A Comprehensive Study on Metaheuristic Techniques Using Genetic Approach

G. Kalyani Assistant Professor Department of CSE, SNIST R.R District, T.S, India *e-mail:ghanta.kalyani@gmail.com* K. Krishna Jyothi Assistant Professor Department of CSE, SNIST R.R District, T.S, India *e-mail:kkjyothi86@gmail.com* T. Pratyusha Student Department of CSE, SNIST R.R District, T.S, India *e-mail:pratyusha.thumiki@gmail.com*

Abstract-- Most real-life optimization problems involve multiple objective functions. Finding a solution that satisfies the decision-maker is very difficult owing to conflict between the objectives. Furthermore, the solution depends on the decision-maker's preference. Metaheuristic solution methods have become common tools to solve these problems. The task of obtaining solutions that take account of a decision-maker's preference is at the forefront of current research. It is also possible to have multiple decision-makers with different preferences and with different decision-making powers. It may not be easy to express a preference using crisp numbers. In this study, the preferences of multiple decision-makers were simulated and a solution based on a genetic algorithm was developed to solve multi-objective optimization problems. The preferences were collected as fuzzy conditional trade-offs and they were updated while running the algorithm interactively with the decision-makers. The proposed method was tested using well-known benchmark problems. The solutions were found to converge around the Pareto front of the problems.

Key words-- Optimization, computational intelligence, Fuzzy logic



 $\mathbf{11000}011 + 110111\mathbf{01} = \mathbf{11000101}$

b) Two Point Crossover: In this, two Crossover points are chosen such that the resultant binary string is formed by copying from the beginning to the first Crossover point one parent chromosome. The portion from the beginning to the second Crossover point of second parent is formed, and the remaining part is copied from the first parent[5]. Thus, new offspring is formed.



 $\mathbf{10}0010\mathbf{01} + 11\mathbf{0101}11 = \mathbf{10010101}$

c) Arithmetic Crossover: Some arithmetic operations will be executed to create a new offspring.



d) Uniform Crossover: Here, the new offspring is formed by copying the bits randomly either from the first parent or the second parent.

In the area of cyber security and working research, Genetic Algorithm (GA) is a metaheuristic technique provoked the process of usual choice which belongs to the bigger class of evolutionary algorithms (EA). Genetic algorithms are mostly used to produce good quality solutions to search and optimization problems by depending on biologically inspired operators such as selection, cross-over and mutation.

Darwin's theory about evolution inspired Genetic Algorithms. It began with a set of solutions which are represented by chromosomes and is called population [20]. A new population is formed from the solutions obtained from the previous population. The significant part of the genetic algorithm involves the mutation and crossover operators. These two operations influence the performance of the algorithm. In some way, the chromosome should contain the information about the solution that it represents. A binary string is the widely used way of encoding.

A. Crossover

a) Single Point Crossover: A single Crossover point is selected and the resultant binary string is formed by copying from beginning to the crossover point of one parameter chromosome, and the remaining part is copied from the second parent [7]. Thus, new offspring is formed.



11101010 + 11001101 = 11101110

B. Mutation

Bit inversion: Some bits are selected and these selected bits are inverted.



Fig.1. Basic Architecture of Genetic Algorithm

Genetic Algorithms are used mostly to generate high quality solutions to search based and optimization problems by depending on biologically inspired operations such as selection, crossover and mutation.

Genetic Programming:

- Derivation information is not required.
- Fast and efficient compared to traditional methods.
- Have very good parallel capabilities.
- Both continuous and discrete functions can be optimized along with multi-objective problems.
- Can have multiple good solutions instead of only one solution.
- Ensures that we get an answer every time, improving the solution every time.
- Useful when we have large number of parameters

The main contributions of this paper are to explain about genetic algorithm capabilities in four-fold[1]. (1) We present outline of necessities of a genetic algorithm by discussing the current usages of genetic algorithm to avoid different problems. (2) The present use of genetic algorithm over different problems are typically reviewed in the course of the systematic taxonomy (3) This paper gives a systematic view of the proposed security techniques for each technique. The survey proposes a new taxonomy of Security Approaches of Genetic Algorithm. The aim of our survey is to recognize the strong and frail features of existing security approaches.

The hierarchy of our paper is categorized as follows. The uses of genetic algorithm over different problems are typically reviewed in section 2. We discuss the classification of newly proposed security protocols for genetic algorithm the Section 3. Section 4 describes the existing security protocols for the corresponding models. The concluding notes are discussed in the final section i.e., Section 5.

II. EXISTING USAGE OF THE GENETIC ALGORITHM

A. Cryptography:

Cryptography is a method used to protect the information and to provide safe communication by using codes in such a way that only those can read the information for whom it was intended and then, can process the information. In the word Cryptography, "crypt" means hidden and "graphy" means write. It uses different approaches called as cryptographic algorithms, or ciphers that are used to encrypt and decrypt messages to have a secure way of communication amongst the smart devices and the computer systems [5]. It involves three algorithms, one for authentication, and another for key exchange and the other one for encryption. It can involve have private or public key generation for data signing and verification, data encryption/decryption, for key exchange and for message authentication.



Fig 2: Genetic Crypto Flow graph

B. Neural networks

Neural networks are also called as connectionist systems. A neural network is a computational approach used in various disciplines like computer science and other research fields.

It deals with an immense collection of neural (artificial neurons) units, to create a replica of biological/ human brain which can solve problems with huge clusters of biological neurons which are connected by axons[19]. A neural net can be connected with many other neural nets, and the links between them can be inhibitory or enforcing in their effect on the activation state of connected with many others, and links can be enforcing or inhibitory in their effect on the activation state of the overall neural network units connected. These systems are trained using the data and undergo self-learning process, rather than being programmed explicitly, and outshine in the areas where its difficult to express the solution or feature detection in a traditional computer program.

Artificial Neural Networks consists of units, connections and weights. Here is the basic architecture diagram of ANN:



Fig.3. Artificial Neural Networks

Evolutionary Artificial Neural Networks (EANNs) are the Combination of the Neural Networks with the evolutionary algorithms.

To create a string or chromosome using a simple Neural Network:

All the wrights in a network are combined in order to form a single string. The population now includes the generated string as a member. Every string in the population represents the weights of the entire network.



Fig 4: Simple Neural Network



Fig 5: String or Chromosome

This generated string represents the value obtained from a single Neural Network.

Fitness Evaluation:

The error is calculated first to measure the fitness. Error = (target-output) and fitness is calculated as fitness = (1/error).

Error and fitness are inversely proportional which means that if the error is lower then, the fitness is higher.

C. Intrusion Detection System

An Intrusion Detection System (IDS) is a system which is used to monitor the traffic in the network for detecting distrustful activity and on discovering such activities, a system issues alerts [13]. While detecting anomaly and reporting are the fundamental functions, some of the intrusion detection systems are accomplished to take actions when anomalous traffic or malicious activity is detected, which includes traffic blocking when sent from some suspicious IP addresses.

These systems are also vulnerable to invalid positives (false alarms), though they detect networks for potentially malicious activity. Consequently, during the first installation of the IDS products, the organizations need to fine tune them which means, their intrusion detection systems should be thoroughly configured in order to differentiate between the standard traffic and the potentially malicious activity on their network.



Fig 6: Intrusion Detection System (IDS)

Types of intrusion detection systems:

Intrusion detection systems are of different types and use different methods to detect suspicious activities. IDS are of the following types:

- Host intrusion detection systems (HIDS)
- A network intrusion detection system (NIDS)
- Anomaly-based intrusion detection systems
- Signature-based intrusion detection systems.

The following are the sequence of steps to view intrusion detection when a genetic algorithm is applied to it: [18]

- i) The information about the network traffic or logs is collected by the sniffer or packet capturing module present in the intrusion detection system.
- ii) The genetic algorithms are then applied to the captured data by the intrusion detection system. At this stage, the genetic algorithm has already learned some classification from the collected information.
- iii) The rules that are produced in the preceding phases are applied to the incoming traffic by the intrusion detection system. By applying the rules to data that's captured, population initialization is done. Thus, a new population with good qualities is created. The resulted population is then assessed and evaluated resulting in a new generation with better qualities. Now, the genetic operators are implemented on the newly formed generation till the most suitable individual is found.



Fig 7: Implementation of Genetic Algorithm in IDS.

D. Fuzzy logic

A Fuzzy logic is one of the forms of many valued logic. Fuzzy logic based techniques are used in a Fuzzy Genetic Algorithm (FGA) which is also considered as a Genetic Algorithm. For the notions that can't be explained exactly, but are dependent on the contexts, Fuzzy logic form of representing the knowledge is more suitable. Binary sets a fuzzy logic than the traditional. Variables used in a fuzzy logic representation can have a truth value which usually is in the range with degree between 0 and 1.

As we are mainly concerned with the multiple criteria of stringing the data items to clusters, a single objective optimization model may not serve the purpose of a fitness measuring index. It is true; not only for the clustering problem but also for the problems that use Genetic Algorithm involving multiple criteria. In multiple criteria optimization models, the concept of optimality is not precisely defined [12]. A solution obtained can be the best w.r.t. a particular criterion but not the best w.r.t. to some other criteria. Pareto optimality provides a set of no dominated solutions called the P-optimal set in which the righteousness of each criterion is regarded.



Fig 8: Fuzzy Genetic Algorithms

III. TAXANOMY

The existing proposal on genetic algorithm uses Metaheuristic algorithms.. Hence, we categorize genetic algorithm security solutions into four categories – Fuzzy, cryptography, IDS and Neural networks as shown in Figure 9. The comparison of different techniques used with genetic algorithm are discusses in Table 1 with their features and challenges.

[1] This paper was proposed by Chawla.S using Genetic Algorithm and Fuzzy set to get better results while doing web search even for imprecise user queries. This technique optimizes web pages. But, the limitation of this technique is the accuracy can be further improved by using feature reduction method.

[2] The use of Genetic Algorithm along with Fuzzy Logic has been done by Anderson Hiroshi Hamamoto, Luiz Fernando Carvalho, Lucas Dias Hiera Sampaio, Taufik Abr⁻ao, and Mario Lemes Proenc, aJr. In this technique, they have used an unsupervised learning technique along with fuzzy logic and genetic algorithm. Supervised learning cannot detect unknown problems. Unsupervised learning causes recurrent problem of false positive rates. Therefore, this system helps in providing unsupervised learning NADS with high accuracy and low FPR on real time. For this technique, further evaluation in different networks is required and is compared to different state of art approaches.

[3] N. E. Naily, S. M. Saad, T. Hussein, K. El-Arroudi and F. A. Mohamed proposed a technique called SAGA (Self Adaptive Genetic Algorithm) to take advantage of Back propagation, Genetic Algorithm and Intrusion Detection System; they combined all these implemented to get better results and got high Detection Rate and low False Alarm Rate. This can be improved such that Adaptive Genetic Algorithm (AGA) adjusts automatically, crossover rate parameter of GA to provide further enhancement.

[4] Chiba Z., Abghour N., Moussaid K., El omri A., Rida M. proposed a technique which uses Genetic Algorithm and Deep learning DNA technique. The biggest advantage of using DNA as basis of computation is its storage capacity. 1gm of DNA = 108TB. GA provides key generation with encryption whereas DL (Deep learning) DNA helps in encryption, decryption and reduces the time taken by the algorithm. This technique gives higher accuracy but doesn't provide cost effectiveness and time effectiveness.

[5] Genetic Algorithm along with Decision tree has been proposed as a technique by Kalsi, S., Kaur, H. & Chang, V. J Med Syst where they mentioned that Decision tree C4.5 gives better detection rate, but not for small disfuncts. The proposed system gives better results than C4.5, Naive Bayes. But the problem is the proposed technique mostly focuses on the small disfuncts.

[6] This technique was proposed because Deep learning cannot detect all the attacks. Hence, it uses Deep Belief Network which contains Back propagation neural network that propagate error function information and if DBN is finely tuned, global optimization can be achieved. But, here in this technique, the training time can be further reduced and the accuracy can be improved further.

[7] The proposed technique involves the use of Multilayer Perceptron along with Genetic Algorithm. The GA helps in feature selection and MLP helps in classification. This technique was done on NSL-KDD dataset which doesn't lead to negative effect on training process. Supports different kinds of evaluation metrics. But the proposed method didn't achieve greater increase in the accuracy. Only a little increase was seen compared to the existing systems

[8] This paper proposes a technique using VBGA (Vector Based Genetic Algorithm). Here we treat Chromosomes as vectors and training data as matrices. There is an increase in detection rate and false positives are less compared to string based GA. It can be improved for getting novel fitness function in which fitness is calculated directly from overlapping arrays of chromosomes.

[9] This paper uses Genetic Algorithm along with Profiling. It has been proposed because the existing work is for signature based Intrusion Detection System for labeled data. Here, it adapts to new attacks iteratively, like business needs, staff preferences, and threats identification. It performs well on small datasets and doesn't achieve good results on larger datasets.

[10] In this paper, they proposed a technique where they have used Genetic Algorithm along with Multiple Support Vector Machines (MVSM). This was proposed to overcome the drawbacks like high computational intensity and coarse function approximation of instance and model based methods. It is more efficient than conventional system with common feature selection technique. More accuracy, less computational complexity, less communication overhead, improved security, less time for the training system.

[11] In this paper proposed, GA is used for cluster based routing for Wireless network security (WSN). To prevent attacks when cluster size is increased or number of surviving nodes are reduced, probabilistic voting-based filtering scheme, shortest path to test and got good results.

[12] The use of Genetic Algorithm along with FCM (Fuzzy C-Means) Algorithm was done by Alessandro G. Di Nuovo, Vincenzo Catania, Maurizio Palesi have proposed a technique which is a hybrid method. Here, Evolutionary Algorithms (EA) are used perform better on feature selection. Genetic Fuzzy C-Means (GFCM) is two times faster compared to (FCM) Fuzzy C-Means Algorithm and give seven times faster classification accuracy. The drawback was the performance accuracy for heavy weight models was less compared to the Genetic Algorithm Approach.

[13] In 2010, IDS (Intrusion Detection System) alert management with genetic algorithm and two clustering algorithms was done to improve the performance by removing the disadvantage of the IDS system where number of alerts generated were failing and the two new clustering algorithms were based on genetic algorithm and were compared for which it successfully classified the alerts and causes reducing the false positive alerts. Here they have used a symmetric genetic algorithm and this was a new system to evaluate genetic algorithm based clustering algorithms in intrusion alert management system.

[14] The next one was proposed by N. Arastouie and E. Salimi in 2011 which consists of Backdoor detection system using ANNs (Artificial Neural Networks) and Genetic algorithm. They have used a symmetric genetic algorithm and it takes advantages from genetic algorithm and artificial neural networks where Genetic Algorithm gives deterministic answer to the issue and artificial neural networks classify the system features and predict the percentage of the back door problem.

[15] In 2012, Md. Abu Naser Bikas proposed a technique using genetic algorithm and implemented intrusion detection system. This had a drawback when there are discrete features and the implementation was a little bit difficult. This was developed to overcome the drawback of IDS including resource usage, fidelity and reliability. When both IDS and genetic algorithm were combined, it has given a FPR (False Positive Rate) of 0.3% and a DR (Detection Rate) of 95%. But this was less when compared to the

results of the technique where we use only the genetic algorithm which has given almost 100% detection rate and the false positive rate was also very less i.e., 0.2%.

[16] In 2009, C. Grosan, Y. Chen, H. Liu and A. Abraham have developed a new technique called Hierarchical Takagisugeno model for online security evaluation systems. This was better than genetic algorithm and neuro fuzzy but it was only suitable for lightweight risk assessment models and not for the heavyweight models.

[17] In 2014, an Asymmetric key encryption using genetic algorithm was proposed by Poornima Naik where the tools used are Java and a word document and it was purely genetic algorithm based. It strengthens the security encryption and decryption was done end to end.

[18] From the survey done by authors Parry Gowher et.al have portrayed a novel symmetric block cipher system named ICIGA (Improved Cryptographic Inspired by Genetic Algorithm) that gives a session key in a haphazard process. The key length and block size are fixed by the end client in the start of the cipher progression. ICIGA is an improvement of the scheme GIC (Genetic Algorithm inspired Cryptography).

CONCLUSION

Genetic Algorithm is used in many applications for solving non-linear optimization problems in various fields. However a few articles are available which exploits the arbitrariness in the algorithm for security. These days, the metaheuristic methods have become the common tools for solving optimization kinds of problems. Here in this study, the simulation of preferences of multiple decision-makers is done and a solution has been developed based on the genetic algorithm to solve multi-objective optimization problems.

REFERENCES

- Chawla, S. (2018). Application of hybrid of Fuzzy Set, Trust and Genetic Algorithm in query log mining for effective Information Retrieval. International Journal of Intelligent Systems and Applications in Engineering, 6(1), 47-52
- [2] Anderson Hiroshi Hamamoto, Luiz Fernando Carvalho, Lucas Dias Hiera Sampaio, Taufik Abrao, Mario Lemes Proenc, aJr., Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic, Expert Systems With Applications (2017)
- [3] N. E. Naily, S. M. Saad, T. Hussein, K. El-Arroudi and F. A. Mohamed, "On-line adaptive protection scheme to overcome operational variability of DG in smart grid via fuzzy logic and genetic algorithm," 2018 9th International Renewable Energy Congress (IREC), Hammamet, 2018, pp. 1-6.
- [4] Chiba Z., Abghour N., Moussaid K., El omri A., Rida M. (2019) Novel Network IDS in Cloud Computing Based on

Optimized Back Propagation Neural Network Using a Selfadaptive Genetic Algorithm. In: Ben Ahmed M., Boudhir A., Younes A. (eds) Innovations in Smart Cities Applications Edition 2. SCA 2018. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham.

- [5] Kalsi, S., Kaur, H. & Chang, V. J Med Syst (2018). DNA Cryptography and Deep Learning using Genetic Algorithm with NW Algorithm for Key Encryption., Springer US, Volume 42, pp 17.
- [6] Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 1–1.
- [7] Htwe T.T., Kham N.S.M. (2019) Improving Accuracy of IDS Using Genetic Algorithm and Multilayer Perceptron Network. In: Bhattacharyya S., Hassanien A., Gupta D., Khanna A., Pan I. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 56. Springer, Singapore.
- [8] Ijaz, S., Hashmi, F.A., Asghar, S. et al. Appl Intell (2018), Vector Based Genetic Algorithm to optimize predictive analysis in network security, Springer US, Volume 48, pp 1086-1096.
- [9] Resende, Paulo Angelo Alves and Drummond, André Costa (2018), Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling, volume 1, 4e36.
- [10] R.Vijayanand, D.Devaraj, Kannapiran, Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection, Computers & Security, Volume 77, 2018, pp. 304-31
- [11] Nazeer, Muhammad Irshad, et al. "Implication of Genetic Algorithm in Cryptography to Enhance Security." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 9.6 (2018): 375-379.
- [12] Nuovo, Alessandro G. Di, Vincenzo Catania and Maurizio Palesi. "The hybrid genetic fuzzy C-means: a reasoned implementation." Conference Proceedings Chicago (2006).
- [13] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas, "An implementation of intrusion detection system using genetic algorithm", arXiv preprint arXiv: 1204.1336 (2012).
- [14] N. Arastouie and E. Salimi, "Backdoor Detection System Using Artificial Neural Network and Genetic Algorithm," 2011 International Conference on Computational and Information Sciences (ICCIS), Chengdu, Sichuan Chengdu, 2011, pp. 817-820.
- [15] H. Bahrbegi, A. Habibizad Navin, Amir Azimi Alasti Ahrabi, M. K. Mirnia and A. Mollanejad, "A new system to evaluate GA-based clustering algorithms in Intrusion Detection alert management system," 2010 Second World Congress on Nature and Biologically Inspired Computing (NaBIC), Fukuoka, 2010, pp. 115-120.
- [16] C. Grosan, Y. Chen, H. Liu and A. Abraham, "Hierarchical Takagi-Sugeno Models for Online Security Evaluation Systems," Information Assurance and Security, International Symposium on(IAS), Xi'An China, 2009, pp. 687-692.

- [17] Naik, Poornima & Naik, Girish. (2014). Asymmetric Key Encryption using Genetic Algorithm. International Journal of Latest Trends in Engineering and Technology (JJLTET). 3. 10.13140/2.1.3621.0889.
- [18] Parry Gowher Majeed and Santosh Kumar "Genetic Algorithms in Intrusion Detection Systems: A Survey" International Journal of Innovation and Applied Studies -January 2014.
- [19] Richa Mahajan, Gaganpreet Kaur "Neural Networks using Genetic Algorithms" International Journal of Computer Applications Volume 77– No.14, September 2013.
- [20] Muhammad Irshad Nazeer, Ghulam Ali Mallah, Noor Ahmed Shaikh, Rakhi Bhatra "Implication of Genetic Algorithm in Cryptography to Enhance Security" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 6, 2018.



G.Kalyani is working Assistant Professor at the Department of CSE, SNIST, Hyderabad. She has completed her Bachelor of Engineering in Computer science and Engineering from JNTU, Hyderabad, India. She has completed her Master of Technology in Computer Science from IETE, Hyderabad, A.P., India. She has 13 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently doing her Ph.d in Computer science and Engineering from REVA University Bangalore. Her areas of research and teaching include Programming languages, Compiler Design, network security, computational intelligence, wireless networks. She has published 6 international journal papers. She can be reached at <u>ghanta.kalyani@gmail.com</u>.



K.Krishna Jyothi is working Assistant Professor at the Department of CSE, SNIST, Hyderabad. She has completed her Bachelor of Engineering in Computer science and Engineering from JNTU, Hyderabad, India. She has completed her Master of Technology in Computer Science from JNTU, Hyderabad, A.P., India. She has 8 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently doing her Ph.d in Computer science and Engineering from REVA University Bangalore. Her areas of research and teaching include network security, computational intelligence, wireless networks. She has published 4 international journal papers. She can be reached at kkjyothi86@gmail.com.



1 15.7.	raxonomy c	JI Genetic	ingoriumi

S. No	Technique used	Features	Challenges
1	GA + Fuzzy set = GFS	Better results while doing web search even for imprecise user queries. Optimizes web pages.	Can be improved by using feature reduction method.
2	GA + Fuzzy = GFS	Supervised learning cannot detect unknown problems. Unsupervised learning causes recurrent problem of False positive rates. Therefore, this system helps in providing unsupervised learning NADS with high	Further evaluation in different networks is required and is compared to different state of art approaches.

Table 1: Comparative analysis of Metaheuristic Techniques

		accuracy and low FPR on real time.	
3	SAGA	To take advantage of Back propagation, Genetic Algorithm and Intrusion Detection System, we combined all these implemented to get better results and got high Detection Rate and low False Alarm Rate.	Can be improved such that Adaptive Genetic Algorithm (AGA) adjusts automatically, crossover rate parameter of GA to provide further enhancement.
4	GA + DLDNA	The biggest advantage of using DNA as basis of computation is its storage capacity. 1gm of DNA = 108TB. GA provides key generation with encryption whereas DL (Deep learning) DNA helps in encryption, decryption and reduces the time taken by the algorithm.	A lot can be done on cost and time effectiveness.
5	GA + Decision tree	Decision tree C4.5 gives better detection rate, but not for small disfuncts. The proposed system gives better results than C4.5, Naive Bayes.	Mainly concentrates on small disfuncts.
6	GA + DBN = GADBN	Deep learning cannot detect all the attacks. Deep Belief Network contains Back propagation neural network that propagate error function information and if DBN is finely tuned, global optimization can be achieved.	The training time can be further reduced and the accuracy can be improved further.
7	GA + Multilayer Perceptron = GAMLP	GA helps in feature selection and MLP helps in classification. This technique was done on NSL- KDD dataset which doesn't lead to negative effect on training process. Supports different kinds of evaluation metrics.	Only slight increase in accuracy compared to existing methods.
8	VBGA (Vector Based Genetic Algorithm)	Here we treat Chromosomes as vectors and training data as matrices. There is an increase in detection rate and false positives are less compared to string based GA.	It can be improved for getting novel fitness function in which fitness is calculated directly from overlapping arrays of chromosomes.
9	GA + Profiling	Existing work is for signature based Intrusion Detection System for labeled data. Here, it adapts to new attacks iteratively, like business needs, staff preferences, and threats identification.	Not so good results. Not sure about large datasets.
10	GA + Multiple Vector Support Machines	To overcome drawbacks, high computational intensity and coarse function approximation of instance and model based methods. It is more efficient than conventional system with common feature selection technique. More accuracy, less computational complexity, Less communication overhead, improved security, less time for the training system.	Only used for Wireless Mesh Networks Security (WMNS).
11	GA	GA is used for cluster based routing for Wireless network security (WSN). To prevent attacks when cluster size is increased or number of surviving nodes are reduced, probabilistic voting-based filtering scheme, shortest path to test and got good results.	Difficult for most complex networks.
12	Genetic Crypto	Existing work has used some existing algorithm with GA. But, here it is a novel cryptographic algorithm with GA, easy to implement and secure in terms of key strength and attack time.	Takes little longer encryption than DES and AES.

13	Fuzzy C- Means + GA = GFC M	EA'S(Effective Algorithm) are effective for feat ure selection. GFCM is better compared to C4.5 and 2 times faster than FCM and 7 times in class ification accuracy.	Less accuracy compared to other fusion algo rithms.
14	IDS alert manageme nt with GA+2 cluste ring algorithms.	To overcome the disadvantages caused by indivi dual algorithms.2 cluster algorithm are based on GA and compared. They give better results and r educe false positive alerts.	IDS-number of alerts generated are failing.
15	ANN+GA	To take the advantages of both the techniques w here ANN classifies system features and predicts percentage of backdoor problem and GA gives deterministic answer to issue.	Accuracy for the classification can be further improved.
16	IDS+GA	This technique was proposed to overcome the li mitations of IDS like fidelity, resource usage an d reliability. This gave a result with a false positi ve rate of 0.3% and Detection Rate of 95%	The accuracy is less compared to the use of Genetic Algorithm where 99.8% accuracy ha s been achieved.
17	Hierarchical Takegi Sugeno Model using EA (Evolutionary A lgorithms)	Better than GA and Neuro- Fuzzy algorithm. It has been integrated with Intr usion Detection and prevention systems.	Suitable only for the light- weight risk assessment models.
18	Asymmetric Genetic Algorithm	It strengthens the security. The encryption and d ecryption are done end to end and has achieved a FPR of 0.2% and DR of almost 100%	_