Adaptive fuzzy model for detecting of vulnerabilities of unmanned vehicles interfaces based on evaluation of the information state of resources

A V Skatkov, A A Bryukhovetskiy and D V Moiseev
Sevastopol state university, 33 Universitetskaya str., Sevastopol, 299053, Russia

E-mail: dmitriymoiseev@mail.ru

Abstract. An adaptive model for detecting vulnerabilities in the interfaces of unmanned vehicles based on dynamic assessment of information states of resources is proposed. The method is based on fuzzy logic and immunological principles. Rules classify objects belonging to several classes at the same time with different degrees of belonging. Resource state recognition is performed under conditions of a lack of a priori information about the properties of the intrusion source and the stochastic nature of the recognized events. To increase the level of reliability of vulnerability detection, the model makes adaptive dynamic tuning of decision-making rules for classifying the information state of unmanned vehicle resources.

1. Introduction
The need to solve problems that ensure the security of critical information infrastructure "smart city" is caused not only by the growth trends in traffic flows, but also by significant changes in the field of applied digital technologies on vehicles, when the network is used to interact with the environment using interfaces: V2V, V2X, V2P, V2G, V2D, and in intelligent transport systems-Big Data + Business Intelligence. Failure or disruption of the unmanned vehicles (UMV) can lead to disorganization of the entire infrastructure and, consequently, the risk of critical situations that can have catastrophic consequences. Securing VANET networks involves developing methods to detect attacks on vehicles and vehicle networks, including type attacks: DoS – denial-of-service[1], DDoS- distributed denial of service, Black-hole[2], Man in the middle [3], Sybil [4], Impersonation Attack and Masquerade [5], Timing Attacks [6], as well as attacks on smart vehicle components.

Development of models of protection mechanisms in information and computer networks and research of their effectiveness is considered in works [7-9]. A special place is occupied by the problem of ensuring the security of critical infrastructures, which include the "smart city" system, which is a large-scale cyber-physical system that coordinates interactions between heterogeneous physical devices and computer systems in real time [10].

The main purpose of UMV interfaces is to provide information exchange of data. There are three types of interfaces: UMV - UMV, UMV- dispatch center, UMV - base stations of the smart city infrastructure. The main requirements for interfaces are: high reactivity, noise immunity, and dialog support. The main characteristics of interfaces also include the bandwidth of the communication channel, speed, cryptographic stability, availability coefficient, time to failure, etc. Therefore, the development of methods that ensure the security of information interaction between UMV and other subjects of the "smart city" is an urgent task. The article considers an adaptive approach based on
fuzzy logic methods in combination with artificial immune system (AIS) methods used to optimize the model parameters [11].

2. Building a vulnerability detection model

We will evaluate the impact of information impact on the state of UMV resources, such as the communication channel, processor, memory, etc. The state of a resource can be evaluated by such characteristics as: resource loading, the rate of change in resource loading, and so on. For example, the amount of channel, processor, input memory buffer load, or the rate of change in the load of these resources that exceeds a specified threshold can be classified as a pre-critical / critical state of the UMV.

We introduce the notation for the evaluation of initial specifications:

\[ RV = \{RV_1, ..., RV_m \} \]  – the set of UMV resources, \( m \) – number of resources,

\[ SF = \{SF_1, ..., SF_l \} \]  – the set of the initial specifications of UMV, \( l \) – number of specifications, \( SF \in \{D, V\} \), for example:

\[ D_j \]  – loading the \( j \)-th resource, a vector quantity with components of sets elements \( RV_j \),

\[ V_j \]  – the rate of loading change \( D_j \), a vector quantity with components of sets elements \( RV_j \),

where \( V = V/Δt \), \( ΔV = D(t) - D(t_0) \), changing the \( D_j \) value over time \( Δt \), \( Δt = t_i - t_{i-1} \) – the interval between two adjacent time points, \( t_i \) – the \( i \)-th time of measurement of specifications, \( t \in [0;T] \).

The values of the \( D_j \) and \( V_j \) are normalized and defined in the range \([0;1]\) and correspond to fractions of values \( D_0 \) and \( V_0 \) accordingly, at the time moment \( t_i \). The \( \{D, V\} \) structures are vector matrix functions of the operational moments of decision time, i.e. they form numerical matrices for a fixed \( t_i \).

We assume that the \( SR_j \) state of the \( RV_j \) resource at a given time \( t \) depends on:

- values of controlled specifications \( SF_j \),
- methods for evaluating resource specifications – MD\( j \), for example, statistical methods,
- metrics – MR\( j \), for example, sample mean, sample variance, etc.,
- range values – R\( j \) intervals for determining the physical state of the resource,
- criteria \( CR_j \) for evaluating resource states.

Let these states be denoted by \( SR_j = \{SR_{j0}, SR_{j1}, SR_{j2}\} \) – the set of possible states of the \( RV_j \) resource at the time moment \( t \). State values are defined and normalized in the range \([0;1]\). Let states be defined at intervals \([R_k; R_{k+1}]\), where \( R_k \) – range for setting the scope for determining the resource state, \( k=0,2 \). Without losing generality, for example, we will assume that we have three intervals on which possible states are determined \( SR_{j\epsilon} \in \{0, 1, 2\} : \)

\[ SR_{j0} \epsilon [0;R_0], \ SR_{j1} \epsilon (R_0;R_1], \ SR_{j2} \epsilon (R_1;R_2]. \]

Without breaking the generality of the description, let's assume that the area with the number " 0 " - indicates a normal state, area " 1 " - a pre-critical state, a slight deviation from the normal state, and area " 2 " correspond to the critical state of the resource, when the deviation from the normal state is significant. The level of detail of resource States is determined by the expert and depends on the operating conditions of the UMV.

We introduce the notation for the estimation of information state \( S_j \) of the \( RV_j \) resource at a given time moment \( t \), which depend on:

- values of controlled specifications \( SF_j \),
- initial states – \( SR_j \),
- methods for evaluating information states – MD\( j \), for example, methods of nonparametric statistics, etc.,
- information metrics – \( MI_j \), which can be referred to the Spearman coefficient, the Kullback divergence, Schwarz information metric and others,
- range values – \( R_{ij} \) intervals for determining the information state of the \( St_j \) resource.
- \( Cl_j \) criteria for evaluating information states of resources, level of reliability, errors of the first and second kind.
Taking into account the designations introduced above, we present a sequence of main stages for evaluating the information state of UMV resources, which includes the following sets of objects (figure 1):

**Evaluation of initial specifications of the resource states of UMV**

- UMV resources
- Specifications
- Methods
- Metrics
- Set of ranges
- Set of criteria
- Set of resource states

**Evaluation of information specifications of UMV resource states**

- Methods for evaluating information states
- Set of criteria
- Classification of information states
- Decision Support System

**Figure 1.** Sequence of main stages of evaluating the information states of UMV resources.

3. **Methods and results**

The decision support system performs the functions of assessing the reliability of detecting vulnerabilities, errors of the first and second kind, optimizing rule parameters, adapting parameters to the current information state of the resource, making decisions on risk assessment, determining vulnerability detection scenarios, forming a strategy for monitoring the state of resources, etc. Thus, the formation of the information state of UMV resources is carried out as a result of the following main transformations:

\[ S': (SR^1, MDI, CI), \]

\[ MDI: (RV_{1}, . , RV_{p}, PR_{j,MI} ) \]

\[ PR_{j,MI} - \text{procedures for selection of range } RI_{j} \text{ for } j\text{-th resource by using } MI \text{ metric} \]

\[ SR^2: (V(G,v), MD, CR, \xi(t), \alpha, z), \]

where, \( V(G,v) \) – sample from the general set \( G \) with the volume \( v \),

\( MD \) – method for evaluating resource specifications,

\( \xi(t) \) - perturbation vector \( \xi(t) \),

\( \alpha \) – the level of reliability of control,

\( z \) – risk and loss evaluation.

As a result, the information state of the UMV at the time moment \( S'_{UMV} \) for the specifications \( D_{j}, V_{j} \) on the time interval \( T \) can be represented by a tuple:

\[ UMV: \langle D_{j}, V_{j}, SR^1_{Dj}, SR^1_{Vj}, S'_{Dj}, S'_{Vj}, T, S'_{UMV} \rangle. \]
Structurally, the tuple describing the information state of the UMV is represented by the n-component vector \( x=\langle x_1, \ldots, x_n \rangle \), belonging to one of the \( C_i \) \( (i=1..k) \) classes of possible states, for example, \( S_{\text{UMV}} \in \{0,1,2\} \), where «0» - normal state, «1» - pre-critical state, «2» - critical state. The level of detail of the UMV states is determined by the expert and depends on the operating conditions of the UMV.

Taking into account the considered sets, we can state that the solution of the problem of assessing the information state of UMV resources is an optimization problem of multidimensional multi-criteria classification, which can be solved using adaptive technologies based on artificial immune systems. Adaptive approaches allow us to solve problems of compensating for missing information and evaluating the dynamics of resource availability in the process of detecting UMV vulnerabilities. Therefore, an expert approach based on data mining is needed. One of the most powerful tools in the implementation of intelligent technologies is technologies based on AIS, which allow solving a wide range of problems of image recognition, identification, forecasting, and optimization. With these technologies, learning, self-learning, and adaptation modes are easily implemented. Implementation of such problems is not always possible using an analytical approach, since these problems are characterized by non-linearity, undifferentiability, multi-extremality, complex topology of the range of acceptable values, high computational complexity of optimized functions, high dimension of the search space, etc. Therefore, the use of bioinspired search methods based on local and global optimization in the state space are necessary tools in the process of solving problems of computer security of UMV.

Next, as an example, we consider the case of classifying the state of network traffic, the structure of which is similar to the structure of the tuple describing the information state of the UMV – \( S_{\text{UMV}} \). The model is based on the results of analyzing information that is presented in a public database of network traffic samples KDD Cup [12]. The input data is structurally n-dimensional vectors belonging to one of the five classes \( C_i (i=1..5) \) of possible states of the network traffic: NS – normal state, DoS — denial of service, R2L — unauthorized access from a remote computer, U2R — unauthorized access to privileged user rights, Probing — scanning ports to identify vulnerabilities in the system.

We will use the following solving rules for fuzzy inference to solve the problem of \( k \)-dimensional classification of vectors \( x=\langle x_1, \ldots, x_n \rangle \) with \( n \)-numeric attributes when using \( C_i \) classes:

\[
R_j: \text{if } x_i \text{ is } L_i \text{ and ... and } x_n \text{ is } L_n \text{ then CLASS } C_i | \alpha_{j} | \beta_{j} \]

where \( R_j \) — label of the \( j \)-th fuzzy rule, \( j=1,\ldots,N \); \( N \) — number of fuzzy rules; \( L_i \) — linguistic term (the input interval of each \( x_i \)-th numeric attribute is divided using three linguistic terms \( a,b,c \) ); \( \alpha_{j} | \beta_{j} \) — function that determines the degree of belonging to a particular class, \( \alpha_{j} \in [0,1] \); \( j \) — quality metric of classification rules \( \beta_{j} \in [-1; 1] \):

\[
\beta_{j} = \frac{w_1 \cdot a_j}{|\text{AS}|} - \frac{w_2 \cdot b_j}{|\text{NS}|},
\]

where \( a_j \) — number of correct classifications AS; \( b_j \) — number of misclassified NS; \( |\text{AS}| / |\text{NS}| \) — the total number of AS and NS respectively; \( w_1, w_2 \) — non-negative weight coefficients; \( w_1 + w_2 = 1 \).

The structure of the vulnerability detection model consists of the following main modules: training, testing and configuration, traffic status classification, adaptation, and decision making.

Training module. The module is designed to identify informative signs of network traffic and form fuzzy rules of the form (1). Functional transformation is reduced to forming a set of rules based on a training sample: \( X^{(d)} \rightarrow X^{(e)} \rightarrow R \), \( (d=41) \), \( n \leq d \). Using the preprocessing procedure, the most informative signs of network traffic are identified [13]. For each element of the Cartesian product of the set of examples – \( X \) and the set of rules – \( R \) the \( \alpha_{j} \) score is calculated. The generated sets of \( R_k \) rules can be considered in terms of AIS as a population of antibodies. The quality of the rules included in \( R_k \) is integrally evaluated by the metric \( F_w \). The most effective subset of \( R_k \) rules has the maximum value of the \( F_w \) metric: \( F_{\text{max}} = \max \{ F_w \} \).

Testing and configuration module based on AIS methods. The main function of this module is to generate an optimized set of rules: \( R \rightarrow R_n \). The algorithm for forming and optimizing the structure and parameter values of fuzzy rules is based on an iterative procedure for processing training sample examples based on the methods of the AIS. In this case \( n \)-dimensional numerical vectors of the training sample act
as an antigen, and fuzzy rules act as antibodies [11]. The model uses triangular membership functions with parameters \( a, b, c \), which are configured on the training sample. In the testing mode, the values of the \( f_j \) metrics are corrected for the quality of the rules. As a result, many optimized classification rules are generated – \( R_\alpha(\text{NS}) / R_\alpha(\text{AS}) \) with the specified parameters \( w \).

**Classification module.** The classifier performs the following basic functional transformations: \( X(n) \rightarrow R_\alpha \rightarrow \{Y(\text{NS}), Y(\text{AS})\} \). When classifying the current state of traffic on the set of rules \( R_\alpha(\text{NS}) \) a binary signal \( Y(\text{NS})=1 \) is generated and the hypothesis \( H(\text{NS}|\text{NS}) \) is confirmed. In the classification of the current state (CS) on a set of rules \( R_\alpha(\text{AS}) \) a binary signal \( Y(\text{AS})=1 \) is generated and the hypothesis \( H(\text{AS}|\text{AS}) \) is confirmed. Otherwise, signals \( Y(\text{NS})=0 \) и \( Y(\text{AS})=0 \) are generated respectively. However, when classifying the current state of traffic, there may be errors of the first and second kind. These cases are shown using the functional elements of traffic state classification on the sets of rules \( R_\alpha(\text{NS}) \) and \( R_\alpha(\text{AS}) \) (figure 2):

**Figure 2.** Functional elements of vehicle classification procedures: a) by the rules \( R_\alpha(\text{NS}) \), b) by the rules \( R_\alpha(\text{AS}) \).

In this case it is necessary to clarify the hypotheses:
- \( H(\text{NS}|\text{AS}) : \text{CS} = \text{AS} \), abnormal traffic is assumed to be normal,
- \( H(\text{AS}|\text{NS}) : \text{CS} = \text{NS} \), normal traffic is mistaken for abnormal traffic.

Therefore it is proposed to determine the output signal \( Y \) or evaluating the current traffic state based on the maximum value of the total \( f_j \) ratings of the activated rules for each class:

\[
F_{\max}(C_i) = \max \{ F(C_i) \},
\]

where \( F(C_i) = \sum_{R_\alpha(C_i)} f_j(C_i) \).

The adaptation module. In order to improve the quality of classification, the system provides a mode for adapting rules to the state of current traffic. The adaptation module corrects the metrics of the activated rules \( R_j \in R_\alpha \) depending on the current state of the traffic. By introducing feedback, the values of the \( Y \) signals of the activated rules are analyzed. Correction of rules is performed as a result of recalculation of \( f_j \) values.

Decision making module. In order to assess the quality of traffic state classification, the system is also self-tested in the operating mode of the adaptive model. For this purpose, during the operation of the model, the current values of the intrusion detection confidence level and the false alarm level are generated, which are compared with the corresponding values generated during the training process. If the classification quality has deteriorated, the rule base needs to be modified. In this case, a decision is made to switch to the training mode on the updated sample \( X \) and then to the optimization mode, after which the testing is repeated and updated values of the CF and \( f_j \) metrics of the rules are formed and new values of the DR, FAR parameters are calculated on their basis.

4. Conclusion
The purpose of experimental studies is to assess the quality of traffic status classification for different volumes of testing samples, with varying range values of \( CF_\alpha, f_\alpha \), the influence of the adaptation mode,
and others. Fourteen features out of forty one that were identified using the decision tree method were used as informative features [13]. An individual sample was used for each of the experiments. The average level of likelihood (for the mode with adaptation ~97.99 – 92.00%, without adaptation mode ~95.04 – 85.62%) and false positives for classes in experiments with adaptation (~1.24 – 3.97%) and without adaptation (~2.20 – 4.48%) is shown in figure 3. The results obtained in solving the problem of network traffic classification are statistically stable and generally represent the features of the proposed approach. Using the adaptation mode increases the likelihood of classifying network states. For FAR estimates of all classes, this pattern is observed in every experiment performed. Thus, the results of the experiments confirm that the proposed model is sensitive to the configurable parameters of fuzzy rules and the ranges $CF_\alpha, f_\alpha$.

![The results of the traffic classification](image)

**Figure 3.** The results of the traffic classification.

The use of a fuzzy adaptive model in combination with AIS methods allows us to reasonably choose the intervals for recognizing information situations, increase the level of likelihood of classifying information states of objects, and minimize errors of the first and second kind.

**Acknowledgments**

This work was supported by the Russian Foundation for Basic Research (projects № 19-29-06015/19, 19-29-06023/19).

**References**

[1] Cho K and Shin K 2016 Fingerprinting electronic control units for vehicle intrusion detection, *USENIX Security Symposium* **40** 911–27
[2] Sedjelmaci H and Senouci S 2015 An accurate and efficient collaborative intrusion detection framework to secure vehicular networks, *Computers & Electrical Engineering* **43** 33–47
[3] Al-kahtani M 2012 Survey on security attacks in vehicular ad hoc, *Signal Processing and Communication Systems* **12**(19)
[4] Wang L and Kangasharju J 2013 Measuring large-scale distributed systems: case of bittorrent mainline dht, *IEEE P2P 2013 Proceedings* **3** 1–10
[5] Chima T, Yiu S, Lucas C, Victor O 2011 SPECS: Secure and privacy enhancing communications schemes for VANETs, *Journal of Ad Hoc Networks* **9** 189–203
[6] Irshad A, Jamalul-lail M and Hasbullah H 2011 Timing Attack in Vehicular Network, *Recent Researches in Computer Science* **4** 151–5
[7] Zaidi K, Milojevic M, Rakocevic V, Nallanathan A and Rajarajan M 2016 Host-based intrusion detection for vanets: a statistical approach to rogue node detection, *IEEE transactions on vehicular technology* 65 8 6703–14

[8] Pokusaev O N 2019 Ontologies and safety of autonomous (unmanned) vehicles, *International Journal of Open Information Technologies* 7 2 2307–8162

[9] Skatkov A V, Bryukhovetskiy A A and Moiseev D V 2017 Intelligent monitoring system for solving large-scale scientific problems in cloud computing environments, *Information and control systems* 2 87 19–25

[10] Zegzhda P D Systematization of cyber-physical systems and assessment of their security, *Computer systems* 2 127–38

[11] Dasgupta D 2006 *Artificial immune systems and their application* (Moscow: Fizmatlit)

[12] Kabiri P and Ghorbani A 2005 Research in Intrusion Detection and Response. A Survey *International Journal of Network Security* 2 102-184

[13] Bryukhovetskiy A A, Skatkov A V and Berezenko P O 2013 Vulnerability detection in critical applications based on decision trees, *Electronic and computer* 5 64 18–23