Genetic Gray Wolf Improvement for Distributed Denial of Service Attacks in the Cloud

Preprint *in* Journal of Computational and Theoretical Nanoscience · September 2018

DOI: 10.1166/jctn.2018.7463

1 author:

Velliangiri Sarveshwaran
SRM Institute of Science and Technology

Journal of
Computational and Theoretical Nanoscience
Vol. 15, 1–6, 2018

Genetic Gray Wolf Improvement for Distributed Denial of Service Attacks in the Cloud

S. Velliangiri[1,*], R. Cristin[1], and R. Karthikeyan[2]

[1] *Department of CSE, GMR Institute of Technology, Rajam, Andhra Pradesh, India*
[2] *Department of CSE, Karunya University, Coimbatore, Tamil Nadu, India*

In cloud service provider to lease space on their physical and virtual structures. Denial of Service (DoS) strikes weakens the limit of the cloud to respond to clients requests, which realizes broad money related disasters. Distributed Denial of Service (DDoS) strikes are one of the genuine risks and conceivably the hardest security issue for the present web. In this paper proposes GA (Genetic Algorithm) with Gray wolf improvement (GWO) for recognizing the DDoS assaults in an automatic way. The Proposed method named as Genetic Gray wolf optimization. Using a genetic algorithm to adjust the weights and width of RBF neural system; it picks better approaches for hybrid encoding and improving at the same time. However the optimization of connection weights is not complete; we have to utilize Least Mean Square (LMS) algorithm for additionally inclining, a variant of Gray wolf optimization is presented. The proposed method is assessed by experimentation techniques to sort out coming about systems. DARPA 99 Datasets are utilized to assess the execution of the proposed technique by accuracy and false positive Value. Moreover, the execution measurements are demonstrated preferable outcomes over existing techniques.

Keywords: Gray Wolf Optimization, Radial Basis Function, Genetic Algorithm, Denial of Service.

RESEARCH ARTICLE

1. INTRODUCTION

Cloud Computing is used to provide the services through internet and its act of utilizing a remote server (web) or network of remote servers facilitated on the Internet to store, oversee, and process information, as opposed to nearby capacity arrangements. There are three types of cloud services provided by vendors. These services are Infrastructure as a service (IaaS), Platform as a service (IaaS) and Software as a service (SaaS). There are three ways to implement the cloud computing. These options are public cloud, private cloud, and hybrid cloud. In recently cloud computing has seen amazing growth in each sector. From the earliest starting point there have been numerous advantages of cloud computing, for example, bring down equipment costs, higher adaptability, and expanded cooperation. In spite of these advantages, amid its initial years, cloud computing was not embraced so promptly in view of security concerns.[1–2]

Despite the fact that cloud computing is focused to give better use of assets utilizing virtualization methods and to take up a significant part of the workload from the customer, it is loaded with security dangers. Most serious threats are distributed denial of service assault which is anything but difficult to actualize and full of feeling. DDoS (Distributed Denial of Service) is a cloud-particular assault in which assault source is constantly more than one; numerous machines assaults on a client by sending more packets with huge data and its leads to overhead. Such assault leads to resources unavailable to the client by overpowering the system with undesirable movement.[3–4]

Distributed Denial of Service (DDoS) assaults utilizes generally disseminated zombies to send a lot of movement to the objective framework, hence keeping honest to goodness clients from getting to arrange assets. In a previous couple of years, DDoS assaults have broadly undermined the Internet. For instance, as per an overview from Neustar, the half of the reviewed organizations had endured a DDoS assault in 2014 and mid-2015, and 54% of the assaulted organizations had been assaulted no less than six times. What's more, it was accounted for that a DDoS assault against BBC destinations in January 2016 achieved 602 gigabits for each second and "brought them down at any rate for three hours." McAfee Inc. detailed that cybercrime is costing the world roughly one trillion dollars consistently. Along these lines, anticipating DDoS assaults not exclusively is by and large generally looked into for the present Internet, yet in addition has turned into an essential target in outlining the future Internet.[4–8]

*Author to whom correspondence should be addressed.

Radial basis function neural networks (RBFNNs) as a sort of capable kernel methods have been connected to numerous territories with progress. The hypothetical investigation of RBFNN structures and algorithms incorporates the orthogonal least square algorithm, the guessability examination, the outline of RBFNN structure utilizing fuzzy clustering technique, the mistake bound assessment, the advancement of RBFNN the structure utilizing kernel orthonormalization strategy or together with supervised and unsupervised learning method.[9–10] Evolutionary computation has additionally been utilized for choosing factors for RBFNNs and for improving RBFNN training. The transient consistency of RBFNN was utilized to foresee reverse channel yield and it was discovered that the coefficients of a constructed RBFNN with mistake limited are indistinguishable to those of an obscure framework.[11–15]

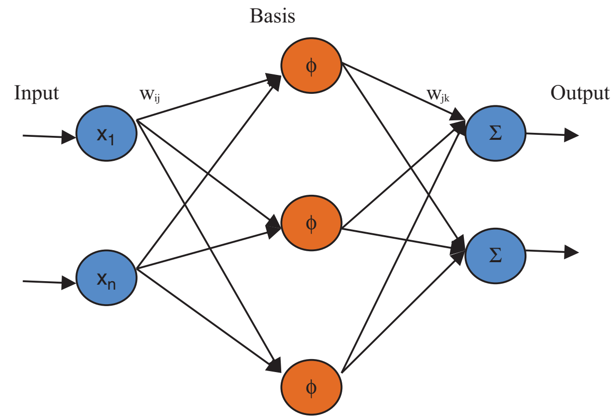

Fig. 1. Structure of radial basis function neural network.

2. RELATED WORK

The author developed two critical enhancements for the Three-Phased PSO with OSD RBFNN. Preliminary changes are presented another rendition of PSO algorithm for deciding the centres of the RBFNN units which expanded both global and local inquiry capacities of the PSO and together with speed of convergence. At that point another strategy for deciding the widths of the RBFNN was proposed in which spatial data of the information and nonlinearity of the capacity to be approximated was considered. The trial comes about demonstrated that applying every one of the changes independently caused expanding the execution of the classifier.[16]

The author proposed another algorithm that utilizations GA to enhance the RBF neural system structure (concealed layer neurons) and associate weight all the while and after that utilization LMS strategy to modify the system further. The new method optimized the quantity of the concealed neurons and in the meantime totally optimized the association weights. Newer method takes longer running time in hereditary algorithm optimization; however it can diminish the time which is spent in building the system. Through these two investigations examination, the outcomes demonstrate that the new calculation significantly enhances in speculation ability, operational productivity, and characterization accuracy of RBF neural system.[17] The Author investigated and discussed about nature-inspired algorithm and proposed a novel optimization for enhancement issues. By and large, unwavering quality enhancement issues are exceptionally unpredictable in nature and NP-hard from the computational perspective. Subsequently, they are especially hard to tackle as contrasted and general nonlinear streamlining issue. The outcomes acquired by GWO for the perplexing extension and LSS in the space container demonstrate that GWO has elite on complex dependability improvement issues. Besides, the similar examination with the writing having similar issues demonstrates that GWO algorithm has better proficiency as it can give an answer that is either better or tantamount than the best accessible outcomes. Accordingly, GWO is ended up being a promising and practical device to tackle the unwavering quality distribution streamlining issues. Presently, the creators are exploring various changes and expansions identified with the benchmark issues in unwavering quality streamlining field.[18]

3. METHODOLOGY

3.1. Generalized Radial Basis Function Neural Network

Assume that system has n inputs and m yields, the shrouded layer has s neurons, the association weight between the input layer and the concealed layer is w_{ij}, and the association weight between the shrouded layer and yield layer is w_{jk}. The preparation procedure of RBF system can be separated into two stages; the initial step is to figure out how to distinguish the weight w_{ij} without instructor, and the second step is to recognize the weight w_{jk} with educator.[17] It is a key issue to recognize the quantity of the concealed layer's neurons; for the most part it begins to prepare from 0 neurons; the shrouded layer neuron is expanded naturally by checking the blunder and rehashes this procedure until the point that the asked for accuracy or the biggest number of concealed layer's neurons is accomplished.

3.2. Genetic Algorithm

Genetic algorithm begins from a populace of spoke to potential arrangement set; be that as it may, the populace is made out of a specific number of encoded quality genes, which are the substances with trademark chromosome. Main principle issues of building the genetic algorithm are the feasible encoding strategy and the outline of genetic operator. Looked with changed advancement techniques, we have to utilize distinctive encoding strategy and genetic operator of various activity, so they and the level of the comprehension of the issues to be settled are the principle point deciding if the use of hereditary methods can succeed.

3.3. Gray Wolf Optimization

The Grey wolf Optimization (GWO) techniques is a populace based metaheuristic algorithm reproduces the initiative chain of significance and chasing technique of dark posers by Mirjalili et al. in 2014.[19] The numerical model for the GWO, the fittest arrangement is known as alpha α. e beta β and delta δ are streamlined in the second and third best arrangements respectively. In order to that rest of the applicant arrangements are thought to be known as omega ω. GWO techniques are chasing and hunting is guided by α, β, δ, and ω take after these three applicants. All together for the pack to chase a prey they initially surrounding it. In a request to mathematically model encompassing behavior, the following Eqs. (6)–(9) are utilized

$$\vec{X}(t+1) = \vec{X}_p(t) + \vec{A} \cdot \vec{D} \tag{1}$$

Where $\vec{X}$ is the grey wolf position, $\vec{X}_P$ is the prey position, $\vec{A}$ and $\vec{C}$ are co-efficient vectors, t is the iteration number $\vec{D}$ is as expressed in Eq. (2),

$$\vec{D} = |\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)| \tag{2}$$

In Eqs. (8) and (9) are used to calculate the vectors of the $\vec{A}$, $\vec{C}$

$$\vec{A} = 2a \cdot \vec{r_1} - a \tag{3}$$

$$\vec{C} = 2\vec{r}_2 \tag{4}$$

Where is an linearly diminished from 2 to 0 through the span of emphasess, and r_1, r_2 are irregular vectors in [0, 1]. The chase is normally guided by the alpha. The beta and delta may likewise take an interest in chasing infrequently. So as to scientifically mimic the chasing conduct of grey wolfs, the alpha (best applicant solution), beta (the second best competitor solution), and delta (the third best hopeful solution) are accepted to have better learning about the potential location of prey. The initial three best applicant arrangements got up until this point and oblige the other hunt operators (including the omegas) to refresh their situations as per the situation of the best pursuit specialists. So the refreshing for the wolves positions is as in Eq. (5):

$$\vec{X}(t+1) = \frac{\vec{X_1} + \vec{X_2} + \vec{X_3}}{3} \tag{5}$$

$$\vec{X}_1 = |\vec{X_\alpha} - \vec{A_1} \cdot \vec{D_\alpha}| \tag{6}$$

$$\vec{X}_2 = |\vec{X_\beta} - \vec{A_2} \cdot \vec{D_\beta}| \tag{7}$$

$$\vec{X}_3 = |\vec{X_\delta} - \vec{A_3} \cdot \vec{D_\delta}| \tag{8}$$

Where $\vec{A}_1$, $\vec{A}_2$, $\vec{A_3}$ are expressed as Eq. (3) and $\vec{X}_\alpha$, $\vec{X}_\beta$, $\vec{X}_\delta$ are the foremost three best solution in the given iteration t, $\vec{A}_1$, $\vec{A}_2$, $\vec{A_3}$ are defined in the Eqs. (6)–(8) and $\vec{D}_\alpha$, $\vec{D}_\beta$, $\vec{D}_\delta$ are defined in the Eqs. (9)–(11), respectively.

$$\vec{D}_\alpha = |\vec{C_1} \cdot \vec{X_1} - \vec{X}| \tag{9}$$

$$\vec{D_\beta} = |\vec{C}_2 \cdot \vec{X}_\beta - \vec{X}_1| \tag{10}$$

$$\vec{D_\delta} = |\vec{C}_3 \cdot \vec{X}_\delta - \vec{X}_1| \tag{11}$$

$\vec{C_1}$, $\vec{C_2}$, and $\vec{C_3}$ are defined as in Eq. (4). A last comment about the grey wolf streamlining agent is the refreshing of the parameter that controls the trade-off amongst investigation and abuse. The parameter is linearly refreshed in every cycle to run from 2 to 0 as per Eq. (12).

$$a = 2 = t\frac{2}{MaxIter} \tag{12}$$

where *MaxIter* is the total no. of iteration allowed for the optimization and t known as number of iterations.

3.4. Proposed GA-GWO-RBF

In this paper, major important role of Genetic algorithm to optimized the center and widths of RBF neural networks and easily encoded by the chromosomes, and utilizing the genetic operators to yield a better optimal solution. Using GA-RBF algorithm to adjusts the network structure and association weights. The basic steps of GA-RBF described as follows:

Step 1: To find the RBF Center of basis function by using K-Clustering algorithm and determine the width of the center by utilizing the formula $\sigma = d/\sqrt{2s}$.

Step 2: Initiate the population P size randomly, indicates the size by N (No. of neural network in RBF) and the particular networks were represented by encoded using the formula

$$c_1 c_2 \ldots c_s w_{11} w_{21} \ldots w_{s1} w_{12} w_{22}$$
$$\ldots w_{s1} \ldots w_{1m} w_{1m} \ldots w_{sm} \ldots w_{sm} \theta_1 \theta_2 \ldots \theta_m$$

Step 3: Training samples are used to train and built the RBF network structure, and determining the amount of size is N and utilizing the formula of $e = \sum_{k=1}^{n} (t_k - y_k)^2$ to find the network output error E.

Step 4: To find the resultant chromosome fitness of each network by $F = C - E \times S/S_{\max}$ based on training error E and the no. of hidden neurons s.

Step 5: According to fitness value and sort out of chromosome, to choose the best fitness of the population. It's indicated by F_b and verifies the $E < E_{\min}$ or $G \geq G_{\max}$ then indicates yes, skip to step 8 otherwise it's continue.

Step 6: To choose the best individuals for reserved to the second generation P directly.

RESEARCH ARTICLE

Step 7: For single crossover to choose a pair of chromosomes and members of two new individuals were generated for next generation and do this procedure until then new generation were reaches the maximum population size P_s.
Step 8: Mutation of new generation; using different mutation techniques were implemented for real number coding and binary coding. Set $P = \text{New } P$, $G = G+1$ for generating new population and returned to step 4.
Step 9: To obtain the finest neural structure and the iteration are terminated. Further optimal neural networks weights learning are not adequate. Using Least Mean Square (LMS) method for further learn the weights End of the algorithm.

The importance of setting up new model for optimizing neural system, to decide the quantity of hidden layer neurons and the focal point of the basis function, to enhance the association weight and limit, so as to enhance training speed and convergence, to save system running time, and afterward to enhance the working proficiency of network and the capacity of managing issues.

After using LMS Method decide to choose Gray wolf optimization (GWO) is presented for finest parameters of the weights between the hidden layer and output layers (w) and the parameter of spread (α), the center of hidden layer (μ) and an output layer (β). Assurance of a number of cells in the middle layer is fundamental in RBF structure as it influences the speed of joining. In the event that the quantity of cells is low then the convergence speed is moderate and if an extensive number of cells, then the complexity of network is elevated. The basic steps of GWO are described:

Step 1: Initialize a population of gray wolves positions randomly.
Step 2: Find α, β and δ as the first three best solutions based on their fitness values.
Step 3: Until then value of $t = 0$,
while $t \leq MaxIter$ do
for each $Wolf_i \in pack$ do
and update the current wolf's position according to Eq. (5).
Step 4: Update a, A, and C as in Eqs. (3), (4) and (12).
Step 5: To Evaluate the positions of individual wolves.
Step 6: Update α, β and δ positions as the first best three solutions in the current population and its increase the iteration $t = t+1$.
Step 7: Select the optimal gray wolf position and update the weights.
Step 8: RBF is run using the weights and ε yields from GWO.
Step 9: GWO iterates computing the best possible weight, α, β and δ till convergence.
Step 10: End While.

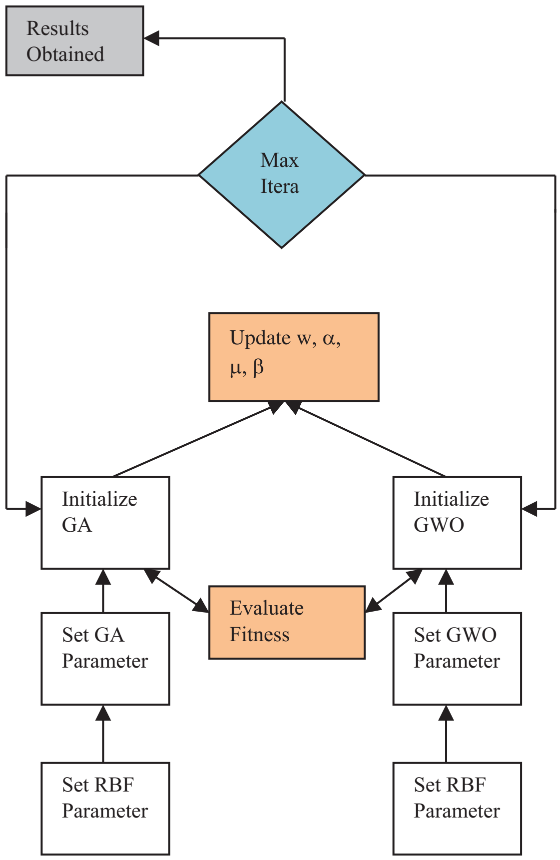

Fig. 2. Comparison between GA and GWO for training RBF network.

4. EXPERIMENTAL RESULTS AND DISCUSSION

We utilize the C++ and Matlab for hybrid programming. The trials are done on Intel Core i3, CPU 2.66 GHz and 4 GB RAM under similar conditions. The KDD 99 cup datasets were chosen to shape the testing and training set and training sample to train every algorithm and test by simulation. Outcome to be evaluated by the detection rate, False alarm rate is characterized as,

$$\text{Detection Rate} = \frac{\text{TP}}{\text{TP}+\text{FP}}, \quad \text{False Alarm Rate} = \frac{\text{TP}}{\text{TP}+\text{FN}}$$

Table I. Parameter settings for experiments.

Parameter	Value(s)
Genetic Algorithm	
Population	50
Crossover rate	0.9
Mutation rate	0.01
No. of iterations	500
Gray wolf optimization	
Search agent	8
α and β in the fitness function	0.99 and 0.01
Δ for changing exploration rate	0.1
No. of iterations	100

RESEARCH ARTICLE

Table II. Classification accuracy.

Seconds	RBF	GA-RBF	GA-GWO-RBF
2	84.15	85.73	94.23
4	85.45	86.44	96.55
6	82.38	90.22	97.88
8	83.68	92.33	98.15
10	84.76	93.45	98.23

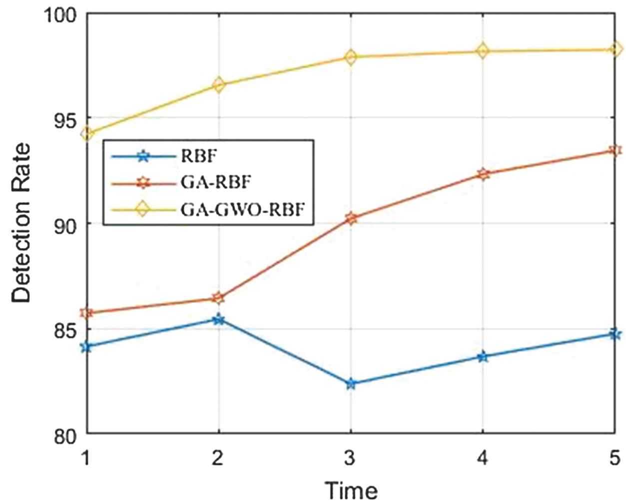

Fig. 3. Classification accuracy.

From the Table II and Figure 3 shows that GA-GWO-RBF yields higher classification accuracy than GA-RBF and RBF. From the Table III and Figure 4 shows that GA-GWO-RBF obtained lower false alarm rate compared to GA-RBF and RBF. The system structure will influence the speculation capacity of the method, looking at RBF, GA-RBF, and GA-GWO-RBF-; while the RBF network gets the little training blunder, its acknowledgment exactness isn't tantamount to GA-GWO-RBF algorithm whose hidden layer neurons are less. Genetic algorithm is powerful for the development of the system structure; it can locate a superior system structure, however it isn't great at enhancing connection weights. Moreover, after 500 iterations it leads to downtrend of the preparation mistake turn moderate, with the goal that we utilize LMS method further to change the weights and after that get the ideal solutions. The new method is a self-adjusted and shrewd calculation, an exact model; it is deserving of further advancement.

Table III. False alarm rate.

Seconds	RBF	GA-RBF	GA-GWO-RBF
2	0.2289	0.1823	0.123
4	0.2207	0.1604	0.110
6	0.2118	0.1442	0.126
8	0.1889	0.1340	0.110
10	0.1667	0.1230	0.104

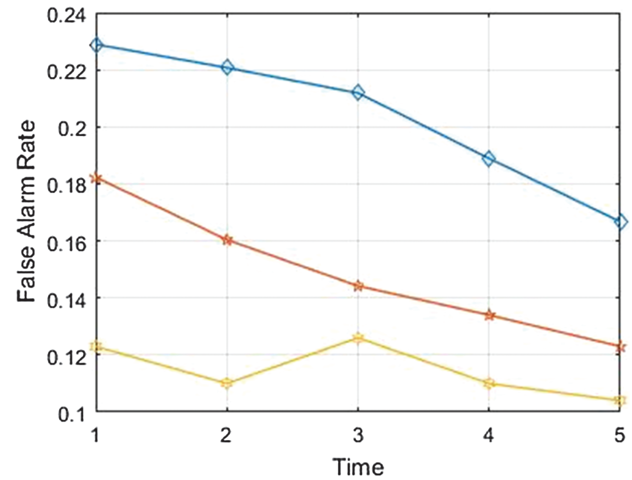

Fig. 4. False alarm rate.

5. CONCLUSION

We bring up that DDoS attacks are as yet a powerful device for digital crooks to close down individual cloud clients, despite the fact that it is relatively difficult to prevent the service from claiming a cloud platform. In the meantime, we additionally take note of that a cloud has a possibility to counter this sort of brute force assault by utilizing its significant assets. In this paper presents an efficient intrusion detection framework using Genetic Algorithm with Gray Wolf Optimization (GA-GWO) technique for tuning the weights and widths of the RBF neural network structure. The overall performance of proposed algorithm for classification accuracy and false alarm rate are yields better than existing algorithm. At last, real cloud environment tests for the proposed technique are normal in the close future.

References

1. S. Yu, Y. Tian, S. Guo, and D. O. Wu, *IEEE Transactions on Parallel and Distributed Systems* 25, 2245 (**2014**).
2. S. Yu, W. Zhou, R. Doss, and W. Jia, *IEEE Transactions on Parallel and Distributed Systems* 22, 412 (**2011**).
3. X. Ma and Y. Chen, *IEEE Communications Letters* 18, 114 (**2014**).
4. https://www.neustar.biz/.
5. 602 Gbps! This May Have Been the Largest DDoS Attack in History, http://thehackernews.com/2016/01/biggest-ddos-attack.html.
6. http://news.yahoo.com/truth-behind-biggest-cyberattack-history-210723787.html.
7. S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, *IEEE Communications Letters* 20, 700 (**2016**).
8. S. Yu, W. Zhou, S. Guo, and M. Guo, *IEEE Transactions on Computers* 65, 1418 (**2016**).
9. S. Yu, W. Zhou, W. Jia, et al., *IEEE Transactions on Parallel and Distributed Systems* 23, 1073 (**2012**).
10. S. Yu, W. Zhou, and R. Doss, *IEEE Communications Letters* 12, 319 (**2008**).

RESEARCH ARTICLE

11. C. Bishop, Neural Networks for Pattern Recognition, Oxford Univ. Press, London, U.K. **(1995)**.
12. D. Du and D. Sun, *J. Food Eng.* 68, 277 **(2005)**.
13. N. B. Karayiannis and G. W. Mi, *IEEE Trans. Neural Netw.* 8, 1492 **(1997)**.
14. Q. Li, X. Chen, and Z. Hu, *Chemometrics Intell. Lab. Syst.* 72, 93 **(2004)**.
15. N. Xie and H. Leung, *IEEE Trans. Neural Netw.* 16, 709 **(2005)**.
16. W. Bing, M. Yao-Hua, and Y. Xiao-Hong, Radial Basis Function Process Neural Network Training Based on Generalized FréChet Distance and GA-SA Hybrid **(2013)**, Vol. 3, pp. 1–9.
17. Z. Q. Zhao, X. D. Wu, C. Y. Lu, H. Glotin, and J. Gao, *Sci. China Inf. Sci.* 57, 1 **(2014)**.
18. J. Lu, H. Hu, and Y. Bai, *Neurocomputing* 152, 305.
19. S. Mirjalili, S. M. Mirjalili, and A. Lewis, *Adv. Eng. Softw.* 69, 46 **(2014)**.

Received: 20 June 2018. Accepted: 8 July 2018.