Applied Soft Computing 48 (2016) 404–418

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm

Guan-Yu Hu[a], Zhi-Jie Zhou[b,*], Bang-Cheng Zhang[c,*], Xiao-Jing Yin[c], Zhi Gao[a], Zhi-Guo Zhou[d]

[a] School of Software, Changchun University of Technology, Changchun, Jilin 130012, PR China
[b] High-Tech Institute of Xi'an, Xi'an, Shaanxi 710025, PR China
[c] School of Mechatronic Engineering, Changchun University of Technology, Changchun, Jilin 130012, PR China
[d] Department of Radiation Oncology, The University of Texas Southwestern Medical Center, Dallas, TX 75235, USA

ARTICLE INFO

Article history:
Received 28 December 2014
Received in revised form 1 April 2016
Accepted 28 May 2016
Available online 20 June 2016

Keywords:
Network security situation prediction
Hidden behavior
Belief rule base (BRB)
Covariance matrix adaption evolution strategy (CMA-ES)
Modified operator

ABSTRACT

It is important to establish the forecasting model of the network security situation. But the network security situation cannot be observed directly and can only be measured by other observable data. In this paper the network security situation is considered as a hidden behavior. In order to predict the hidden behavior, some methods have been proposed. However, these methods cannot use the hybrid information that includes qualitative knowledge and quantitative data. As such, a forecasting model of network security situation is proposed on the basis of the hidden belief rule base (BRB) model when the inputs are multidimensional. The initial parameters of the hidden BRB model given by experts may be subjective and inaccurate. In order to train the parameters, a revised covariance matrix adaption evolution strategy (CMA-ES) algorithm is further developed by adding a modified operator. The revised CMA-ES algorithm can optimize the parameters of the hidden BRB model effectively. The case study shows that compared with other methods, the proposed hidden BRB model and the revised CMA-ES algorithm can predict the network security situation effectively to improve the forecasting precision by making full use of qualitative knowledge.

1. Introduction

Network security situation can reflect the network status [1], and it is the important information of the active defense in the network. In order to determine the network status and make the accurate decision, it is necessary to predict the network security situation. There are two characteristics when the network security situation is predicted. Firstly, the network security situation cannot be observed directly and only be measured by other observable data such as attack type and attack strength. In other words, the network security situation can be considered a hidden behavior. Secondly, the available information includes qualitative knowledge and quantitative data when the network security situation is predicted.

In order to establish the forecasting model of the network security situation, three types of methods that include analytical model-based method, data-driven based method, and qualitative knowledge based method have been proposed. In the analytical model-based method, some predictors are firstly developed from the corresponding filters that include Kalman filter [2], strong tracking filter [3], particle filter [4] and so on. Then these predictors and the observable data are used to predict the hidden behavior. In the data-driven based method, the observable data and the corresponding methods are used directly to establish the forecasting model the characteristic value that can reflect the hidden behavior. The data-driven method includes hidden Markov model (HMM) based method [5–8], grey theory based method [9], dynamic Bayesian network (DBN) based method [10,11], and Wavelet neural network (WNN) based method [12]. The qualitative knowledge based method that includes expert system based model [13], Petri net based model [14] and so on can be adopted to establish the forecasting model of the hidden behavior.

However, the limitations are existed in the above methods. The analytical model-based method is not suitable when the analytical model of a complex system cannot be established. The qualitative knowledge based method mainly uses the qualitative knowledge and the forecasting results may be inaccurate. In the HMM based method, the probability of observation only depends on the current state of the system. The grey method can only reflect the trend of the

* Corresponding authors.
E-mail addresses: zhouzhijie1978@163.com, zhouzj04@mails.tsinghua.edu.cn (Z.-J. Zhou), zhangbangcheng@mail.ccut.edu.cn (B.-C. Zhang).

http://dx.doi.org/10.1016/j.asoc.2016.05.046
1568-4946/© 2016 Elsevier B.V. All rights reserved.

Nomenclature

Acronym

BRB	Belief rule base
CMA-ES	Covariance matrix adaption evolution strategy
HMM	Hidden markov model
DBN	Dynamic Bayesian network
WNN	Wavelet neural network
MSE	Mean square errors
SQP	Sequential quadratic programming
PSO	Particle swarm optimization
EvHMM	Evidential hidden markov model

Notation

$x(t)$	Hidden behavior at time instant t
t	Time instant
R_k	kth rule in BRB
D_k	Consequent of the kth rule
G	Good security situation level
O	Common security situation level
W	Warning security situation level
T	Terrible security situation level
$\beta_{j,k}$	Belief degree of D_j
$\beta_{D,k}$	Remaining belief degree
θ_k	Rule weight of the kth rule
δ	Weight of the attribute
w_k	Activation weight of the kth rule
a_k	Matching degree of the input in the kth rule
$\mathbf{y}(t)$	Observable data in time instant t
f	Observation equation
ϕ	Parameters of the observation equation
$\boldsymbol{\nu}(t)$	Noise vector of the observation equation
A	Parameter of the observation equation
B	Parameter of the observation equation
σ	Parameter of the observation equation
H	Likelihood function
Ω	Parameter vector of the BRB model
l	Number of parameters in Ω
T	Maximum time instant
$U(D)$	Utility of the evaluated degrade
q	qth solution of CMA-ES
λ	Population size of CMA-ES
g	Generation of CMA-ES
m	Mean value of population of CMA-ES
S	Step size of CMA-ES
$\mathbb{N}$	Normal distribution
C	Covariance matrix of CMA-ES
Ex	Excess value in modified operator of CMA-ES
τ	Offspring population size of CMA-ES
h	Weight coefficient of CMA-ES
$\Omega_{i:\lambda}$	ith individual in the λ individuals of CMA-ES
E	Orthogonal matrix
I	Identity matrix
F^2	Diagonal matrix
c_1, c_2	Learning rate for updating the covariance matrix
τ_{eff}	Variance effective selection mass of CMA-ES
p_c	Evolution path of CMA-ES
c_c	Backward time horizon of the evolution path
d_σ	damping parameter of the evolution path
c_σ	backward time horizon of the conjugate evolution path
p_σ	Conjugate evolution path of CMA-ES
$E\Vert\mathbb{N}(0, I)\Vert$	Expectation of the Euclidean norm
$\mathbb{N}(0, I)$	Distributed random vector
Ω_{best}	Best solution of CMA-ES

network security situation. The DBN method is an important tool to deal with uncertain information, but it is too hard to complete the training of DBN model. Therefore, the current methods cannot use the hybrid information effectively to predict the hidden behavior.

In order to solve the above problems, a new model has been proposed by Zhou et al. on the basis of belief rule base (BRB). In particular, the proposed model is named as the hidden BRB model and has been applied in the prediction of gyro drift in the navigation system [15] and other fields [16–19]. The initial parameters of the hidden BRB model are given by experts and the expert knowledge plays an important role at establishing a nonlinear relationship between antecedent attributes and an associated consequent. However, the hidden BRB model was only used to predict the hidden behavior when the input is one-dimensional.

Although the network security situation is a hidden behavior, it can be reflected by some other observable data. In this paper, three types of attack data of a web server in 2013 are chosen as the observable data. As such, the hidden BRB model is extended so that the multidimensional inputs can be dealt with. Then the extended hidden BRB model is used to predict network security situation, and the referential points including good (G), common (O), warning (W) and terrible (T) are assigned to security situation. The qualitative knowledge and observable data are used to establish the belief rules, and the initial parameters of belief rules are given by experts.

The initial parameters given by experts may be subjective and inaccurate. Therefore it is necessary to train the parameters by using optimization algorithm. In particular, the likelihood function is constructed to estimate the parameters on the basis of the observable data. In order to optimize the likelihood function, the traditional optimization algorithms that are given in Matlab Optimization Toolbox have been used to train the parameters of the hidden BRB model when the inputs are single-dimensional [15]. But when the inputs are multidimensional, the traditional optimization algorithms are easy to fall into the local peak, and the optimal parameters cannot be obtained. As such, a revised covariance matrix adaption evolution strategy (CMA-ES) algorithm is developed further in this paper. In the revised CMA-ES algorithm, the modified operator is used to handle the constraints in the forecasting model of network security situation. A novel leaky bucket mechanism is introduced in the modified operator. By filtering out the excess part, the parameters of the hidden BRB model can meet the constraints through the iterations. When the iteration stops, the optimal solution will be used as the trained parameters of the forecasting model, then the trained hidden BRB model can be used to forecast the network security situation. The experimental results show that the revised CMA-ES algorithm is an effective and robust approach for optimizing the hidden BRB model.

The paper is organized as follows. In Section 2, the problem for network security situation prediction is formulated. In Section 3, the revised covariance matrix adaption evolution strategy is further developed by adding a modified operator. In Section 4, a numerical example for predicting the network security situation is given, and the simulation results are analyzed. Finally, this paper is concluded in Section 5.

2. The hidden BRB model for network security situation prediction

2.1. Problem formulation

As mentioned above, network security situation is a hidden behavior of network platform. Fortunately, the network security situation can be measured by some other security factors. These