ISSN 2394-739X

IJRSET JUNE Volume 9 Issue 6

International Journal for Research in Science Engineering & Technology (IJRSET)

https://www.doi.org/10.5281/zenodo.6759140

ENHANCED GENETIC ALGORITHM USES TSP (EGA-TSP) FOR NETWORK SECURITY

[1] Dr. P. E. Elango, [2] Mrs. R. Naleiny
[1, 2] Assistant Professor,
[1, 2] Department Of Computer Science,
[1, 2] Gobi Arts & Science College, Gobichettipalayam,
[1, 2] Tamilnadu, India.

ABSTRACT - Security is the conspicuous worry for the network and it is energetically prescribed to keep up with security. There exists a few methodologies has been endeavoured to address this difficult undertaking. This paper presents the appropriateness of the genetic algorithm (GA) for security concerns. The working of the GA vigorously relies upon the different variables incorporates: propagation operators, selection techniques, chromosome portrayal and issue type an exhaustive investigation of various selection techniques in proposed Enhanced genetic algorithm to settle Travelling Salesman Problem (EGA-TSP). Then thought about their presentation as far as the base distance expected to get the briefest way in TSP. Then, a security circumstance prediction model considering GA to tackle TSP is proposed to comprehend the security circumstance prediction for the attack graph information plane. As per the trials led, Rank based selection technique gave the best outcome with regards to separate.

Keywords: [Network Security, Genetic Algorithm, Situation, Rank, Tournament selection, TSP.]

1. INTRODUCTION

Network security is a broad term that covers a huge number of innovations, contraptions and cycles. In its most direct term, it is a lot of rules and game plans planned to defend the genuineness, security and accessibility of PC networks and data using both programming and gear advances. Every affiliation, paying little brain to gauge, industry or establishment, requires a degree of network security game plans put in a position to shield it from the consistently creating scene of digital dangers in the wild today. The current network configuration is puzzling and is stood up to with a danger environment that is consistently changing and attackers that are persistently endeavouring to find and exploit shortcomings. These shortcomings can exist in a wide number of districts, including contraptions, data, applications, clients and locations. In this manner, there is a lot of network security the board gadgets and applications being utilized today that address individual dangers and exploits and moreover managerial defiance. Exactly when several snapshots of individual time can make inevitable interference and tremendous damage an affiliation's essential concern and reputation, is key that these protection measures are set up.

Network security involves the policies, cycles and practices took on to prevent, recognize and screen unapproved access, misuse, change, or renouncing of a PC endlessly network open resources. Network security remembers the endorsement of induction to data for a network, which is compelled by the network head. Clients pick or are consigned an ID and secret expression or other affirming data that licenses them permission to data and undertakings inside their power. Network security covers a combination of PC networks, both public and private, that are used in normal positions: proceeding with trades and exchanges among associations, government offices and individuals. Networks can be private, for instance, inside an association, and others which might be accessible to community. Network security is related with affiliations, adventures, and various kinds of associations. It does as its title explains: it gets the network, as well as shielding and it being done to oversee errands. The most notable and clear way to deal with defending a network resource is by designating it a remarkable name and a contrasting secret key.

Genetic Algorithms (Gas) are "adaptive heuristic search algorithms" chips away at the Darwin's guideline of "survival of the fittest". GA has been applied in various fields of designing incorporates machine learning, image processing, linguistic deduction normal language processing, language translation and others. Individual each other in an age one that succeeds passed to the future. This paper, the correlation of various selection procedures for taking care of Travelling Salesman Problem (TSP) is introduced. TSP is NP-Complete "combinatorial optimization problem " in which point is to find the most limited course of a salesman for example voyaging beginning from his home city, covering every city in his rundown somewhere around once and getting once again to his home city. There are different ways to deal with settle TSP like brain networks, mimicked strengthening, branch and bound10, Genetic Algorithm and some more. Since Gas is optimization search algorithms utilized for limiting or amplifying specific capability is considered to address TSP in experiment.

2. EXISTING METHODOLOGY

2.1 Yanzhi Ren et.al proposed Detecting Wormhole Attacks in Delay-Tolerant Networks. Delay-tolerant networks are particularly valuable in giving strategic

administrations including crisis situations and combat zone applications. In any case, DTNs are helpless against wormhole attacks, in which a malevolent node records the parcels at one area and passages them to another plotting node, which transfers them locally into the network. Wormhole attacks are an extreme danger to ordinary network activity in DTNs. In this article portray different techniques that have been created to distinguish wormhole attacks. Be that as it may, the vast majority of them can't work proficiently in DTNs. To perceive the presence of a wormhole assault, propose a recognizable proof part that exploits the presence of an untouchable geology in the organization. Evaluated approach through expansive re-establishments using both Random Way Point and Zebranet adaptability models. Results demonstrate the way that the proposed strategy can distinguish wormhole attacks productively and actually in DTNs.

2.2 Bang-Cheng Zhang et.al a method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm. It is vital to lay out the forecasting model of the network security situation. Yet, the network security situation can't be noticed straightforwardly and must be estimated by other perceptible data. In this paper the network security situation is considered as a hidden way of behaving. In this manner, a determining model of organization security circumstance is proposed in view of the hidden belief rule base (BRB) model when the information sources are multi-faceted. To prepare the boundaries, an overhauled covariance matrix adaption evolution strategy (CMA-ES) algorithm is additionally evolved by adding a changed administrator. The context oriented examination shows that differentiated and various procedures, the proposed secret BRB model and the modified CMA-ES algorithm can anticipate the network security situation successfully to further develop the forecasting precision by taking advantage of qualitative knowledge.

2.3 M. Roopak et.al proposed Deep Learning Models for Cyber Security in IoT Networks. In this paper we propose profound learning models for the cyber security in IoT (Internet of Things) networks. IoT network is as a promising innovation which interfaces the living and non-living things all over the planet. The execution of IoT is developing quickly yet the cyber security is as yet a proviso, so it is powerless to numerous cyber-attacks and for the progress of any networks it most vital that the network is totally secure, any other way individuals could be hesitant to utilize this innovation. DdoS (Distributed Denial of Service) attack has impacted numerous IoT networks in ongoing past that has brought about tremendous misfortunes. We have proposed significant learning models and evaluated those using latest CICIDS2017 datasets for DdoS assault area which has given most vital precision as 97.16% additionally proposed models are contrasted and machine learning algorithms. This paper likewise recognizes open research difficulties for utilization of profound learning algorithm for IoT cyber security.

3. PROPOSED METHODOLOGY

3.1 Genetic Algorithm and Security Concerns

Maintaining security is energetically prescribed to guarantee protected and confided in communication, yet it is a moving undertaking to achieve. It has been seen that communication over the Internet or over other network framework experiences because of interruptions and abuse of the data. It roused researchers to endeavor this moving undertaking to accomplish computer network security. There exist a few methodologies being utilized for the interruption recognition, however tragically not even one of them is flawless. In the new years, a few empowering results have been gotten, consolidating the GA. This segment basically talks about the methodologies created for the network security where GA has been used.

The GA for the network security and proposed a changed variant of the GA utilizes exceptional wellness capability to distinguish security. This conversation prompts an end that the force of the GA can be used for the network security and optimization reason. The selection (survival selection, and parent selection) is essential ordnance of the GA, significantly adds to the achievement. Additionally, it is worth to specify that there are a few selection techniques existing and more often than easy to pick the right one to play out the computational experiments.

3.2 Enhanced Genetic Algorithm uses TSP (EGA-TSP)

The parts of GA and their activities for tackling TSP. GA utilize a stochastic methodology for haphazardly searching and enhancing the arrangements. It guarantees irregularity and productivity in the search. In GA, a chromosome shows a potential arrangement. The chromosome in TSP can be addressed by the 'path' portrayal. In TSP principal point is to limit the distance that need to travel. Consequently, 'path' is the arrangement that necessities to enhance and hence, it is addressed as a chromosome in the EGA-TSP process.

Algorithm-1: Procedure EGA-TSP (No. Of cities)
Begin
Initialize GA and TSP parameters:
No. Of cities
Cities' coordinates
G_{max} Shows the maximum number of generations
Size of the population
Crossover rate
Mutation rate
Tournament size
Generate random, initial population P (G)
Fitness ← Evaluate P (G)
While (((Result is not Optimum) OR (Generation $<G_{max}$))
Do select a couple of parent population P1 from P (G)
Apply crossover to P1
Apply mutation to P1
G=G+1
Update Population (P(G),P1(G))
End while
Display optimum result
End

The strategy for TSP utilizing GA is made sense of utilizing Algorithm-1 - begins by introducing GA's boundaries like complete ages, the size of the populace, the size of the competition and hybrid, transformation probabilities. EGA-TSP additionally supplies significant

information like Number of urban communities and their directions. Then, at that point, irregular populace is created and the wellness of every chromosome is determined. Another age is framed with the assistance of selection, hybrid and transformation operators. The selection administrator picks two parents from the ongoing age, which then imitate another kid with the assistance of hybrid and transformation operators. This new youngster chromosome shapes the future, which is superior to the past one. This cycle go on until an ideal arrangement is accomplished, or age arrives at its greatest cutoff. An answer is supposed to be ideal if a specific level of the populace (say 90%) have same ideal chromosome, out of which the best one is picked as the ideal arrangement.

Three selection plans: Roulette wheel, Rank based and Tournament selection are chosen. Roulette Wheel Selection by Holland accepted that the selection likelihood of an individual chromosome is straightforwardly connected with the wellness. It works likewise as a roulette wheel, in which, the selection likelihood relies upon the focal point of the roulette wheel. Similarly, in GA, an entire populace is divided in various areas and the selection likelihood of an individual (one area) is addressed as an individual's wellness to the all out wellness of the populace. The likelihood of selection of an individual I_i can be calculated using equation (1).

$$PS(I_i) = \frac{f(I_i)}{\sum_{i=1}^{n} f(I_j)}; j = 1,2,\dots.,n \quad (1)$$

Where 'n' is the population size and $f(I_i)$ is the fitness value of an individual I_i .

Linear Ranking Selection was proposed by Baker. In this, an individual in a populace is first arranged according to their wellness, and afterward task of the position happens, 'N' is the position given to the best individual, though rank '1' is allotted to awful. The likelihood of selection of an individual '1' is assigned to the worst. The probability of selection of an individual I_i is given in equation (2).

$$P_i = \frac{1}{n}\left(n^- + (n^+ - n^-)\frac{i-1}{N-1}\right); i \in \{1,\dots.,N\} \quad (2)$$

Where $P_i, \frac{n^-}{N}$ and $\frac{n^+}{N}$ respectively denotes the selection probability of i_{th} individual, worst individual and best individual.

Tournament Selection the most famous selection techniques because of its less time intricacy and in this, 'n' arbitrary individuals are looked over the whole populace and the individual with best wellness esteem is chosen for the further processing of EGA-TSP. Number of individuals participating in every tournament is known as tournament size.

4. EXPERIMENT RESULTS

4.1 Accuracy

Particle	DTN	CMA-ES	Proposed EGA-TSP
1	20	30	50
2	35	45	65
3	40	50	70
4	55	65	85
5	65	75	95

Table 1.Comparison of Accuracy

The table 1 Comparison of Accuracy values explain the different values of existing algorithms (DTN, CMA-ES) and proposed EGA-TSP. While comparing the Existing algorithm (DTN, CMA-ES) and proposed EGA-TSP, provides the better results.

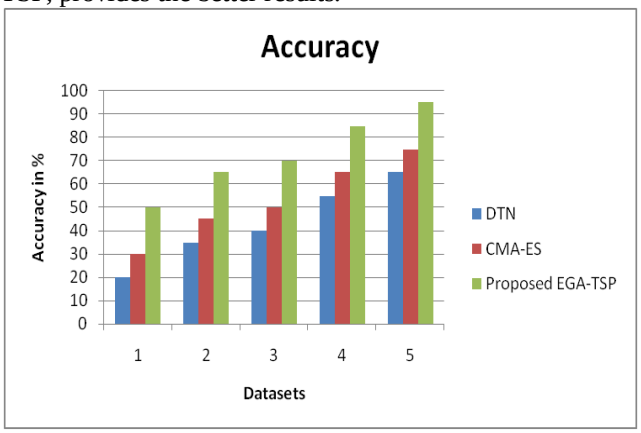

Figure 1.Comparison of chart Accuracy

The figure 1 Comparison chart of Accuracy values explain the different values of existing algorithms (DTN, CMA-ES) and proposed EGA-TSP. X axis denote the Nodes Accuracy in percentage and y axis denotes the Particles. While comparing the Existing algorithm (DTN, CMA-ES) and proposed EGA-TSP, provides the better results. The existing algorithm values start from 20 to 65, 30 to 75 and proposed EGA-TSP values starts from 50 to 95.

Prediction Errors

Particle	DTN	CMA-ES	Proposed EGA-TSP
5	0.80	0.91	1.10
10	0.82	0.92	1.11
15	0.83	0.93	1.15
20	0.85	0.95	1.17
25	0.87	0.97	1.21

Table 2.Comparison of Prediction Errors

The table 2 Comparison of Prediction Errors values explain the different values of existing algorithms (DTN, CMA-ES) and proposed EGA-TSP. While comparing the Existing algorithm (DTN, CMA-ES) and proposed EGA-TSP provides the better results.

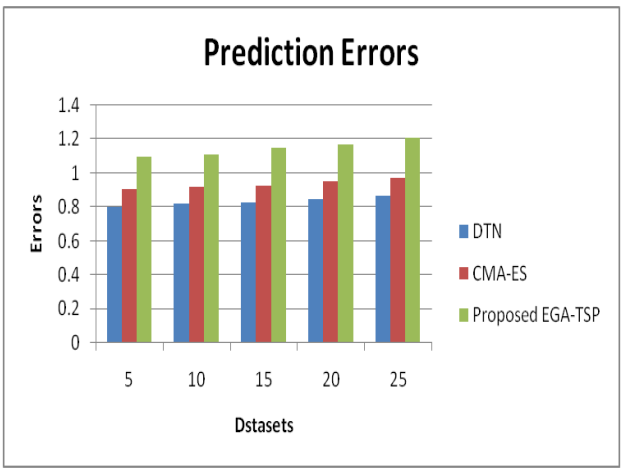

Figure 2.Comparison of chart Prediction Errors

The figure 2 Comparison chart of Prediction Errors values explain the different values of existing algorithms (DTN, CMA-ES) and proposed EGA-TSP. X axis denote the Errors and y axis denotes the Particles. While comparing the Existing algorithm (DTN, CMA-ES) and proposed EGA-TSP, provides the better results. The existing algorithm values start from 0.80 to 0.87, 0.91 to 0.97 and proposed EGA-TSP values starts from 1.10 to 1.21.

CONCLUSION

This paper designs an extensive investigation of various selection techniques in proposed Enhanced genetic algorithm to settle Travelling Salesman Problem (EGA-TSP). Then compared their performance as far as the base distance expected to get the shortest path in EGA-TSP. For examination reason, have taken 20, 40 and 60-city TSP with 10 examples for every selection conspired; each example I a normal of 10 tests run. EGA-TSP gives the specific results, yet gives most proper outcome for the ideal problem. It was then trailed by Roulette wheel and Tournament selection.

REFERENCES

[1]. M. Sheng, H. Liu, X. Yang, W. Wang, J. Huang and B. Wang, "Network Security Situation Prediction in Software Defined Networking Data Plane," 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA), 2020, pp. 475-479, doi: 10.1109/AEECA49918.2020.9213592.

[2]. Y. Kai, H. Qiang and M. Yixuan, "Construction of Network Security Perception System Using Elman Neural Network," 2021 2nd International Conference on Computer Communication and Network Security (CCNS), 2021, pp. 187-190, doi: 10.1109/CCNS53852.2021.00042.

[3]. Y. Wang, J. Lu, Z. Wu and Y. Lu, "Component Based Security Control for Information Network," The Proceedings of the Multiconference on "Computational Engineering in Systems Applications", 2006, pp. 1357-1360, doi: 10.1109/CESA.2006.4281849.

[4]. M. H. Khyavi and M. Rahimi, "Conceptual Model for Security in Next Generation Network," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 591-595, doi: 10.1109/WAINA.2016.12.

[5]. G. Goth, "Functionality Meets Terminology to Address Network Security Vulnerabilities," in IEEE Distributed Systems Online, vol. 7, no. 6, pp. 4-4, June 2006, doi: 10.1109/MDSO.2006.40.

[6]. T. Yin, L. Han, C. Wan, X. Qu and Y. Li, "The Probability of Trojan Attacks on Multi-level Security Strategy Based Network," 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 555-559, doi: 10.1109/MINES.2010.122.

[7]. "IEE Colloquium on 'Security and Networks' (Digest No.114)," IEE Colloquium on Security and Networks, 1990, pp. 0_1-.

[8]. Z. Qu and X. Wang, "Study of Rough Set and Clustering Algorithm in Network Security Management," 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 326-329, doi: 10.1109/NSWCTC.2009.47.

[9]. Z. Chen, "Research on the Application of Intelligent Learning Algorithms in Network Security Situation Awareness and Prediction Methods," 2021 5th Asian Conference on Artificial Intelligence Technology (ACAIT), 2021, pp. 309-311, doi: 10.1109/ACAIT53529.2021.9731205.

[10]. J. Li and C. Dong, "Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 483-485, doi: 10.1109/NSWCTC.2010.247.