BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 64, No. 3, 2016
DOI: 10.1515/bpasts-2016-0070

Fuzzy interpretation for temporal-difference learning in anomaly detection problems

A.V. SUKHANOV[1,2]*, S.M. KOVALEV[1] and V. STÝSKALA[2]

[1]Rostov State Transport University, 2 Rostovskogo Strelkovogo Polka Narodnogo Opolcheniya sq., Rostov-on-Don 344038, Russia
[2]VŠB Technical University of Ostrava, 17. listopadu 15/2172, 708-33 Ostrava-Poruba, Czech Republic

Abstract. Nowadays, information control systems based on databases develop dynamically worldwide. These systems are extensively implemented into dispatching control systems for railways, intrusion detection systems for computer security and other domains centered on big data analysis. Here, one of the main tasks is the detection and prediction of temporal anomalies, which could be a signal leading to significant (and often critical) actionable information. This paper proposes the new anomaly prevent detection technique, which allows for determining the predictive temporal structures. Presented approach is based on a hybridization of stochastic Markov reward model by using fuzzy production rules, which allow to correct Markov information based on expert knowledge about the process dynamics as well as Markov's intuition about the probable anomaly occurring. The paper provides experiments showing the efficacy of detection and prediction. In addition, the analogy between new framework and temporal-difference learning for sequence anomaly detection is graphically illustrated.

Key words: anomaly prediction, Markov reward model, hybrid fuzzy-stochastic rules, temporal-difference learning for intrusion detection.

1. Introduction

Automatic analysis, which allows for detecting specific or unusual temporal sets, becomes the key task in many application domains and research areas [1]. Here, one of the most interesting and important questions is the determination and prediction of time structures or temporal patterns related to emergency of faults and unexpected events. These events are often called as anomalies and outliers and do not conform to expected behavior. From a practical point of view, the task of unusual pattern detection is linked to problems of technological process control. The decision plays a vital role when preventing signalization is needed before an emergency occurs, diagnosis of technical devices is required before a fault appears, intrusion detection is necessary before a virus is received, etc.

A popular solution to this problem is using temporal data mining tools [2]. Temporal data mining is one of relatively young research directions, which comes from new directions of informatics and artificial intelligence domains. The main aim of temporal data mining is the extraction of useful information for further usage in support decision systems. Because of these facts, modern temporal data mining techniques still require modifications and improvement.

Because of new generations of the intelligent information control groups based on knowledge bases, complicated systems such as railway transport systems face new technological problems. These problems are related to big data analysis, whose main objective is to determine sequences leading to abnormal events for trouble-free control provision [3]. Moreover, modern technological problems are caused by a high degree of dynamism as well as soft real-time and hard real-time requirements. The second key factor is the presence of "non-stochastic" types of uncertainty, which refer to noises and distortions of different nature and to inaccuracy of analyzed data. The above mentioned aspects show the difficulty of temporal data mining implementation resulting in a need for new methods elaboration.

This paper presents the hybrid fuzzy-stochastic approach for anomalous events prediction and specific temporal patterns detection in stochastic time series of general form, which describe non-Markov processes. Key feature of the proposed framework is incorporation of fuzzy rules and drawing an analogy between the new technique and temporal-difference learning technique. In other words, the paper provides a statistical model by intelligent correction according to anomalous forthcoming.

The paper is organized as follows. Section 1 discusses the background of sequence anomaly detection and Markov reward modeling. Section 2 presents fuzzy temporal detection notions and proves the possibility of fuzzy generalization for temporal-difference learning. Section 3 provides experimental results of benchmarking with existing sequence anomaly detection techniques. Moreover, it proves the framework efficacy of anomaly prediction. In Section 4, the conclusions and future work are proposed.

2. State of art

2.1. Anomaly detection. Anomaly detection in time series is referred to the problem of finding sequence patterns which conform (or do not conform) to the criteria of a certain task [2]. Sequences are ordered series of consequent events which can be presented by different types, such as binary, discrete and continuous, depending on the application domain. Real conditions give the preference to discrete and continuous forms of representation. Note that the specific form, in which continuous patterns are presented when the anomaly detection task should

*e-mail: drewnia@rambler.ru

be decided, suggest to transform them into phase space [4] or discrete time series [5]. Anomaly detection for discrete sequences is often called sequence anomaly detection.

The most common way for problem statement for sequence anomaly detection is converged to finding and/or predicting specific types of events, which are not expected when the normal behavior of a system is observed. Different problem interpretation proposes the objectives like anomalies, outliers or even interesting events. Based on training data availability, existing approaches for sequence anomaly detection can be merged into three groups [1]:

1. Supervised anomaly detection. Techniques trained in supervised mode assume the availability of a training data set that has labeled instances for normal as well as anomaly class. Typical approach in such cases is to build a predictive model for normal and anomaly classes. Any unseen data instance is compared against the model to determine which class it belongs to [6].
2. Semi-supervised anomaly detection. Techniques that operate in a semi-supervised mode assume the availability of only normal or abnormal class [7].
3. Unsupervised anomaly detection. Techniques that operate in this mode do not require any training sequences. Unsupervised approaches are commonly used for clustering [8]. Here, the most remote patterns are labeled as anomalous.

Proposed framework is dedicated to supervised anomaly detection, but it can be improved for utilizing in other modes. A particular problem statement for presented framework can be formulated as follows.

Let the initial time series data set describe the behavior of complex technological system when it is functioning. This set has some events, which are labeled as anomalies by human expert. There is also one assumption, according to which each anomaly is a result of specific patterns evolution. These patterns are unknown to the expert. The key task of our framework is to detect these patterns presence in a test set, and thus to predict the probable anomalous emergence.

In recent years, some data mining researches try to decide the above mentioned problem by the development of new techniques on the basis of soft computing and machine learning incorporation. These techniques utilize neural networks [9], fuzzy sets [10] and artificial immune systems [11]. It should be noted that one of the popular cores of anomaly detection techniques is stochastic modeling, which allows for deciding the prediction task when uncertainty factors of stochastic type are presented. Here, Markov reward models should become one of the most common techniques for stochastic uncertainty description. The proposed technique also uses the Markov reward model as a main core for behavior profile construction.

2.2. Markov reward model. Markov reward model (also called Markov reward process) can be denoted by a tuple:

$$\{S,\ P,\ R\} \tag{1}$$

where $S = \{s_i\}$ $(i \in [1, n])$ is state space, $P = \{p_{i,j}\}$ is transition probability matrix and $R\colon x \to r(x)$ is reward transition function represented by the reward vector with the length of $|S|$.

Let $X = \{x_t \mid t \in \mathbb{N}\}$ be the discrete stochastic process. This process is considered as generated by the Markov chain if it satisfies to the following assumptions [12]:

- the probability distribution of the state at time t depends on the state at time t–1 and does not depend on the previous states leading to the state at time t;
- a state transition from time t to time $t + 1$ is independent of time.

In other words, a transition probability satisfies the following property:

$$\begin{aligned} &P(x_t = s_i \mid x_{t-1} = s_j, x_{t-2}, \ldots, x_1) = \\ &= P(x_t = s_i \mid x_{t-1} = s_j) = p_{ij} \end{aligned}. \tag{2}$$

The complete matrix P is presented as follows:

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots \\ p_{21} & \ddots & p_{n(n-1)} \\ \vdots & p_{(n-1)n} & p_{nn} \end{pmatrix}. \tag{3}$$

Each element of the matrix P in case of discrete time is computed in the following way:

$$p_{ij} = \frac{c^2{}_{ij}}{c^1{}_i}, \tag{4}$$

where $c^2{}_{ij}$ represents the support of transition from s_i to s_j and $c^1{}_i$ represents the support of the single state s_i.

Classical approach considers support of pattern (state, transition) to be a number of occurrences of this pattern in the initial time series X. Obviously, the training phase suggests the increasing by one for $c^2{}_{ij}$, $c^1{}_i$ and $c^1{}_j$, when the transition $x_{t-1} = s_i$ $x_t = s_j$ is obtained.

It should be noted that elements of matrix P conform to the following rules:

$$\begin{aligned} &\forall i \in [1,n], \sum_{j=1}^{n} p_{ij} = 1 \\ &\forall i, j \in [1,n], 0 \le p_{ij} \le 1 \end{aligned}. \tag{5}$$

For the sequence $Y = y_1, y_2, \ldots, y_T$, the reward function R can be defined as

$$r(x) = \begin{cases} 1, & \text{if } Y \text{ is specific}, x = y_T \\ 0, & \text{if otherwise} \end{cases}. \tag{6}$$

Methodology of preventing anomaly detection based on Markov reward modeling analyses the probability $P_a(x)$ of evolution of a specific (or anomalous) sequence from the observed state x [13], i.e., the testing phase suggests the computing of future occurrence probability for the sequence which starts from the observed state x and terminated by the anomalous state x_T, i.e.

$$P_a(x) = P\big((x_1, x_2, \ldots, x_T) \in A(x) \mid x_1 = x\big), \tag{7}$$

where $A(x)$ is the set of specific sequences.

In [13], authors prove that the problem of computing probability of a specific pattern evolving from the observed state can be decided by discovering the value of function for prediction of future Markov rewards:

$$P_a(x) = \sum_i P\left(x_{i1}, x_{i2}, \ldots, x_{iT(i)} \mid x_{i1} = x\right) \cdot r\left(x_{iT(i)}\right), \tag{8}$$

where $P(x_{i1}, x_{i2}, \ldots, x_{iT(i)} \mid x_{i1} = x)$ is the probability that sequence $\{x_{i1}, x_{i2}, \ldots, x_{iT(i)}\}$ with the length of $T(i)$ and the initial state x may be observed with.

If Markov assumptions of a process are taken into account, equation (8) can be described by computing the probability of transition from the current state to anomalous one. It is mathematically represented in the following form:

$$P_a(x) = \sum_j p_{ij} r(s_j). \tag{9}$$

In this case, a state is considered as anomalous when a probability exceeds the threshold μ, which is human-established.

Efficacy of this stochastic model is decreased when non-Markov transitions occur as well as appearance of anomalous rewards, which are referred to as linguistic uncertainties [14]. In this connection, the necessity for development classical Markov reward model arises.

2.3. Temporal-difference learning approaches for Markov reward modeling. The particular ways to decide the problem development for Markov reward processes are presented in [13, 15]; authors present the temporal-difference learning based algorithms for Markov modeling. The main idea of temporal-difference learning is to update rewards and probability characteristics for an observed state based not only on previous, but also on consecutive states, which were observed in the past. It can be described as follows.

Let the classical Markov transition support (here and hereafter, denote each parameter a in the time of t as $a(t)$) be computed by the next equation when the new state is observed:

$$c_{ij}^2(t) = \begin{cases} c_{ij}^2(t-1) + 1, & \text{if } x_t = s_i \text{ and } x_{t+1} = s_j \\ c_{ij}^2(t-1), & \text{if otherwise} \end{cases}. \tag{10}$$

From the temporal-difference perspective, the support of transition from s_i to s_j is sensitive not only when the time difference between them is 1 ($\Delta t = 1$), but also when $\Delta t > 1$, i.e

$$\forall \delta \in [0, 1, \ldots, t]$$

$$c_{ij}^2(t) = \begin{cases} c_{ij}^2(t-1) + 1, & \text{if } x_{t-\delta} = s_i, x_{t+1} = s_j, \delta = 0 \\ c_{ij}^2(t-1) + \lambda^\delta, & \text{if } x_{t-\delta} = s_i, x_{t+1} = s_j, \delta > 0 \\ c_{ij}^2(t-1), & \text{if otherwise} \end{cases}, \tag{11}$$

where $\lambda \in [0, 1]$ is a bias-variance parameter, which defines the continuity of a process (when the bias-variance is zero, the continuity is Markovian).

Similarly, the single state support may be computed:

$$\forall \delta \in [0, 1, \ldots, t]$$

$$c_i^2(t) = \begin{cases} c_i^2(t-1) + 1, & \text{if } x_{t-\delta} = s_i, \delta = 0 \\ c_i^2(t-1) + \lambda^\delta, & \text{if } x_{t-\delta} = s_i, \delta > 0 \\ c_i^2(t-1), & \text{if otherwise} \end{cases}, \tag{12}$$

To avoid confusion, the background of temporal-difference learning [13, 15] state that transition probability, which is computed by (4), in case of temporal-difference learning should be denoted as A.

The reward function is also temporal-difference learnt (denote the temporal-difference reward vector as B). It is computed as follows:

$$\forall \delta \in [0, 1, \ldots, t]$$

$$B_i(t) = \begin{cases} B_i(t-1) + r(x_t), & \text{if } x_{t-\delta} = s_i, \delta = 0 \\ B_i(t-1) + \lambda^\delta \cdot r(x_t), & \text{if } x_{t-\delta} = s_i, \delta > 0 \\ B_i(t-1), & \text{if otherwise} \end{cases}, \tag{13}$$

In this case, a reward function is defined as the function, which characterizes the closeness of reward (or anomalous) state to previous ones.

Temporal-difference learning also changes the definition of probability from (9). It states that current reward is defined not only by the previous state, but also by the state sequence in the past; it is computed as follows:

$$P_a(x) = \sum_j A_{ij} B_j. \tag{14}$$

To decide the problem of random fluctuations, a memory of past state may be incorporated into the prediction model [16]:

$$P_a(x) = \sum_j A_{ij} B_j + \alpha \cdot P_a(x_{t-1}), \tag{15}$$

where $\alpha \in [0, 1]$ is memory rate.

One of the key shortcomings is rigid adjustment of the technique that sometimes does not allow for emphasizing the patterns which highly affect to anomalous states. This shortcoming takes place because of strict power polynomial nature of both bias-variance parameter and memory rate. It can be graphically illustrated in Fig. 1. Here, the addition ΔB is shown for each state x_t (Fig. 1a) when the anomalous state is observed in time T (Fig. 1b). In this case, it is difficult to emphasize states lying

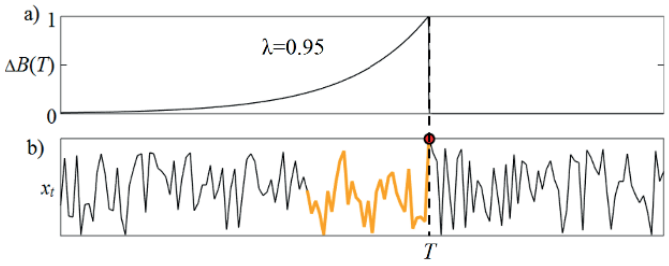

Fig. 1. The additional rewards in case of anomalous observation

in the specific pattern without affecting the weights of the remaining states. One decision is to make the general so-called "reward function", which can not only occupy the power type (which is used by temporal-difference learning), but also provide other kinds of reward functions.

3. Fuzzy form of Markov reward process

3.1. Fuzzy temporal relations. Let the temporal relation τ^k for the temporal set $X = \{x_t\}$ ($t \in [1, N]$) within state space S be defined for the observed time t as follows:

$$g\tau_k q \Leftrightarrow (g = x_t) \& (q = x_{t-k}), \tag{16}$$

where q and g are observed states at time t and $t-1$, respectively.

The relation (16) means "The states q and g are separated by k time steps in time period".

Model of temporal scenario can be computed for the observed time t as follows:

$$\Phi = \&_{i=1}^{t-1} x_i \tau^{t-i} q . \tag{17}$$

Particular presentations of past for an observed process may be modeled by emphasis on particular conjuncts from (17). Here, the focus is on the estimation of the optimal scenarios, which allow to correctly adjust the parameters of Markov reward model based on the past [17]. Fuzzy interpretation of (16) can be used to solve this problem.

Fuzzy interpretation of temporal relation can be produced if parameter k from (16) is replaced by fuzzy value. In particular, if fuzzy value ≈1 "approximately one" is taken instead of k (the membership function is $\mu_{\approx 1}(k)$) then the fuzzy relation φ_1: "in immediate past" is produced. The fuzzy relation is defined by membership function μ_φ within pair set $S \times q$. In this case, the membership of pair (g, q) ($g = x_i$, $i \in [1, t]$) is computed as follows:

$$\mu_{\varphi_1}(g,q) = \mu_{\approx 1}(t-i). \tag{18}$$

The temporal relation φ_k "in several previous steps" is produced if k is reduced by fuzzy interval value, which reflects intuitive ideas of human experts about the qualitative value "several steps".

In general, the system $T = \{\varphi_{z1}, \varphi_{z2}, \ldots, \varphi_{zk}\}$ ($z_i \in [1, N]$) may be used. Each element from T characterizes the time interval "approximately z_j". The membership function is produced for each fuzzy relation φ_{zk} and computed by the following equation:

$$\mu_{\varphi_{z_j}}(g,q) = \mu_{\approx z_j}(t-i), \tag{19}$$

where is the membership function for fuzzy value "approximately z_j".

Fuzzy model of temporal scenario, which reflects the past evolution of an observed process relatively to the state $q = x_t$, can be computed as follows:

$$\Phi = \&_{i=1}^{t-1} \&_{j=1}^{|T|} x_i \varphi_{z_j} q . \tag{20}$$

Before equation (20) is applied, the procedure of preprocessing should be provided by a human expert to emphasize on interesting events in past and eliminate insignificant conjuncts.

Markov model corrections are made based on past and described by production rules of the following form:

$$\text{IF } G \text{ THEN } \Delta, \tag{21}$$

where G is fuzzy model of temporal scenario at time t and Δ is real value, which defines the correction for a Markov parameter (transition probability, support, reward, etc.).

Correction rules are produced by human expert based on his intuitive ideas about the temporal correlations between process states. Here, the antecedents are special variants of temporal scenarios which affect stochastic outcomes, thus breaking Markov assumptions.

3.2 Markov chain with fuzzy production rules. The generalization of temporal-difference learning approach can be done by incorporation of data which describes the non-Markov dynamics of analyzed process, as well as by integration of human expert information which comes from intuitive knowledge about anomalous occurrence.

One of the ways for this problems decision is the foundation of hybrid fuzzy-stochastic model by merging the above described Markov model with fuzzy production model mentioned in this paper.

When fuzzy production rules are incorporated into Markov model, it is represented by the following quadruple tuple:

$$\{S, P, R, \Pi\}, \tag{22}$$

where Π is a set of fuzzy production rules used for Markov model correction.

Let Π contain four fuzzy rules, which are in form (21) and are defined by the apparent human considerations:

$$\text{IF } g\varphi_{\approx 1} q \text{ THEN } \Delta_i \,\&\, \Delta_{it}, \tag{23}$$

$$\text{IF } g\varphi_{\tilde{m}} q \text{ THEN } -\Delta_i \,\&\, -\Delta_{it}, \tag{24}$$

$$\text{IF } g\varphi_{\approx 1} q \text{ THEN } \Delta_{R_i}, \tag{25}$$

$$\text{IF } g\varphi_{\tilde{m}} q \,\&\, t \in A(t) \text{ THEN } -\Delta_{R_i} \tag{26}$$

where q is an observed state; $g = x_i$ ($i \in [1, t-1]$) is a state in the past of q; Δ_i is a value representing the correction for support of state $s_a = g$; Δ_i is a value representing the correction for support of transition from $s_a = g$ to observed state $s_b = q$; is a fuzzy value "long time"; $A(t)$ is a set of time indexes, which are labelled as anomalous by human expert and Δ_{Ri} is a value representing the correction for reward of state $s_a = g$.

The membership functions in general case for all fuzzy values may be represented by Gaussian function (Fig. 2). It should be noted that power form of the membership function leads to temporal-difference equations discussed above.

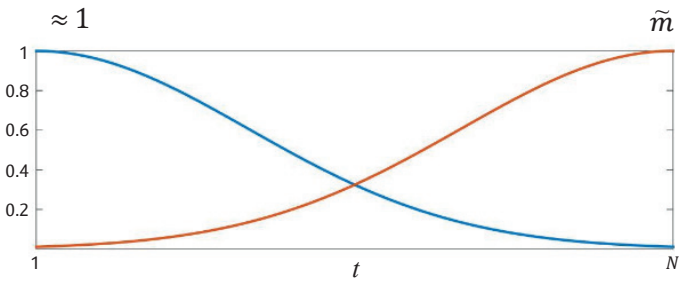

Fig. 2. Utilizing fuzzy membership functions

Based on above mentioned, it can be concluded that when a new state is observed, fuzzy rules mechanism update rewards and supports for each state and transition.

To make a prediction of future rewards robust to non-Markov situations, the following fuzzy rule for anomalous probability can be used:

$$\text{IF } g\varphi_{\approx 1}q \text{ THEN } \Delta_{i_{P_a(x_t)}}, \tag{27}$$

where $\Delta_{i_{P_a(x_t)}}$ is a value representing the correction for probability of transition from observed state q to anomalous one based on its relation with state in the past $g = x_i\,(i \in [1, t-1])$.

Therefore, the probability of transition from observed state to anomaly is computed as follows:

$$P_a(x_t = s_i) = \sum_j p_{ij} r(s_j) + \sum_{k=1}^{t-1} \Delta_{k_{P_a(x_t)}}. \tag{28}$$

Based on the above mentioned description, it can be concluded that presented technique is a theoretically generalized form of temporal-difference learning approach, and hence, it has more robustness for dynamics than non-Markov processes with regard to specific pattern emphasis. Moreover, it can be carefully adjusted because of human expert knowledge incorporation, and hence, it may find wider application than in case of original temporal-difference framework.

4. Computational experiments

4.1 Intrusion detection. The experiments with system calls collected from *MIT* and *UNM*, which are often used for stochastic models benchmarking, were performed to prove the presented framework is generalized form of temporal-difference learning and can be reduced [18]. These databases include normal data, i.e. traces of programs obtained from computer system usage by real users, and different kinds of multi-stage cyber-attacks (buffer overflows, symbolic link attacks, Trojan programs, etc.). We chose two databases for our research. The first one was collected from *MIT* and second one was from *UNM*. Both are called *live lpr*. Table 1 shows the main details of the data.

To make the benchmarking similar to previous experiments, the data was divided into two groups: one for training and the other one for testing [13, 15]. As for estimation, true detection rate *TDR* and false detection rate *FDR* were used. These rates are computed as follows:

Table 1
MIT and *UNM* datasets characteristics

Property	MIT	UNM
Total number of normal traces	2207	1231
Total number of attack traces	1001	1001
Total number of system calls	2746655	717568
Sequence of calls per one state	6	6
Number of normal train sequences	10	10
Number of attack train sequences	20	20
Number of normal test sequences	2207	1231
Number of attack test sequences	1001	1001

$$\begin{aligned} TDR &= n_{ad} / n_a \\ FDR &= n_{normd} / n_{norm} \end{aligned}, \tag{29}$$

where n_{ad} is the number of correctly identified abnormal traces, n_a is the number of abnormal traces, n_{normd} is the number of normal traces that have been incorrectly identified as anomalies and n_{norm} is the number of normal traces.

All the experiments were implemented by using C#. The average time of the calculations for one sequence was 36 μs. The membership functions for relation "in immediate past" and "in long previous time" were taken in power form:

$$\mu_{\approx 1}(x) = \lambda^x, \tag{30}$$

$$\mu_{\tilde{m}}(x) = \lambda^{N-x}, \tag{31}$$

where λ is a bias-variance parameter, which is described above and N is a length of trace, which is considered as normal.

To make the presented framework be the same as the last form of temporal-difference learning approach [15], utilizing values were established as λ = 0.995 for *MIT* and λ = 0.95 for *UNM*. For both *MIT* and *UNM* $N = 1000$.

The results show the presented technique allows to reach 99.8% of *TDR* when the *FDR* is zero for *MIT* and 100% of *TDR* when *FDR* is 1.29%. Therefore, it is computationally proved that the new framework can be reduced to temporal-difference learning one.

4.2. Fault prediction. To show that the presented technique allows not only to detect anomalous sequences in databases, but

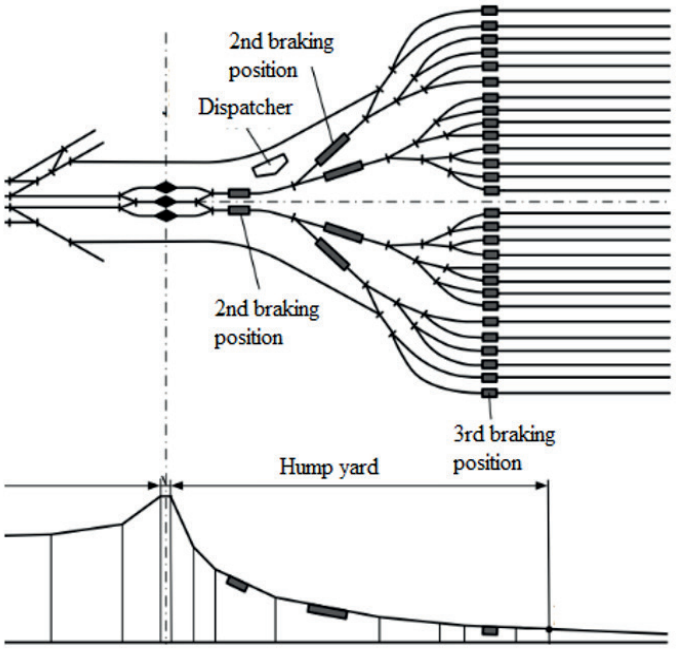

Fig. 3. Hump yard of Russian railway

also to predict forthcoming anomalous unexpected events, this subsection describes the problem of fault prediction decision for rail hump yards (Fig. 3) [19].

Here, the fault may appear when cars with big weight and speed overtakes cut with cars with lower weight and speed. In this case, both kinds would be on one track. To prevent this, dispatcher should adjust braking position based on intuitive ideas. As empirical experiments show, the dispatchers usually do not find a way to prevent these faults. To solve this problem, a decision support system should be developed. Therefore, proposed technique can be a good basis for this system.

To present a temporal scenario of process on rail yard, the following quadruple tuple may be used:

$$\{D, \Delta V, W_1, W_2\}, \tag{32}$$

where D is distance between cuts, m; ΔV is speed difference between cuts, m/s; W_1 is resistance to movement of back cut, ‰ and W_2 is resistance to movement of front cut, ‰.

Speed difference is computed as follows:

$$\Delta V = V_1 - V_2, \tag{33}$$

where V_1 is speed of back cut, m/s and V_2 is speed of front cut, m/s.

To avoid the complicated analysis of multidimensional temporal sets, the following convolution is defined. Let the tensity of situation on hump yard be defined as the certain variable x_t. The value of zero characterizes optimal conditions when a hump yard process is in normal mode. In contrast, the value of one show that fault is observed. The Mamdani inference used in proposed experiments to produce this variable. Here, the term sets are represented by the following grammars:

$$T_D = T_X = \left\{ \begin{array}{l} \text{VERY SMALL (VS), SMALL (S),} \\ \text{MEDIUM (M),} \\ \text{BIG (B), VERY BIG (VB)} \end{array} \right\}, \tag{34}$$

$$T_{\Delta V} = \left\{ \begin{array}{l} \text{NEGATIVE MEDIUM (NM),} \\ \text{NEGATIVE SMALL (NS),} \\ \text{NEGATIVE VERY SMALL (NVS),} \\ \text{VERY SMALL (VS), SMALL (S),} \\ \text{MEDIUM (M),} \\ \text{BIG (B), VERY BIG (VB)} \end{array} \right\}, \tag{35}$$

$$T_{W_1} = T_{W_2} = \left\{ \begin{array}{l} \text{SMALL (S), MEDIUM (M),} \\ \text{BIG (B)} \end{array} \right\}, \tag{36}$$

Therefore, the intuitive dispatcher idea about the situation on a hump yard may be represented in a form of fuzzy rule system. The system produced during experimental yard (it is a particular system of combination of (34–36) made by human experts) is illustrated in Fig. 4.

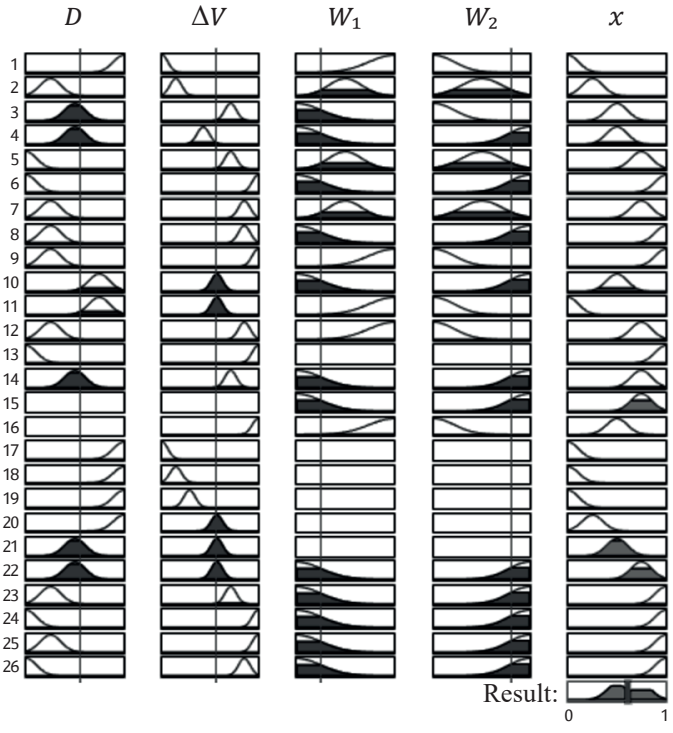

Fig. 4. Fuzzy rules for producing tensity variable

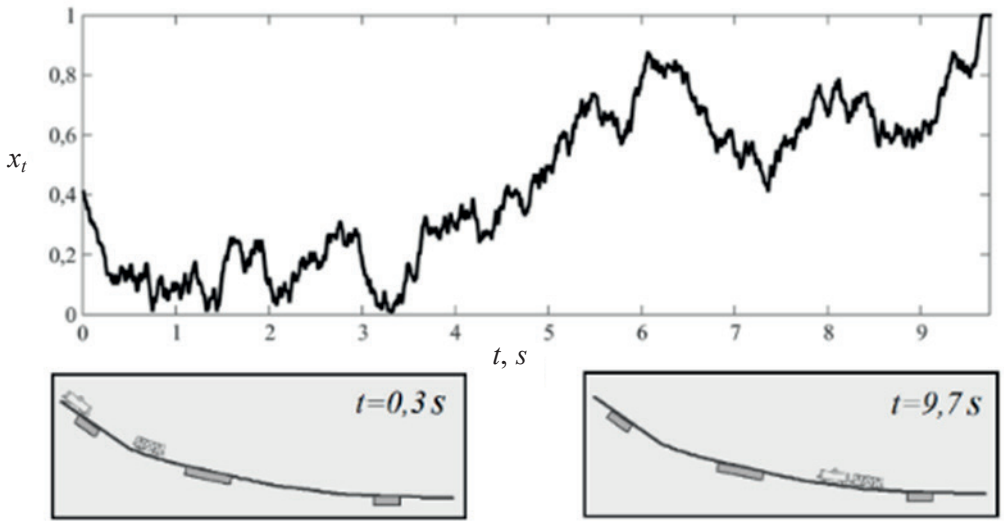

Fig. 5. Time-series representing the overtaking car pair

As a result of Mamdani inference, each pair of cuts is represented in form of curves, which are converged to anomalies (or overtaking situations). The particular overtaking situation is graphically depicted in Fig. 5.

Based on presented technique, the observed time series $X_n = \{x_{t(n)}\}$, where $n = [1, N]$ (N is the general number of pairs) undergo modeling. It was discovered that the rate of faults during human dispatcher work without support is 8%. This value is decreased to 5% when the framework is included into the decision process. It proves that the number of overtaking situations is reduced almost two times.

5. Conclusions and future work

The new framework for anomaly detection is presented, in which fuzzy generalization of temporal-difference approach for Markov reward model learning is proposed. To overcome the weakness of previous approaches, fuzzy interpretation of temporal-difference parameters is applied. It is proved that fuzzy rules not only extend the capabilities for non-Markov process modeling, but also allow to incorporate human expert ideas about observed process. Computational experiments shows the technique may be applied not only for anomaly detection, but also for anomaly prediction.

Future research work is needed to show new and more specific applications of the proposed framework. Particularly, efficacy of other membership functions can be shown. Another way to extend the framework is to emphasize the dependency not only on one state, but also on specific sequences of events, i.e. applying other types of temporal scenarios.

Acknowledgments. This work was supported by the Russian Foundation for Basic Research (Grant No. 16–07–20070-a) and partially supported by Grant of SGS No. SP2016/143, VŠB Technical University of Ostrava, Czech Republic.

References

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys (CSUR)* 41(3), 1–72 (2009).

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey", *Transactions on Knowledge and Data Engineering* 24(5), 823–839 (2012).

[3] S.M. Kovalev, A.N. Guda, and M.A. Butakova, "Hybrid stochastic detection model of specific patterns in temporal data", *Vestnik RGUPS* 3 (51), 36–42 (2013) (in Russian).

[4] R.J. Povinelli and X. Feng, "A new temporal pattern identification method for characterization and prediction of complex time series events", *Transactions on Knowledge and Data Engineering* 15 (2), 339–352 (2003).

[5] S.M. Kovalev and A.V. Sukhanov, "Hybrid stochastic model based detection of specific patterns in time series", *Izvestiya SFesU. Engineering sciences* 4(153), 142–149 (2014) (in Russian).

[6] P. Cunningham, M. Cord, and S. J. Delany, "Supervised learning", *Machine Learning Techniques for Multimedia*, 21–49 (2008).

[7] S.S. Khan and M.G. Madden, "A survey of recent trends in one class classification", *Artificial Intelligence and Cognitive Science*, 188–197 (2010).

[8] Z. Ghahramani, "Unsupervised learning", *Advanced Lectures on Machine Learning*, 72–112 (2004).

[9] M. V. Mahoney and P. K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks", *Proceedings of the 8th ACM SIGKDD international conference on knowledge discovery and data mining*, 376–385 (2002).

[10] I. Aydin, M. Karakose, and E. Akin, "The prediction algorithm based on fuzzy logic using time series data mining method", *World Academy of Science, Engineering and Technology* 51 (27), 91–98 (2009).

[11] E. Zitzler and L. Thiele, "Multiobjective evolutionary algorithms: a comparative case study and the strength Pareto approach", *IEEE transactions on evolutionary computation* 3 (4), 257–271 (1999).

[12] N. Ye et al., "A Markov chain model of temporal behavior for anomaly detection", *Proceedings of the 2000 IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, 171–174 (2000).
[13] X. Xu, "Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies", *Applied Soft Computing* 10 (3), 859–867 (2010).
[14] A.V. Leonenkov, *Fuzzy Simulation in the Environment MATLAB and FuzzyTECH,* BKV, Petersburg, 2005 (in Russian).
[15] A.V. Sukhanov, S.M. Kovalev, and V. Styskala, "Advanced temporal-difference learning for intrusion detection", *13th IFAC and IEEE Conference on Programmable Devices and Embedded Systems PDES* 48 (4), 3–48 (2015).
[16] A. Sukhanov, "Behavior prediction for time series", *Results and Solutions of Young R&S for Innovations and Progress Final Report*, 88–91 (2014).
[17] S.M. Kovalev, A.N. Guda, and A.V. Sukhanov, "Hybrid method based on fuzzy productions for prediction stochastic model learning", Vestnik RGUPS 59 (3), 40–46 (2015) (in Russian).
[18] S. Forrest, *Computer immune systems – data sets*, http://www.cs.unm.edu/~immsec/systemcalls.htm. [accessed 11.12.2014], 2006.
[19] A.N. Shabenikov, A.V. Sukhanov, and S.M. Kovalev, "Intelligent technique for faults prediction on hump yards", *Inženernyj vestnik Dona* 4, http://ivdon.ru/ru/magazine/archive/n4y2015/3334 [accessed 11.11.2015] (2015) (in Russian).