ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

# A Novel Approach for Intrusion Detection System Using Genetic Algorithm

Anil Dhankhar

Assoc. Professor, RIET Jaipur, Rajasthan, india

**ABSTRACT:** The heading of the project is to identify the hidden intrusion in a network and improve the Intrusion Detection System using Genetic Algorithm. Many works have been done in the past for Intrusion Detection System using Genetic algorithm, however very less work has been done using Elitist Approach. In this thesis work, we have tried using Elitist Approach by using KDD cup '99 datasets. It is very clear that almost all the networks are suffering from unethical attacks because of intruder interference in the communication of those networks with other person/organization. Therefore, in this paper we have created a simulation of mesh network using Cisco Packet Tracer, introduce an attack and the detection and prevention of that attack will be implementing by using various algorithms. Further, predictive analysis is done to improve the performance of existing system.

**KEYWORDS:** Intrusion Detection System, Genetic Algorithm, Elitist Approach, KDD Cup'99, Cisco Packet Tracer, Predictive Analysis.

## I. INTRODUCTION

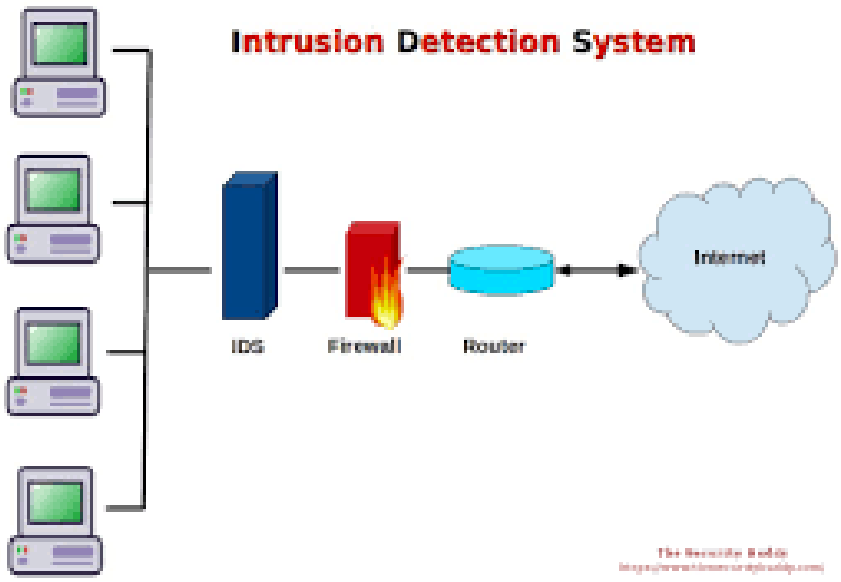



**Figure 1 Intrusion Detection System**

**Outline**

Intrusion detection have been used to detect the malicious bodily process in computer arrangement because of their ability to identify and stopover attack in mental process. More recently, algorithmic trading has programmed to make the network faster and Reliable communication, such as Gentic algorithm and Elitist approach.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

**Network Issues**

Today's network is part of our daily life, but we have to face many network issues while communicating so to make communication more easy, faster and error free intrusion detection is implemented. There are many network issues, some of them are –

**Virus**: A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Contrasts among worms and ailments As depicted in the "Security of the Internet" report, discharged in 1996 by the CERT Division of the Software Engineering Institute at Carnegie Mellon University, PC worms "are self-duplicating programs that spread with no human intercession after they are begun." of course, "[v]iruses are in like way self-reproducing programs, yet when in doubt require some development concerning the client to spread out of the blue to different endeavors or frameworks." After a PC worm loads and starts running on a starting late sullied structure, it will routinely take after its prime demand: to stay dynamic on a ruined structure for whatever timeframe that conceivable, and to spread to at any rate various distinctive weak structures as could be ordinary thinking about the current circumstance.

## II. SYSTEM DESIGN


**Figure 2: Use Case Diagram**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 6, Issue 11, November 2018**

## III. SYSTEM DESIGN AND IMPLEMENTAION

The dataset is divided into train and test data and then we match the actual values with the predicted values. For simplicity, we are attaching only ten actual and their corresponding predicted values for each algorithm we have performed.

**Design of Networking**

Framework masterminding and setup is an iterative strategy, wrapping topological layout, sort out mix, and framework affirmation, and is away to ensure that another media correspondences framework or organization tends to the issues of the endorser and chairman. The methodology can be uniquely fitted as shown by each new framework or organization. Here we have laid out a framework using Cisco Packet Tracer in which there are number of end customers, switches and switches.

**Introduction of Attacks**

This course gives understudies a check appreciation of normal computerized security risks, vulnerabilities, and perils. An audit of how basic advanced attacks are assembled and associated with honest to goodness structures is furthermore included. Cases join essential Unix partition hacks, Internet worms, and Trojan horses in programming utilities. Framework strikes, for instance, circled dispute of organization (DDOS) and botnet-ambushes are moreover portrayed and outlined using honest to goodness cases from the ongoing decades. Conspicuous indicative models are plot, for instance, the order/uprightness/openness (CIA) security chance structure, and cases are used to portray how these assorted sorts of risks can corrupt certifiable assets. The course furthermore joins a preamble to fundamental advanced security chance examination, with a chart of how risk asset systems can be used to compose danger decisions. Perils, vulnerabilities, and ambushes are dissected and mapped with respect to structure security building approaches.

**What is a DDoS Attack?**

This course gives understudies a check appreciation of normal computerized security risks, vulnerabilities, and perils. An audit of how basic advanced attacks are assembled, and associated with honest to goodness structures is furthermore included. Cases join essential UNIX partition hacks, Internet worms, and Trojan horses in programming utilities. Framework strikes, for instance, circled dispute of organization (DDOS) and botnet-ambushes are moreover, portrayed and outlined using honest to goodness cases from the ongoing decades. Conspicuous indicative models are plot, for instance, the order/uprightness/openness (CIA) security chance structure, and cases are used to portray how these assorted sorts of risks can corrupt certifiable assets. The course furthermore joins a preamble to fundamental advanced security chance examination, with a chart of how risk asset systems can be used to compose danger decisions. Perils, vulnerabilities, and ambushes are dissected and mapped with respect to structure security building approaches.

**How Do Know When a DDoS Attack Is Occurring?**

The hardest part about a DDoS strike is that there are no alerts. Some enormous hacking social events will send risks, yet generally an attacker sends the charge to trap your site without any alerts by any stretch of the inventive vitality. Since you don't ordinarily investigate your site, it isn't until the point that the minute that clients complain that you at last perceive something isn't right. At first, you most likely don't confide in it's a DDoS strike yet rather think your server or empowering is down. You check your server and perform principal tests, yet you will essentially watch a high extent of system development with assets enlarged. You may check whether any exercises are missing the mark decisively, yet you won't locate any noticeable issues. Between the time it takes for you to fathom it's a DDoS strike and the time it takes to alleviate the insidiousness, two or three hours can voyage by. This induces a few expanded lengths of missed association and wage, which basically takes a basic cut in your wage.

**Genetic Algorithm**

A natural calculation is a model for machine learning in which a masses of haphazardly made people experiences a reproduced arrangement of change - a mechanized survival of the fittest in which every individual tends to a point in an

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

issue's answer look space. An individual is suggested as chromosome. A chromosome includes attributes, which address the parameters of the issue being made strides. A get-together of chromosomes on which a hereditary check works is signified a people.
Through made by a wellbeing work, chromosomes are assessed and arranged by their relative quality/shortcoming inside the general population. The fitter are duplicated while the less fit everything considered don't get by into succeeding ages.
This estimation mirrors the strategy of run of the mill choice where the fittest people are chosen for augmentation recollecting a definitive goal to make group of the all inclusive community to come

Five phases are considered in a genetic algorithm.
1. Initial population
2. Fitness function
3. Selection
4. Crossover
5. Mutation

**Algorithm**

Begin
*Step 1. Initialization. Set the generation counter* $G = 1$ *and the discovery rate* $p_a$*; initialize the population* $P$ *of* $n$ *host nests randomly.*
*Step 2. While* $G <$ *MaxGeneration do*
*Sort all the cuckoos.*
*Randomly select a cuckoo* $i$ *and implement Lévy flights to replace its solution.*
*Evaluate its fitness* $F_i$.
*Randomly choose another nest* $j$.
*if* $(F_i < F_j)$
*Replace* $j$ *by the new solution.*
*end if*
*Randomly generate a fraction* $(p_a)$ *of new nests and replace the worse nests.*
*Keep the best nests.*
*Sort the population and find the best cuckoo for this generation.*
*Pass the current best to the next generation.*
$G = G + 1$.
*Step 3. end while*
End.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

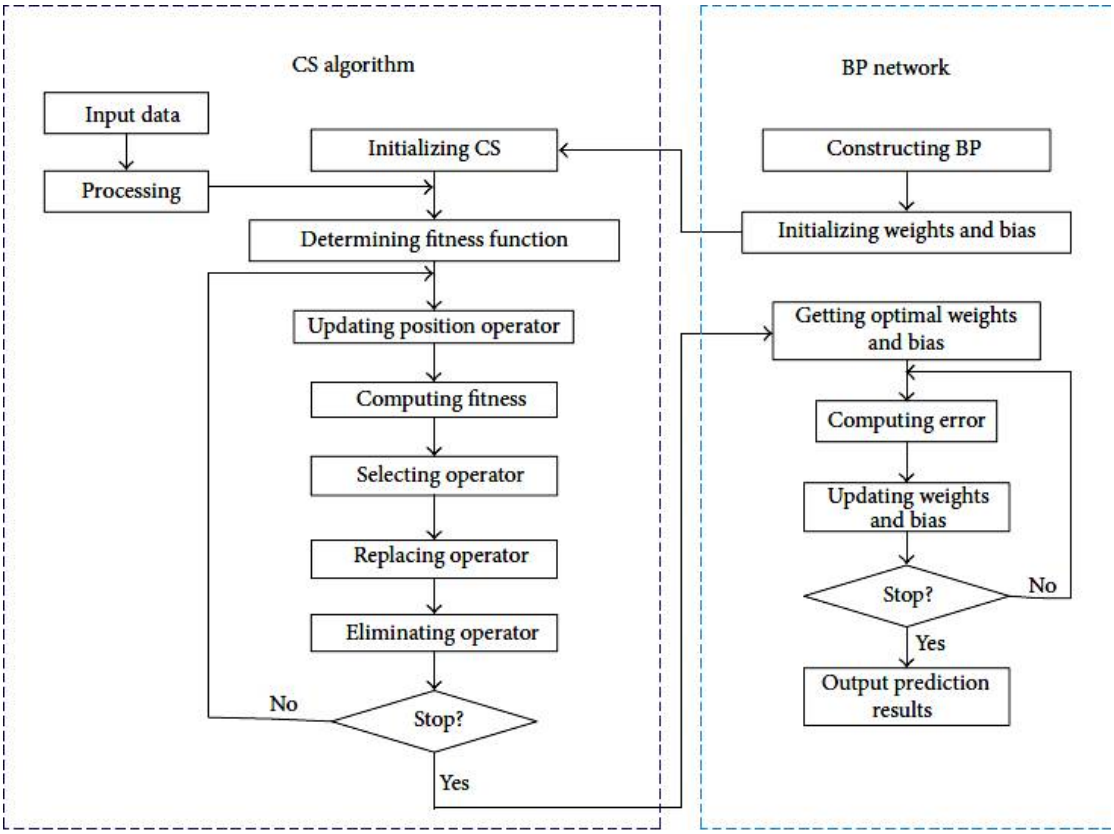
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

**Flowchart**




## IV. ALGORITHM OF THE PROPOSED SYSTEM

| **Algorithm – Rule set generation using GA** | |
|---|---|
| Input | Network audit data, number of generations and population size |
| Output | A set of classification rules |
| Algorithm | *1. initialize the population*<br>*2. generate random population*<br>*3. W1=0.2, W2=0.5, W3=0.3, T=0.5, chrom_length=9*<br>*4. N=total number of populations to be generated*<br>*5. for each chromosome in the population*<br>*6. TP=0, TN=0, FP=0, FN=0*<br>*7. for each record in the training set*<br>*8. if the record matches the chromosome*<br>*9. increment membership value of TP*<br>*10. end if*<br>*11. if the records do not match the chromosome*<br>*12. increment membership value of FP*<br>*13. end if*<br>*14. end for* |

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

| | | |
|---|---|---|
| | 15. | *Fitness=W1*TP/(TP+FN)+W2*FP/(FP+TN)+W3*(1-chrom_length/10)* |
| | 16. | *if Fitness>T* |
| | 17. | *if N<1* |
| | 18. | *break* |
| | 19. | *else* |
| | 20. | *select the chromosome into the new population* |
| | 21. | *update the total number of population* |
| | 22. | *N=N-1* |
| | 23. | *end if* |
| | 24. | *end if* |
| | 25. | *end for* |
| | 26. | *for each chromosome in the new population* |
| | 27. | *apply crossover operator to the chromosome* |
| | 28. | *apply mutation operator to the chromosome* |
| | 29. | *end for* |
| | 30. | *if the required number of generation is not reached, then go to step 15* |

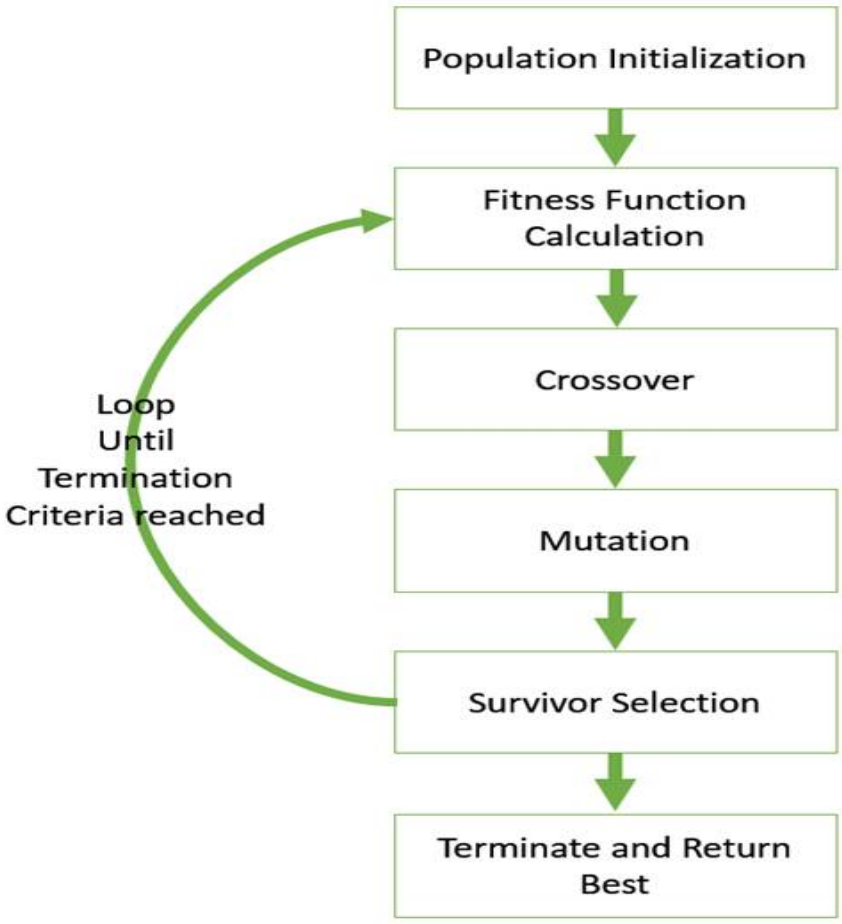



**Figure 3 Genetic Algorithm Process**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

**Table 1: DataSets (KDD'99)**

| Datasets | Normal | Probe | Dos | U2r | R2I | Total |
|---|---|---|---|---|---|---|
| Train(kddcup data 10%) | 97280 | 4107 | 391458 | 52 | 1124 | 494021 |
| Test (corrected) | 60593 | 4166 | 229853 | 228 | 16189 | 311029 |

## V. RESULTS

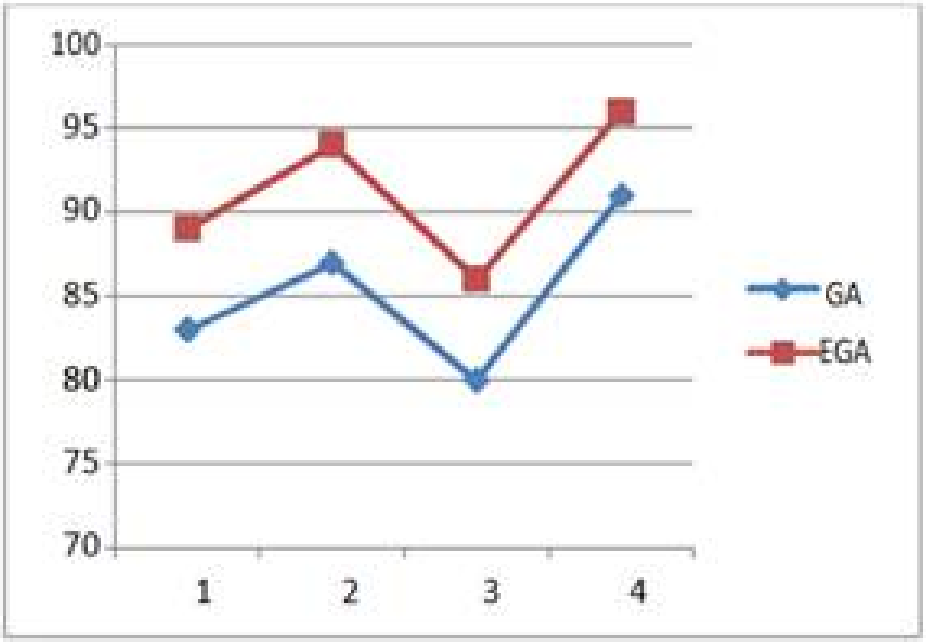



**Figure Path Coverage**

**Test suite for the given program:**

| | GA | EGA |
|---|---|---|
| 1 | 83 | 89 |
| 2 | 87 | 94 |
| 3 | 80 | 86 |
| 4 | 91 | 96 |

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Based on Path coverage and test suite for the program Elitist approach performs better than Genetic Algorithm. When the sample program is taken 1 in that case the path coverage of GA results as 83 and EGA results as 89. Which shows using Elitist approach it works properly?

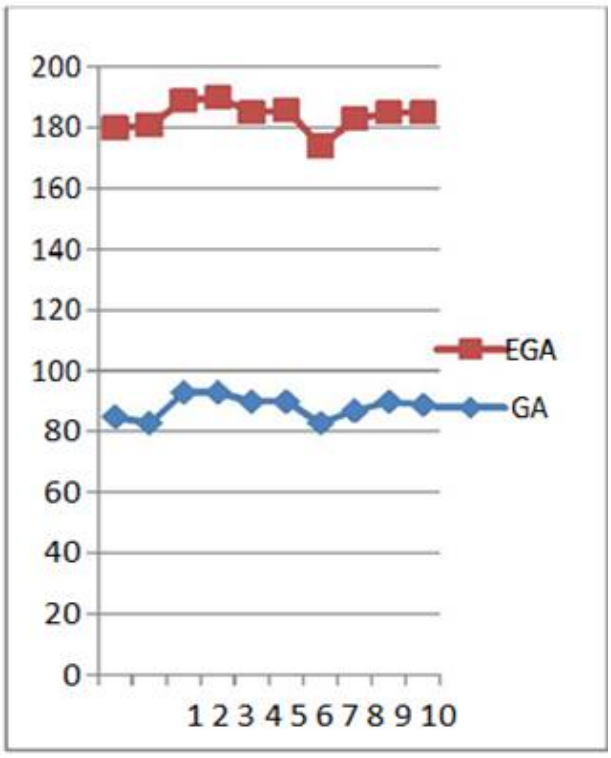



**Figure 5 Path Coverage sample 2**

| | GA | EGA |
|---|---|---|
| 1 | 85 | 95 |
| 2 | 83 | 98 |
| 3 | 93 | 96 |
| 4 | 93 | 97 |
| 5 | 90 | 95 |
| 6 | 90 | 96 |
| 7 | 83 | 91 |
| 8 | 87 | 96 |
| 9 | 90 | 95 |
| 10 | 89 | 96 |

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

## VI. CONCLUSION

In the beginning of this these we have started with problem formulation. We have asked following question:
"How to Improve Network Connection in Intrusion Detection System using different tools and techniques ? " Working on Intrusion Detection using genetic Algorithm and Elitist Approach, analysis and prediction, we have come to the conclusion that there is a huge scope of improvement in this field. As this field is comparatively new, there are many ways to improve the efficiency of network. The algorithms we have so far implemented on our dataset are:
1. Genetic Algorithm
2. Elitist Approach
All our approach and their predictions have some merits and demerits. We hope to have a better insight into it when we perform the comparative analysis. However, Genetic Algorithm and Elitist Approach have yielded good results. The main aim of this project is to understand and analyse the network issues and how we are going to overcome in future. Having knowledge of the network and its problems beforehand will help people reduce the errors.

## REFERENCES

1 A. Kaveh and S. Talatahari, "A novel heuristic optimization method: charged system search," Acta Mechanica, vol. 213, no. 3-4, pp. 267–289, 2010.
2 O. K. Erol and I. Eksin, "A new optimizationmethod: Big Bang-Big Crunch," Advances in Engineering Software, vol. 37,no. 2, pp. 106–111, 2006.
3 A. Kaveh and S. Talatahari, "Size optimization of space trusses using Big Bang-Big Crunch algorithm," Computers&Structures, vol. 87, no. 17-18, pp. 1129–1140, 2009.
4 A. Kaveh and S. Talatahari, "Optimal design of Schwedler and ribbed domes via hybrid Big Bang-Big Crunch algorithm," Journal of Constructional Steel Research, vol. 66, no. 3, pp. 412–419, 2010.
5 A. Kaveh and S. Talatahari, "A discrete Big Bang-Big Crunch algorithm for optimal design of skeletal structures," Asian Journal of Civil Engineering, vol. 11, no. 1, pp. 103–122, 2010.
6 Z.W. Geem, J. H. Kim, and G. V. Loganathan, "A new heuristic optimization algorithm: harmony search," Simulation, vol. 76, no. 2, pp. 60–68, 2001.
7 P. Yadav, R. Kumar, S. K. Panda, andC. S.Chang, "An intelligent tuned harmony search algorithmfor optimisation," Information Sciences, vol. 196, pp. 47–72, 2012.
8 S. Gholizadeh and A. Barzegar, "Shape optimization of structures for frequency constraints by sequential harmony search algorithm," Engineering Optimization, vol. 45, no. 6, pp. 627–646, 2012.
9 J. Kennedy and R. Eberhart, "Particle swarm optimization," in Proceedings of the IEEE International Conference on Neural Networks, pp. 1942–1948, Perth, Australia, December 1995.
10 R. J. Kuo, Y. J. Syu, Z.-Y. Chen, and F. C. Tien, "Integration of particle swarmoptimization and genetic algorithm for dynamic clustering," Information Sciences, vol. 195, pp. 124–140, 2012.