Method for detecting vulnerabilities of unmanned vehicle interfaces based on continuous values discretization

Dmitriy Moiseev[1] and Alexey Bryukhovetskiy[1]

[1] *Sevastopol state university, 33 Universitetskaya str., Sevastopol, 299053, Russia*

Abstract

An approach related to the development of methods for ensuring the safety of unmanned vehicles in the smart city information infrastructure is proposed. The method is based on the continuous values discretization of the state vector's features of UMV resources, which include: communication channel, processor, memory. For each of these resources, it is proposed to evaluate the change in such characteristics as the degree of resource load and the speed of its change. The proposed method allows you to build a system of rules for the membership of the analyzed vectors to the specified classes and minimize the conditions number in the generated rules. The problem of ensuring the unmanned vehicles information security operating in the intelligent networks of the smart city transport infrastructure does not lose its relevance due to the fact that modern networks face an unprecedented range of computer threats that lead to a violation of the integrity, confidentiality and availability of resources.

Keywords

UMV resources, vulnerability detection, continuous values discretization, intelligent technology

1. Introduction

The basis of this article is the material, obtained in the research laboratory of "Intelligent Information Systems and Critical Computing" at the Department of "Information Technologies and Computer Systems" of Sevastopol State University within the framework of the RFBR grants (grant No. 19-29-06015 "Adaptive neural network methods for detecting vulnerabilities in the interfaces of unmanned vehicles based on artificial immune systems" and grant No. 19-29-06023 "Methods of structural synthesis of information exchange channels between an unmanned vehicle and a dispatch center based on stochastic analysis). vector programming with probabilistic criteria"), in which the authors of this article were co-executors.

The experience gained so far in setting problems of describing and analyzing vulnerabilities of information systems of various classes is mostly associated with the analysis of vulnerabilities that directly affect a certain function of information systems, but the problem of integrating systems and nesting components give rise to a high degree of variability of solutions and parametric uncertainties of various types. In the monograph, based on the analysis of the state of the problem, the main vulnerable elements of UMV information systems are considered; the functional-complete set of models for evaluating the effectiveness of the protection of UMV information systems is defined; the approach to variant analysis and selection of vulnerable components based on expert assessments and fuzzy sets is further developed.

The problem of ensuring the unmanned vehicles information security operating in the intelligent networks of the smart city transport infrastructure does not lose its relevance due to the fact that modern

III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021), May 28, 2021, Krasnoyarsk, Russia

EMAIL: dmitriymoiseev@mail.com (Dmitriy Moiseev); a.alexir@mail.ru (Alexey Bryukhovetskiy)
ORCID: 0000-0002-3141-1529 (Dmitriy Moiseev); 0000-0002-2612-2968 (Alexey Bryukhovetskiy)

networks face an unprecedented range of computer threats that lead to a violation of the integrity, confidentiality and availability of resources. To date, there are a large number of methods for detecting vulnerabilities in UMV interfaces, which quite effectively perform detailed researches of the UMV resources information state and search for intrusions sources. The heterogeneity of applications and wireless communications in the smart city infrastructure significantly complicates the facilities security [1]. Therefore, the development and implementation of approaches to the creation of information technologies that ensure the security of the smart city critical information infrastructure are relevant and of scientific and practical interest. The need to solve this problem is associated with significant changes in the field of applied digital technologies in Vanet networks, which use technologies implemented using interfaces: vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-pedestrian, vehicle-to-grid, vehicle-to-device [2].

In the works [2, 3] the applied methods and solutions in intelligent transport networks are considered in order to ensure the safety of the UMV operation. The paper presents the classification of attacks on UMV and means of ensuring information security in Vanet networks. The requirements for the UMV architecture and data exchange between smart city infrastructure objects are defined. The creation of management systems for such tools implies the need to study methods and approaches related not only to the conceptual organization of such systems architecture, but also to their software implementation. When developing software, special attention is paid to ensuring UMV security. For autonomous driving of a vehicle, it is necessary to systematically update its software. Upgrading over a wireless network can bring many benefits to both consumers and manufacturers (Figure 1:).

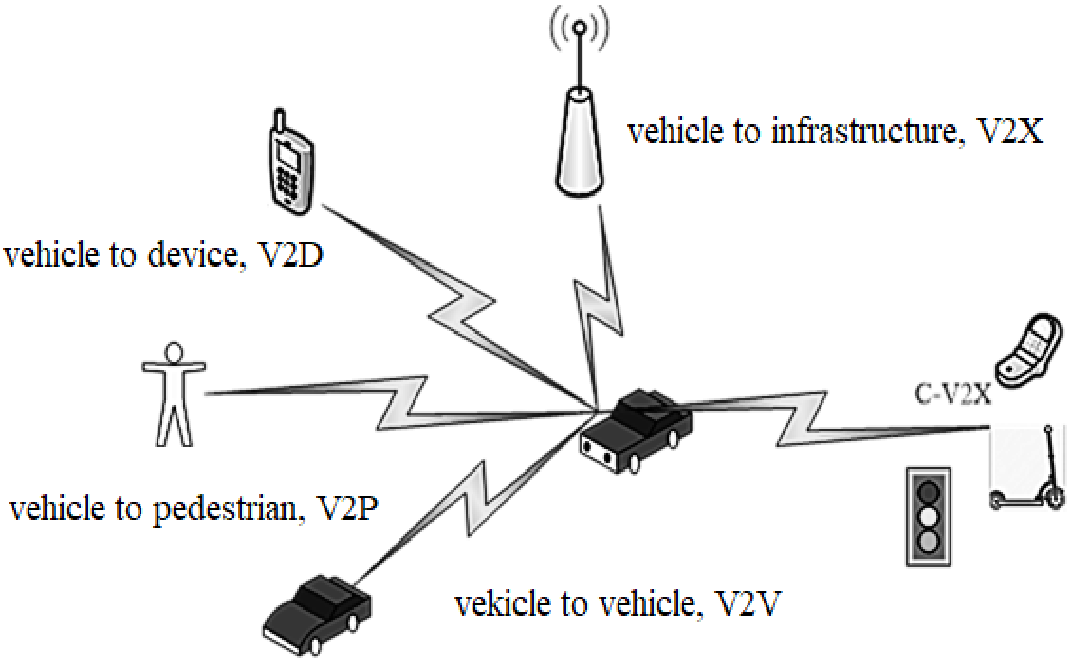

Figure 1: x_r Types of main BTS interfaces

The authors of the article also obtained some results in the works, the solution of problems of intrusion detection in computer networks based on the assessment of changes in the network traffic state using statistical criteria, nonparametric statistics methods [4], multi-agent model of UMV information interaction [5], mechanisms adaptation of artificial immune systems to control the parameters of UMV resources state[6], anomalies detection using Markov sequences [7], and also on the concept development of an intelligent monitoring system for solving large-scale tasks in cloud computing environments [8]

The problem of information security is multifaceted, costly and knowledge-intensive. The search for effective solutions to ensure information security leads to the need to create new structural elements in systems and networks. Their main purpose is to determine the presence of an attack. Timely detection of an attack leads to a reduction in the latent period of its action, minimizes the amount of damage caused, as well as the costs associated with subsequent reengineering.

2. Problem statement

In this article, we propose a method for detecting vulnerabilities in UMV interfaces based on continuous values discretization. Discretization is a technology for separating continuous attribute values in a finite set of adjacent intervals in order to obtain a set of attribute values belonging to a single class [9,10]. One of the main features of the proposed approach is to build a system of rules for determining the ownership of a feature vector describing UMV resources state, containing the minimum number of conditions to be checked.

Given a training data set $\boldsymbol{X}$, containing m objects $\boldsymbol{x_j}$ $(j=1, m)$ each of which belongs to a single class C_k ($k=1, s$). Each $\boldsymbol{x_j}$ is an l-dimensional feature vector describing the state of system resources in the UMV-dispatch center channel at time t. System resources include: data link, memory, and processor. We will assume that the UMV can be in one of three states: normal, precritical, critical. The permissible limits of state changes ranges are set on the interval [0;1], $C_k \epsilon$ [0;1]. We will use metrics as resource characteristics:

- D – loading a resource (M-memory, Ch- channel capacity, Pr-processor),
- V – the rate of decrease in the volume of the resource.

Thus, the vector $\boldsymbol{x_j}$ is represented by a attributes tuple

$$\boldsymbol{x_j} = (D_M, D_{Ch}, D_{Pr}, V_M, V_{Ch}, V_{Pr}, t \mid C_k)$$

We need to find a discretization scheme that will establish a relationship between the impact of attacks and the system resources states that are subject to change under external influence.

3. Method description

We will assume that values range of each attribute $\boldsymbol{x_r}$ is represented on n discrete intervals, each of which is represented by a values pair:

$$\{[z_0, z_1], (z_1, z_2], \ldots, (z_{n-1}, z_n]\},$$

where z_0 – minimum value, z_n – maximum attribute value $\boldsymbol{x_r}$ for any r $(0=< r< n)$, $z_r<z_{r+1}$. Set of values

$$\{z_1, z_2, \ldots, z_{n-1}\}$$

is the split points for the attribute $\boldsymbol{x_r}$. The main idea of the algorithm is as follows. Let the split point in the first iteration be the average value between two adjacent attribute values $\boldsymbol{x_r}$. If the values z_r fall into the intervals $(z_{r-1}, z_r]$ and $(z_r, z_{r+1}]$ and belong to the same class– remove z_r from the list of $\boldsymbol{x_r}$ -attribute split points until we find a pair of values that fall into two adjacent intervals but do not belong to the same class. The process of selecting the split points is proposed to be optimized using the criterion DCR (Discretization using Class Information to Reduce Number of Intervals) [9 - 12].

Each attribute value can only be classified in one of the n intervals. For each attribute, a discretization scheme is constructed (Figure 2:) in the form of a two – dimensional array, the columns of which are associated with the intervals of loading values and the rate of reduction of resources, and the rows-object classes.

Class			*Intervals*			*Total in class*
	$[z_0, z_1)$	……	$[z_{r-1}, z_r)$	……	$[z_{n-1}, z_n]$	
C_1	q_{11}	……	q_{1r}	……	q_{1n}	q_{1+}
……	……	…….	……	…….	……	……
C_i	q_{i1}	……	q_{ir}	……	q_{in}	q_{i+}
…….	……	…….	……	…….	……	……
C_s	q_{s1}	……	q_{sr}	……	q_{sn}	q_{s+}
Total number in intervals	q_{+1}	…….	q_{+r}	…….	q_{+n}	Q

Figure 2: x_r attribute discretization scheme

In this Figure 1:, the following designations are accepted:

q_{ir} – total number of values belonging to the class C_i, which are in the interval $(z_{r-1}, z_r];$

Q_{i+} – total number of objects belonging to the class C_i;

Q_{+r} – total number of attribute values $\boldsymbol{x_r}$, which are in the interval $(z_{r-1}, zr]$.

The criterion used allows us to find a discretization scheme in which each interval belongs to objects of only one class. We will also assume that the resources D_j, V_j, can be in one of the following states:

- normal,
- pre-critical,
- critical,

where D_j, V_j є [0;1]. The number and values of the resource state boundaries are set by the expert depending on the nature of the task to be solved: the UMV purpose, the movement dynamics, environmental conditions, etc.

The algorithm for constructing the sampling scheme contains the following sequence of actions.

1. Perform steps 1 – 6, for $j=1..m$, where m – number of attributes.
2. Arrange attribute values x_j in ascending order. Minimum value – z_0, maximum value – z_n.
3. Create a set of all possible split points Z, for $\boldsymbol{x_r}$ attribute.
4. Construct a discretizatioin scheme for the $\boldsymbol{x_r}$ attribute using the obtained partition points Z.
5. Calculate the value of the *DCR* criterion for all possible obtained partition points Z:
$$\mathrm{DCR} = \frac{\sum_{r=1}^{n}\left(\sum_{i=1}^{S} q_{ir}^2/q_{+r}\right)}{n}$$
6. Select the division boundary that gives the highest value of the criterion *DCR*.
7. Repeat steps 2 – 6 for intervals that contain objects belonging to different classes.
8. Build a rules system for classifying input vectors that describe the resources state.
9. End.

The proposed method allows us to build a rules system for the membership of the analyzed vectors to the specified classes and minimize the conditions number in the generated rules. This circumstance plays an important role in the analysis of information received from the UMV in real time. In addition, it is proposed to use several rules sets built separately for the parameters combinations specified by the expert for the specified sets of resource states $\{D_M, D_{Ch}, D_{Pr}, V_M, V_{Ch}, V_{Pr}\}$ **,** for example, the rules for parameter D, the rules for parameter V, and others. Then the decision about UMV state– S_{UMV} can, for example, be accepted in accordance with the following rules: S_{UMV} є {critical}, if they are in a critical condition:

- one of the resources {*M, Ch, Pr*} by one criteria {D_j, V_j},
- one of the resources based on two criteria {D_j, V_j} etc.

4. Conclusions

The ongoing research in the field of intelligent transport systems is based on a theoretical and methodological basis in the areas of self-organization of complex natural and artificial immune systems, which provide a balanced strategy for finding a solution and combine local and global search for a solution. It has been established that the solution to the problem of detecting BTS vulnerabilities is characterized by multidimensionality, multi-criteria, the influence of information presentation forms on the classification accuracy, the need to use minimal a priori information, a combination of determinism and fuzziness, the possibility of combining formal methods and taking into account expert judgments.

Currently, most of the problems of data analysis are associated with studies of stochastic dynamical systems, in which the detection of significant, but rare information situations is often of decisive importance. The necessity of building information technology is revealed, since an analytical solution is impossible under the given conditions.

The development of an intelligent technology for detecting vulnerabilities in BTS interfaces, based on the use of new approaches and methods, will lead to an increase in the validity, reliability and efficiency of decision support processes for assessing the probability of accepting hypotheses about the presence of anomalous values, taking into account errors of the first and second kind.

Adaptive decision-making methods under conditions of uncertainty will eliminate the shortcomings and limitations inherent in classical approaches in the case of noisy data and incomplete information.

On the basis of Big Data technology and a special modeling stand being developed, the quality of evaluating decisions is improved.

The proposed approach is focused on real-time use, as it has a relatively low computational complexity. Using the simulation mode of decision-making processes allows the expert to: first, implement the training mode, and secondly, gives the system as a whole adaptive properties. A promising direction is to study the sensitivity and stability of the UMV state to the impact of attacks on a resources variety, to determine the probabilities estimates of accepting hypotheses P(H0|H0), P(H0|H1), P(H1|H0), P(H1|H1) when recognizing the UMV resources states.

5. Acknowledgements

The research was carried out with the financial support of the RFBR in the framework of scientific projects № 19-29-06015 and № 19-29-06023.

6. References

[1] P. D. Zegzhda, M. A. Poltavtseva, D. S. Lavrov, Systematization of cyberphysical systems and assessment of their security? Problems of information security Computer system (2017) 127–138.

[2] H. Hasrouny, A. Samhat, C. Bassil, A Laouiti, Vanet security challenges and solutions: A survey Vehicular Communications 7 (2017) 7–20.

[3] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and IoV Ad Hoc Networks 61 (2017) 33-50.

[4] B. Mokhtar, M. Azab, Survey on security issues in vehicular adhoc networks Alexandria Engineering Journal 4 (2015) 1115–1126.

[5] A. V. Skatkov, A. A. Bryukhovetskiy, D. V. Moiseev, Kullback measure in dynamic clustering problems of environment state observations, Environmental monitoring systems 3 (2019) 35–38.

[6] S. Kulbak, Information theory and statistics, Moscow, Nauka, 1967.

[7] A. V. Skatkov, D. V. Moiseev, A. A. Bryukhovetskiy, Model for vulnerabilities detection in unmanned vehicle interfaces based on artificial immune systems, IOP Publishing Ltd Journal of Physics: Conference Series 1515 (2020) 022043.

[8] A. V. Skatkov, A. A. Bryukhovetskiy, D. V. Moiseev, V. I. Shevchenko, Detecting vulnerabilities of information resources of unmanned vehicles method based on dynamic evaluation of Markov sequences properties, IOP Publishing Ltd Journal of Physics: Conference Series 1515 (2020) 022033.

[9] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and IoV Ad Hoc Networks 61 (2017) 33–50.

[10] D. A. Zighed, A method for discretization of continuous attributes for supervised learning, International Journal of Uncertainty, Fuzziness and Knowledge – Based Systems 17 (2001) 307–326.

[11] A. H. Mohammed, A. L. Junaid, A. A. Syed, Classification of Security Attacks in VANET: A Review of Requirements and Perspectives, MATEC Web of Conferences, 150 06038 (2018) doi:/10.1051/matecconf/201815006038.

[12] A. V. Skatkov, A. A. Bryukhovetskiy, V. I, Shevchenko Monitoring of qualitative changes of network traffic states based on the heteroscedasticity effect, Application of Information and Communication Technologies (2016) 7991765.