^{-\alpha_j t}, \tag{12}$$

where:

$$B_{in} = \left[1 + \sum_{\substack{k=i \\ i\neq n-1}}^{n-2} \prod_{j=1}^{k} \frac{\lambda_{j,j+1}}{\alpha_{j+1} - \alpha_i} \right] \cdot \left[p_i + \sum_{\substack{k=1 \\ i\neq 0}}^{i} p_{i-k} \prod_{j=i-1}^{i-k} \frac{\lambda_{j,j+1}}{\alpha_j - \alpha_i} \right]. \tag{13}$$

From the expressions (12) the density distribution function can be calculated of finding the intruder in any of the protection zones except near the protected object, which is expressed by the following formula:

$$f(t) = \frac{dP(t)}{dt} = \sum_{i-0}^{n-1} \alpha_i \cdot B_{in} \cdot e^{-\alpha_i t}. \tag{14}$$

The mean value of time finding the intruder in any of the protection zones except near the protected object will be equal:

$$ET = \int_0^\infty P(t)dt = \sum_{i-0}^{n-1} \frac{B_{in}}{\alpha_i}, \tag{15}$$

and the variance of the time

$$\sigma_t^2 = 2\sum_{i-0}^{n-1} \frac{B_{in}}{\alpha_i^2} - ET^2. \tag{16}$$

3. Conclusion

The practical use of the presented model must be preceded by an estimate of the size occurring in the output, which are the intensity of the protection zones, were created to overcome the storage facility by an intruder, the group. Of course they will depend on the preparation and determination of an intruder on the one hand and the degree of difficulty of overcoming the zone, which in turn depends on its previous facilities and appropriate security measures. Model consideration involves overcoming zones by a determined intruder, but passive, i.e. not affecting destructive to the security measures installed in the zone, and thus not reducing its protective properties. Such situations occur most frequently, and all kinds of intruder impacts on the of security measures in the zone are random.

Despite the high level of generality considered, the model can be used in designing security systems for storage facilities for even approximate estimates of the expected time ET to find an intruder outside the immediate neighborhood of the protected storage object, i.e. outside S_n, because it is actually based on the evaluation of the effectiveness of the security system expressed in the following, applied in practice, the relation:

$$ET > T_a + T_m + T_i, \quad (17)$$

where:

- ET – mean time to overcome the protection zones
- T_α – reaction time of the system (alarm call)
- T_m – time of signal arrival to the monitoring centre
- T_i – time necessary for effective intervention.

Bibliography

[1] I.I. Gichman, A.W. Skorochod, *Wstęp do teorii procesów stochastycznych*, PWN, Warszawa, 1968.

[2] W. Feler, *Wstęp do rachunku prawdo-podobieństwa*, PWN, Warszawa, 1996.

[3] O. Haggstrom, *Finite markov chains and algorithmic applications*, Chalmers University of Technology, 2001.

[4] G. Konopacki, K. Worwa, „Problem eliminowania fałszywych alarmów w komputerowych systemach ochrony peryferyjnej", *Biuletyn Instytutu Systemów Informatycznych*, Nr 5, 37–46 (2010).

[5] G.F. Lawler, *Introduction to Stochastic Processes*, Chapman & Hall / CRC, 1995.

[6] M. Mitzenmacher, E. Upfal, *Metody probabilistyczne i obliczenia*, WNT, Warszawa, 2009.

[7] E. Niezabitowska (red.), *Budynek inteligentny*, Politechnika Śląska, Gliwice, 2010.

[8] M. Nowak, „Strefy ochrony posesji", www.budujemydom.pl, (2007).

[9] J.R. Norris, *Markov Chains* (Cambridge Series in Statistical and Probabilistic Mathematics), University of Cambridge, United Kingdom, 1997.

[10] A. Papoulis, *Prawdopodobieństwo, zmienne losowe i procesy stochastyczne*, WNT, Warszawa, 1972.

[11] K. Sobczyk, *Stochastyczne równania różniczkowe*, WNT, Warszawa, 1996.

[12] O. Stenflo, "Ergodic theorems for Markov chains represented by iterated function systems", in: *Bulletin Polish Academy of Sciences*, 2000.

[13] W.J. Stewart, *Introduction to the Numerical analysis of Markov Chains*, Princeton, 1994.

Model procesu pokonywania wielostrefowej ochrony obiektu stacjonarnego przez intruza

G. KONOPACKI

W artykule rozpatruje się model procesu pokonywania wielostrefowej ochrony obiektu stacjonarnego (zabudowania wraz z przyległym terenem) przez pasywnego intruza zdeterminowanego, co oznacza intruza nie oddziałującego czynnie na system ochrony (dotyczy zarówno urządzeń, jak i osób) oraz nie zamierzającego przerwać działań przed ociągnięciem celu, tj. obiektu chronionego. Jako narzędzie opisu procesu działań intruza został zaproponowany proces Markowa klasy CD, którego postać analityczną przedstawiono w postaci układu równań Chapmana – Kołmogorowa. W artykule przedstawiono rozwiązanie tego układu i omówiono jego przydatność praktyczną.

Słowa kluczowe: ochrona obiektów, modelowanie, proces Markowa.