A Neurograph as a Model to Support Control Over the Comprehensive Objects Safety for BIM Technologies

N V Korneev
Togliatti State University, 445667, Togliatti, 14, Belorusskaya St.
E-mail: niccyper@mail.ru

Abstract. Control over the comprehensive security of facilities requires scientific studying models and algorithms of control support, in particular, development of the methods and algorithms of forming component models of intruders for antiterrorist and anti-criminal protection of facilities and ensuring fire safety. Building a component-based automated control system to support comprehensive security of facilities with the aim of implementing particular BIM technologies improves security, as it allows studying in detail and assessing all the risks that may occur in the operating conditions. The article describes the developed algorithm of solving the problem of supporting control over comprehensive security of facilities by automating the process of creating component-based models of intruders in general terms for the cases where the finite number of states of the controlled facility at each moment is known or unknown. The algorithm is based on the model of the facility proposed by the author, which is similar to a graphic chart, where the vertices represent the neural network that models the corresponding state, the barriers of the facility in real time, and the edges — allowed paths of transition from one state to another, supplemented by tuples <x,d>, where x is the input vector, and d is the corresponding expected output vector of the network. An adaptive fuzzy neural network with a fuzzy-controller is used as the neural network. The resulting model is called a neurographic model of the facility, and the graphic chart in its base — a neurograph. The possibility is shown of amending the neurograph with any external effects described in a similar way by a relevant external neural network, on the example of neural network modeling two-dimensional flame propagation in an enclosed space with the use of the Kuramoto-Sivashinski equation. A generalized condition of transition from vertex to vertex for any arbitrarily complex neurograph has been formulated. The possibility of its implementation has been shown on an example of facility formalization with an intruder.

1. Introduction

In the new conditions of the social existence, and given the reduced funding, security of facilities should be addressed comprehensively and on a scientific basis, whereas particularly relevant become aspects of security associated with controlling the process of ensuring comprehensive safety itself. Control over the comprehensive security of objects requires scientific studying models and algorithms of control support. In particular, one of the areas for such research is development of the methods and algorithms of forming component models of intruders for antiterrorist and anti-criminal protection of facilities and simultaneous solving the tasks of ensuring fire safety. Peculiarities of the antiterrorist and anti-criminal protection of facilities and ensuring fire safety are to be considered as early as at the stage of designing capital construction facilities. Building a component-based automated control system to support comprehensive security of facilities with the aim of implementing particular BIM technologies
results, as practice shows [1], in improving the security, as it allows studying in detail and assessing all the risks that may occur in the operating conditions.

Scientific publications of both domestic and foreign scientists [2-8] show that in domestic and foreign literature and practice in this area, rigorous mathematical models with criteria of control support efficiency in the field of comprehensive security generally do not exist, and the existing comprehensive security systems do not solve the task of automated building a component-based model of a facility as part of comprehensive facility safety control support.

Let us develop an algorithm of solving the problem of supporting control over comprehensive security of facilities by automating the process of creating a component-based model of an intruder in general terms for the cases where the finite number of states of the controlled facility at each moment is known or unknown, and show the possibility of its implementation of the example of formalizing a facility with an intruder.

2. Results and Discussion

Paper [9] shown the possibility of building an algorithm for a facility security control support based on an information-based model of the facility. However, this model has the following disadvantages: it assesses protection of the facility, rather than its security, it is unable to simulate when the finite number of states of the controlled facility at each moment is unknown, it cannot classify intruders into types based on their knowledge and experience of overcoming the engineering and technical means of protection at the facility, it cannot consider the time of evacuating people in an emergency, it cannot use modern tools, such as neural networks, and, therefore, cannot model a random intruder. All this puts limitations on the results obtained in [9] as to their practical use for building a component-based automated facility security protection control support system with the aim of implementing certain BIM technologies.

To build the above-mentioned algorithm, let us use the principles of dynamic programming. The task is finding for a given initial state such method of control that would implement the conditions under which the time of intruder detection, the time of alarm transmission, the time of tact team response $t^{n}_{DS(I_i)} + t^{n}_{P(I_i)}$ and the time of evacuation $t_{e}$ would be less than the time needed by the intruder to overcome the engineering means of facility $t_{ir}$ protection [10]:

$$t^{n}_{DS(I_i)} + t^{n}_{P(I_i)} + t_{e} > t_{ir}. \ (1)$$

Let us restrict ourselves initially to the case where the controlled facility object takes a finite number of states at moment. The graphic diagram of intruder's capabilities at the facility consists of vertices that represent the possible states of the system - premises at the facility, and edges that are valid paths of transition from one state to another. The edges of the graph will be loaded with digits that specify the timestamps when the intruder passes between them.

Fig. 1 shows an example of formalizing a facility with an intruder, which includes 4 barriers (B1-B4) and 6 vertices (N1-N6). In our example, an intruder can freely move and see between vertices N4 and N5, N4 and N6. The time $t_{ir}$ of moving between the vertices along the i-th edge will only depend on the speed of intruder's movement.

Barriers B1, B4, and B3 prevent movement between vertices N1 and N2, N3 and N4, and N2 and N5, respectively. The reason for the barrier is determined by the type of the barrier, the type of the intruder, the location of the barrier, etc. The total expense for overcoming any path between two vertices will be determined by the speed of the intruder's movement, and the cost of overcoming obstacles, as well as the time of evacuation $t_{e}$.

Thus, we will consider an intruder who tends to penetrate to his goal, breaking existing barriers at minimal costs (1). Then, based on the type of the intruder, it is possible to build a graph model for each of his goals. Building an algorithm for control support, in this case, consists in modeling the choice of
the optimal strategy by the intruder – the optimal trajectory of his movement in the facility graph to the
desired aim at minimum costs for overcoming the barriers. The graph model for a facility in Fig. 1 is
shown in Fig. 2. Bold arrows indicate the optimal path of the intruder obtained according to the condition
we need, and non-bold arrows indicate an alternative one.

![Figure 1. An example of formalization of a facility with an intruder.](image)

![Figure 2. The graph model for a facility.](image)

The aim of the intruder is vertex 5 (Fig. 2) – final state N6 (Fig. 1). The vertices of the graph characterize
the corresponding states: 1 – initial state, N1; 2 – barrier B1 (state N2); 3 – barrier B3 (state N5); 4 – barrier B4 (condition 4).
Barrier B2 is knowingly not considered, since overcoming it requires significant costs.

In the case where the finite number of states of the controlled facility at each moment of time is
unknown, it is advisable to use a more sophisticated model similar to the structure of model (Fig. 2),
where the vertices represent the neural network (NN) that models the corresponding state N, the barriers
of the facility in real time, and the edges – allowed paths of transition from one state to another,
supplemented by tuples <x,d>, where x is the input vector, and d is the corresponding expected output
vector of the network. The resulting model will be called a neurographic model of the facility, and the
graphic chart in its base – a neurograph.

Fig. 3 shows an example of such a model for the facility in Fig. 1. An adaptive fuzzy neural network
with a fuzzy-controller is used as the neural network (NN); it is in the core of a fuzzy network determined
by L. Wang and J. Mendel, where the basic algorithm of fuzzy identification is a hybrid algorithm of
the fuzzy network learning. Such a model may be supplemented by virtually any external influences
described similarly by the relevant external neural network (ENN). Returning to the example in Fig. 2
let us supplement it with neural network ENN1, which models two-dimensional flame propagation in an
enclosed space (Fig. 1), with the use of the Kuramoto-Sivashinski equation [11].

The external effects are accounted for in the NN by the feedback with tuples <x,d> from the ENN.
In this case, the NN uses exclusively recurrent neural networks; it is also possible in some cases to use
self-organized networks based on the competition or the correlation type. To harmonize the data in
tuples, ENN in NN may be used as both mathematical functions and logical operators, including the
rules of fuzzy implication.
Figure 3. A neurographic model of the facility: - neurograph edges; -- external effects.

For example, in case of a fire propagating from barrier B3 (Fig. 1), states N2 and N3 will differ not only by the speed of intruder movement, the costs of overcoming the barrier and the tome of people evacuation but also by the nature of flame propagation. If barrier B3 is covered with flame, ENN1 will generate tuple \( <x_{ENN1}(NN3), d_{ENN1}(NN3)> \) for NN3, where vector \( d_{ENN1}(NN3) \) will contain logical “0”, and define in the NN3 the inability of transition from state N2 to state N5 by feedback. The condition of transition to vertice 5 — state N6 will have the form:

\[
\begin{align*}
    d_{ENN1}(NN3) &= d(NN3) = x(NN3); \\
    x_{ENN1}(NN3) &= x(NN3),
\end{align*}
\]

with that, condition (1) should be satisfied for each i-th edge.

For barrier B4, the situation is reverse – vector \( d_{ENN1}(NN4) \) will contain logical “1” until the flame engulfs barrier W4, or the front of flame propagation does not reach barrier B2, blocking passage to barrier B4. This fact shows that for real-world modeling, one has to consider a barrier of type B2, even if overcoming it requires significant costs. In this case, the situation may be complicated by the peculiarities of flame propagation in the areas with disproportional length to width ratio, which is typical for facilities with the massive stay of people, such as long and narrow corridors. In this case, neurograph should introduce additional vertices simulating fire detectors that cover a knowingly determined area, similar to the set of detectors that are potentially able to detect an intruder. Usually, technical means of protection use two classes of detectors: active and passive. Active detectors are constantly “viewing” the specified area within the facility (e.g., cameras and motion detectors). Passive sensors require that the intruder takes some action to be detected. They react to changes in the environmental parameters (e.g., motion sensors, heat sensors, cards, keyboards, control panels).

If the intruder is within the coverage area of such a detector, he is most likely to be detected. The probability of detection depends on several factors: detector type, intruder type, detector state (position), environment parameters and state.

Since passive detectors require actions from the intruder, they can be presented in the neurograph in the form of additional loads on the ribs, or in the form of additional vertices. When the intruder tries to overcome the barrier with a passive detector or arrives at a vertex with an active detector, he may be detected.

Thus, the generalized condition for transition from vertex to vertex for any arbitrarily complex neurograph, given (1) will be:
\[
\begin{align*}
\left\{ t_{r_{DS}(I_j)}^m + t_{r_{IP}(I_j)}^m + t_e^r > t_{i_r}^m ; \\
d_{\text{ENN}_k}(NN_m) = d_{i(\text{in})}(NN_m) = x_{i(\text{out})}(NN_m); \\
x_{\text{ENN}_k}(NN_m) = x_{i(\text{in})}(NN_m),
\end{align*}
\]

where \( m = 2,3,\ldots(M-1) \) is designation of vertices of NN of the neurograph, except for the initial and the final vertices; \( k = 1,\ldots,K \) is the marking of vertices of the ENN neurograph associated with vertices \( m \) according to the neurograph-based model of the facility; \( i(\text{in}) \) \( i(\text{out}) \) are the incoming and outgoing edges of NN vertices of the neurograph, respectively; \( l = 3,4,\ldots,L \) is the marking of the neurograph vertices associated with vertices \( m \) according to neurograph-based model of the facility.

Fig. 3 does not show input tuples of the initial state, and the output tuples of the final one, as a result, it speaks of the fact that the finite number of states of the controlled facility at each moment is unknown; however, it is implied that they exist. With that, the neurograph models development of the situation in real time, which allows considering various scenarios of events development, performing the situational analysis, using a set of typical scenarios for forming the security profile of the facility, elaborating and assessing all the risks associated with comprehensive security of the facility that may arise in the operating conditions. Such formalization allows to algorithmically simulate behavior of the intruder, which facilitates creating an optimal security system with regard to the reaction model of the security services and other services at the facility.

The algorithm of facilities comprehensive security control support by automating the creation of a component-based model is shown in general terms in Fig. 4.

3. Conclusions

1. A neurograph-based model of the facility has been suggested, which is similar to a graphic chart, where the vertices represent the neural network that models the corresponding state, the barriers of the facility in real time, and the edges — allowed paths of transition from one state to another, supplemented by tuples \(<x,d>\), where \( x \) is the input vector, and \( d \) is the corresponding expected output vector of the network. An adaptive fuzzy neural network with a fuzzy-controller is used as the neural network.

2. The possibility is shown of amending the neurograph with any external effects described similar to p.1 by a relevant external neural network, on the example of neural network modeling two-dimensional flame propagation in an enclosed space with the use of the Kuramoto-Sivashinsky equation.

3. A generalized condition of transition from vertex to vertex for any arbitrarily complex neurograph has been formulated. The possibility of its implementation has been shown on an example of facility formalization with an intruder.

4. An algorithm of solving the problem of supporting control over comprehensive security of facilities by automating the process of creating component-based models of intruders in general terms for the cases where the finite number of states of the controlled facility at each moment is known or unknown has been developed. The algorithm is based on the neurograph-based model of the facility suggested by the author.

5. The results obtained in p. 1-4 allow to correctly assess the security status of specific facilities at each moment of time. Implementation of control support requires development of a component-based automated control system for supporting comprehensive security of facilities according to the proposed algorithm, which will allow elaborating and assessing all risks that may occur in the operating conditions.
Determining the category of the facility
Building a neurograph model of the object
Building paths in this neurograph model with regard to the intruder’s aims
Determination of the weights of edges, vertices, tuples \(<x, d>\)
Making changes to the neurograph
Adjusting the paths of the intruder
Calculating in modeling the sums of weights of intruder paths
Comparing the calculated sum of weights of intruder’s paths

1

Making a decision about efficiency of the created system
\(t_{t_{\text{DS}(L)}}^n + t_{t_{P(L)}}^n + t_e > t_e\)
Making changes to the composition of technical means of protection, barriers and the concept of facility protection
Building a component-based model of the intruder model in the form of a document

End

Figure 4. The Algorithm of facilities comprehensive security control support by automating the creation of a component-based model is shown in general terms.

References
[1] Biagini C., Ottobri P. Federated Parametric Models for Seismic Risk Analysis in Existing Buildings. Proceedings of the 18th International Conference on Geometry and Graphics. 2018. pp. 2163-2166.
[2] Ashu G., Paul S. A Template-Based Conceptual Modeling Infrastructure for Simulation of Physical Security Systems. Proceedings - Winter Simulation Conference. 1. 2005. pp. 873.
[3] Volkan U., Jeffrey S. Mental simulation for creating realistic behavior in physical security systems simulation. Proceedings - Winter Simulation Conference. 2008. pp. 879-885.
[4] Garcia M.L. Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann. 2008. p. 370.
[5] Fennelly L. Effective Physical Security. Butterworth-Heinemann. 2016. p. 458.
[6] Young C. The Science and Technology of Counterterrorism. Butterworth-Heinemann. 2014. p. 512.
[7] Thompson P., Marchant E. A computer model for the evacuation of large building populations.
Fire Safety Journal. 1995. V. 24. Issue 2. pp. 131-148.

[8] Owen M., Galea E.R., Lawrence P.J. The Exodus evacuation model applied to building evacuation scenarios. Journal of Fire Protection Engineering. 1996. V.8(2). pp. 65-84.

[9] Jeffrey S., Brett A., Sabina E., Mark K. Distributed real-time simulation for intruder detection system analysis. Proceedings - Winter Simulation Conference. 1999. pp.1168-1173.

[10] Korneev N. V., Goncharov V. A. Mathematical model support management of complex safety objects social sphere with mass stay of people. Natural and technical sciences. 2018. V. 4. pp. 277-281.

[11] Sivashinsky G. I. Instability, pattern formation and turbulence in flames. Ann.Rev. Fluid Mech. 1983. V. 15. pp. 179-199.