Plagiarism - Report

Originality Assessment

14%

Overall Similarity

Date: Feb 20, 2024
Matches: 567 / 3955 words
Sources: 21

Remarks: Low similarity detected, check with your supervisor if changes are required.

Verify Report:

A GENETIC ALGORITHM BASED HYBRID ROUTING TECHNIQUE FOR IoT SYSTEMS

RAKESH KUMAR

Department of Electronics and Communication Engineering, IKG Punjab Technical University,

Kapurthala, Pb, India

drrakeshbanga@gmail.com

Abstract

Internet is gaining new heights in the today's technological environment. 2 Internet of things (IoT) is a new class of Internet based heterogeneous networked application systems which uses various types of sensor/detectors and devices for the exchange and collection of data. Devices need to be in the radio range and must remain continuously connected 15 to the internet. IoT can sense and control the objects remotely across existing networked architecture and builds chances for direct combination among the physical world and computer-based systems. It is believed that, in future many of the household application will be based on IoT. Due to their applications in situations such as building home automation, emergencies, crisis management, energy management and healthcare, message security becomes of top importance in IoT. An optimized 2 routing scheme using the intelligent mathematical techniques, which includes Genetic Algorithms(GA) and Analytical Hierarchy Process(AHP), is proposed here and an optimized route can be encrypted using cryptanalytic techniques. Simulation results of GA and AHP are also presented here for the proposed network. It has been found that overall efficiency of the IoT system can be greatly improved with the proposed model. A comparison is also provided in discussion section which demonstrates that hybrid algorithms developed for IoT systems performs much better than traditional routing algorithms.

Keywords: IoT; AHP; GA; Cryptanalytic Techniques; WSN

1.Introduction

IoT is networking of physical objects and it simply means that anything is connected anywhere at any time. It was the year 1832, when the first electromagnetic telegraph equipment was designed by Samuel F B Morse. In year 1980, Coca Cola vending machine came into existence at the Carnegie

Melan University, which permitted them to count the number of cans that were being dispensed. Later in the year 1990, a toaster was connected to the internet, by John Romkey, using TCP/IP protocol. Until 1998, the term "Internet of Things" didn't even exist. The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Finally, it was the year 1999 when Kevin Ashton coined the term "Internet of Things" first time during his presentation at Procter and Gamble [1]]. Radio Frequency Identifiers (RFID) can be said as the major prerequisite for the development of this technology as it becomes very easy for the computers to manage and invent the devices if they are equipped with certain kind of identifiers like RFID. Quick response (QR) codes, optical tags, Bluetooth and low energy devices are also some of the devices for IoT. It is believed that by the year 2025, approximately one trillion devices will be connected through IoT and in the near future 5G and IoT will be used for remote surgery, connected ambulances and remote sensor monitoring. RFID, Bluetooth, WiFi, Zigbee and 6LoWPAN(IPv6 Low Power Wireless Personal Area Network) allows systems to be connected to internet and cloud service can be used to collect, store and analyse the data collected by various sensors deployed in IoT environment for further processing[2] IoT involves the use of smart objects which possesses smart features so that they can be easily identified and smart features includes sensing abilities, physical shape, unique identity, processing powers, unique address and communication capabilities. Fig 1.shows the future projections by the IoT.

Fig 1. Global IoT Market Forecast 2017-2025

2.Security Concerns in IoT

IoT is basically a network of real-world systems and their interaction and initially it was a M2M with unique characteristics and subscriptions. Unattended operations without the human interventions were possible by WLAN and doing this can cause breach of security of the IoT system and there are following major security issues in IoT [2]

2.1.Front End Sensors and Equipment

 Unauthorized access to data

☐ Threats to Internet

☐ DoS attack

☐ Attacks and Privacy analysis of M2M or contact information.

☐ Attacks to availability of M2M or contact information

2.2. Network

☐ Unauthorized access to data

☐ Unauthorized access to service

☐ Virus or Malware attacks

2.3. Back End Systems

☐ Safety management of code resources

2.3.1. Front-end Sensors and Equipment accepts information through the built-in sensors and send the data using M2M device, thus attaining synchronized services of multiple sensors. This practice comprises the security of machines with business application and node connectivity. Machine or perception nodes are mostly dispersed in the absence of monitoring scenarios. An intruder can easily access these devices causing damage or harmful actions on these nodes. Possible threats are examined and are characterized to unauthorized access to data, threats to the Internet and denial of service attack.

2.3.2. Network plays a very vital part in providing a more complete interconnectedness capability and effectiveness 6 as well as reliable QoS in IoTs. As 3 a large number of nodes participate in sending data and these large number of nodes and groups exist in IoT may be resulted in denial-of-service attacks.

2.3.3. Back-end systems form the gateway, middleware, which has high security requirements, and gathering, examining sensor data in real time or pseudo real-time to increase business intelligence. The security of IoT system can be defined through several terms which includes privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time.[3]

3.Applications of IoT

This section of paper focuses on application of IoT in various domains including environmental, commercial, industrial, smart cities, health and infrastructural which are further reclassified as under

[4]:

3.1. Healthcare

☐ Smart Wearables

☐ Personal Remote health Monitoring

3.2. Infrastructural

☐ Real time performance

☐ Energy Efficiency

3.3. Industrial

☐ Smart Grid

☐ Smart Metering

3.4. Commercial

☐ Shopping Systems

☐ Retail

3.5. Environmental

☐ Smart Farming

☐ Smart Agriculture

☐ Wild Vegetation

☐ Climate Changes Monitoring

3.6. Smart Cities

☐ Smart Homes

☐ Smart Buildings

☐ Urban Computing

☐ Traffic Monitoring

☐ Security and Emergencies

5 In addition to the applications cited above, figure 2 provides a detailed application spectrum of IoT.

Fig 2. Application Spectrum of IoT.

4. Literature Review of the Related work

K Saleem et al stated that Ant colony optimization can also be used to optimize the parameters like, energy level, delay and velocity and the designed algorithm may have enhanced feature of multipath capability to avoid the congestion in the WSN [5]. Genetic algorithms can be used to minimize the energy store of the wireless sensor nodes and accordingly its life time can be maximized. GAs can also be used to optimize the minimum cost function and minimum number of nodes can be selected to obtain the optimal route in terms of energy consumption in WSN [6]. Wireless sensor nodes always have a constraint of energy, which directs hints at lifetime of a node in a wireless network. Analytical hierarchy process can be used to design energy aware geographical multipath routing scheme for WSN which can further and distance to destination location, remaining battery capacity and queue size of candidate sensor node in local communication range can be considered as three parameters for selection of the next relay node[7].Energy expenditure and network life time is very vital concern for implementing any application of WSN and genetic algorithms can easily address such routing algorithms for WSN[8].Wireless sensor networks constitute IoT and Ant Lion Optimization (ALO) can be used for getting the optimal path for high speed data transfer with a focus on minimizing End to End Delay (E2D), overhead, and energy consumption and maximization of packet delivery rate in the data transfer[9].Energy Efficient Probabilistic Routing (EEPR) protocol controls the transmission of the routing request packets stochastically in order to increase the network lifetime and decrease the packet loss under the flooding algorithm in IoT [10].In WSN, network life time and energy consumption are the two most important constraints which require maximum attention. Genetic Algorithms (GA) can be used to formulate a fitness function where protocols performance can be analysed. Simulations results in JPAC, MATLAB, and NS and be compared with present protocols and optimization of the network life time and energy consumption can be achieved[11].A new genetic algorithm based routing technique called MEGA(Maximum

Enhanced Genetic Algorithm) which use the local search mechanism and sleep wake-up mechanism can also optimize the network life time 2 and energy consumption constraints in deploying the WSN[12].In IoT, sensor nodes can be clustered which can be performed on the basis of energy of 15 sensor nodes and genetic algorithm can be used to energy cost of the cluster head and trust level of sensor nodes. The optimal path will provide better speed, more reliability and more lifetime [13]. Genetic Algorithms 3 can be used to develop a Genetic Algorithm based Energy Efficient Routing Protocol(GAEER) which is also based on constructing Cluster Head(CH) which incorporates nodes residual energy, distance, node density and network's remaining energy and the simulation can be done in MATLAB which outperforms the other protocols with different network criteria's. GAEER improves stability period, network lifetime by 26.6% and 67.7% and 76.8% and 173.6% as compared to GADALEACH, and GAOC, respectively [14].

4.Proposed Model

4.1 Problem Formulation

The main objective of this routing model is to select an optimized and secured route among the different zones and each zone having certain number of devices. When the optimized route gets selected with its respective cost function (high throughput route), the message is sent through the route using transposition ciphers with a message divided into various packets (letters) and then the encrypted message will be transmitted through the selected route. 2 On the other side each letter is decrypted according to the agent code or key and the original message is retrieved. 4 In this work, we have taken up an IoT environment between two places on a map and have divided the region into various zones consisting in each region, so as to standardize input data for normalization. In this work three parameters will be considered while selecting optimal route i.e. Latency, Power Consumption and Network Congestion. All these parameters shall be given different priorities according 6 to the AHP scale.The design and development of this routing protocol shall make use of three techniques which are Evolutionary Algorithms, Analytical Hierarchy Process and Encryption algorithms.

4.1.1 4 Genetic Algorithm (GA)

The Genetic Algorithm (GA) is a search heuristic that is based on theory of evolution, stressing on the survival of the fittest, inspired by crossover, mutation, recombination and selection operators

[6][8]. Candidate solutions to the problems of optimization play the role of individuals in a population, and the objective/fitness/cost function calculates the quality of the solution. Evolution of the population then takes place after the repetitive application of the GA operators. Genetic algorithms are best suited for approximation solution of various engineering problems in real life.

1.[Start] Generate random population of n chromosomes (suitable solutions for the problem)

2. [Fitness] Evaluate the fitness f (x) of each chromosome x in the population.

3. [New population] Create a new population by repeating following steps until the new population is complete.

a. [Selection] Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger are the chances for selection)

b. [Crossover] With a crossover probability, cross-over the parents to form new offspring (children). If no crossover was performed offspring is the exact copy of parents.

c. [Mutation] with a mutation probability, it mutates new offspring at each locus (position in chromosome).

4 [Replace] Use newly generated population for a further run of the program.

5 [Test] If the end condition is satisfied, stops, and returns the best solution in the current population

6 [Loop] go to step 2.

Fig 3. Genetic Algorithm Flow Chart

4.1.2 Analytical Hierarchy Process (AHP)

As proposed by Xiaoling Wu et.al in [7], The Analytical Hierarchy Process (AHP) is a decision-making procedure which breaks up a complex task into a hierarchy of basic sub issues, blends their relevance to the issue, and discovers the best results. AHP is utilized to focus the IoT devices which are qualified to be chosen as next hop transfer. Following three steps can be utilized to get the solution in this process.

• Information is gathered and the next hop routing nodes selection problem is formulated as a decision hierarchy of independent factors.

- Calculates the relative local weights of decision factors.

- Processing the values got in the results from above steps to attain the overall weight of each alternative node and choose the nodes with largest weight values which will be eligible for next hop relay nodes.

Fig 4. AHP Multi objective Selection Criteria

4.1.3 Encryption Algorithm

Following are steps involved in encryption –

a. Pass in the agent key to decide the encoding pattern of the message at the transmitting side.

b. Once the agent key is entered, the message is passed to the transmitting end which gets encrypted 2 according to the agent key (ceaser encryption). This sort of encryption is safe from brute force attack as the message gets randomly shuffled infinite no of times which makes the information more secure.

c. When the packet arrive at receiving side it gets decoded and the original message is received

5.Simulations and Results

The simulation is done for various zones (the user defines 6 the number of zones) and the optimized routing is determined by the value of cost function. The optimized route is selected with the use of analytical hierarchy process and evolutionary algorithm. Once the optimized route is selected, the encryption algorithm is applied to make the routing secure.

$$\text{Cost Function} = A_1\lambda_1 + A_2\lambda_2 + A_3\lambda_3 \qquad (5.1)$$

Where λ's are weights and will be calculated using comparison matrix and A1-A3 are local constants and the values of local constants are given as below: -

A1= 0.15, A2= 0.35, A3= 0.50

Enter the agent code: - r,

Enter the message: - information

Enter the encrypted message: - cDWvkFnlcvD

1. For the transfer of the first alphabet 'c' the optimized path is to be decided with the help of 13 analytical hierarchy process and evolutionary algorithm. Since we have taken 3 zones with each zone consisting of 3 nodes, in total there are 27 values.

Performance indices for AHP: -

1 - Equally important

2 - Moderately important

4- Strongly important

6- More strongly important

8- Most strongly important

Following tables will generate the weights associated for each node in the three regions: -

For ZONE 1

NODE 19 1:

Table 1. Comparison Matrix for IoT device 1 in Zone 1

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

6

4

Power Consumption

0.16

1

2

Network Congestion

0.25

0.5

1

NODE 2:

Table 2. Comparison Matrix for IoT device 2 in Zone 1

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

2

8

Power Consumption

0.5

1

6

Network Congestion

0.125

0.16

1

NODE 3:

Table 3. Comparison Matrix for IoT device 3 in Zone 1

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

1

8

Power Consumption

1

1

6

Network Congestion

0.125

0.16

1

For Zone 2

NODE 1:

Table 4. Comparison Matrix for IoT device 1 in Zone 2

Attributes	Latency	Power Consumption	Network Congestion
Latency	1	1	1
Power Consumption	1	1	1
Network Congestion	1	1	1

NODE 2:

Table 5. Comparison Matrix for IoT device 2 in Zone 2

Attributes	Latency	Power Consumption	Network Congestion
Latency	1	4	6
Power Consumption	0.25	1	2
Network Congestion	0.15	0.5	1

NODE 3:

Table 6. Comparison Matrix for IoT device 3 in Zone 2

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

4

2

Power Consumption

0.25

1

2

Network Congestion

0.5

0.5

1

For Zone 3

NODE 1:

Table 7. Comparison Matrix for IoT device 2 in Zone 1

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

4

1

Power Consumption

0.25

1

2

Network Congestion

1

0.25

1

NODE 2:

Table 8. Comparison Matrix for IoT device 2 in Zone 3

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

1

1

Power Consumption

1

1

1

Network Congestion

1

1

1

NODE 3:

Table 9. Comparison Matrix for IoT device 3 in Zone 3

Attributes

Latency

Power Consumption

Network Congestion

Latency

1

2

4

Power Consumption

0.5

1

6

Network Congestion

0.25

0.16

1

In a similar way, comparison matrix for all IoT devices for remaining words of the message in remaining zone can be obtained.

Cost functions in the decimal form 4 for the first alphabet: -

0.230632

0.240936

0.262186

0.333333

0.225564

0.265584

0.294487

0.333333

0.259680

Cost functions in binary form are:

00010111

00011000

00011010

00100001

00010110

00100001

00011101

00100001

00011001

No of generations: 2

Crossover point: 2

Crossover point: 5

Optimized cost function in decimal form is

248

136

164

Genetic Algorithm Result: -

The nodes for optimized route for the encrypted message transmission will be as under

Source Node is IoT device 3 in Zone 1

Intermediate Node is IoT device 3 in Zone 2

Destination Node is IoT device 2 in Zone 3

So, the first encrypted letter which reaches the destination node will be 'c'. Similarly, every encrypted

alphabet of the whole message will be transmitted one by one along with the optimized route and

when all the alphabets has been transmitted, then the whole message will be decrypted at the receiver

end.

The screenshots given below shows the result of simulations. Due to space constraints, simulations for

the optimal route for only first alphabet are shown here

Simulations:

Fig 5: Simulations results showing AHP Multi objective criteria importance's

Fig 6: Simulations results showing the input values for all nodes in zone 1 to make comparison matrix

Fig 7: Simulations results showing the input values for all nodes in zone 2 and 3 to make comparison matrix

Fig 8: Simulation results showing Cost functions of comparison matrix in binary form

Fig 9: Delivery of 1st character of encrypted message

6.Discussions

4 Results obtained from the hybrid algorithm, developed by the use of combined features of genetic algorithm and analytical hierarchy process shows that in simulations, a message is transmitted through an optimized route and AHP works in accordance with user priority depending upon 7 the IoT environment. User priority may be latency, power consumption and network congestion. This will improve the output of the overall IoT network as the route is optimized and there will be lesser power consumption, lesser network congestion and lower latency depending upon the priority assigned by the user to these parameters according to AHP scale. In one case, user can assign highest priority to latency and lower 7 to network congestion as well as power consumption whereas in second case, highest priority can be assigned to network congestion and lowest to latency and power consumption and similarly there can be other combinations too. So, 4 the use of the adaptive techniques gives an optimized route which is further secured by cryptographic techniques, which can be easily seen in the simulation results. In this proposed model 3 nodes have been considered 19 in each zone and zones

are source zone, intermediate zone and destination zone. This algorithm calculates the results 2 based on the theoretical backgrounds of EA, AHP and Encryption techniques used and code is developed in high level language, C++.It is up to the user to enter the no. of generations and no. of crossover points as per the choice during the running of the program code. Based on the optimized cost function, one node in each zone gets automatically selected for transmission of the message. Each alphabet of the entire message will be transmitted through this optimized route one after the other in the encrypted form and it will be automatically decrypted in the original plain text when the whole message is received at the destination node. For the comparison purpose each developed algorithm was taken individually and results showed that the remaining energy of nodes was more in case of hybrid algorithm as compared to AHP ,GAand AODV.Similarly latency was less in case of hybrid algorithm and was more in case of AODV.Remaining bandwidth was available more in hybrid algorithms as compared to AHP,GA and AODV.A consolidated comparison of the three algorithms has been 4 given in the table.

Table 10. Consolidated comparison of Algorithms

Parameters/Algorithms	Latency (Seconds)	Remaining Bandwidth (Kbs)	Energy Remaining (Joules)
AODV	1.28	1040512	43.70
AHP	1.05	1041856	44.75
GA	0.42	1045888	47.90
Hybrid Algorithms	0.27	1047232	48.85

7. Conclusions

By using genetic algorithms (GA) and analytical hierarchy process (AHP) for routing, the IoT network throughput can be greatly improved in comparison to the existing routing algorithms. In this algorithm the message that is sent through the optimized route is secured from hacking, as the security concern has been taken care of by applying data encryption methods with transposition ciphers. From the results obtained it can be concluded that the use of adaptive techniques in combination with the mathematical tools such as AHP, brings a pronounced throughput improvement in ad-hoc networks which results in a more secured and protected message transmission. By using Genetic Algorithms and Analytical Hierarchy Process for routing in IoT, the throughput has shown an improvement of 70% to 85% in comparison to the existing routing algorithms. In the comparison of latency between AODV and hybrid algorithm,it can be concluded that latency in hybrid algorithm is less than the latency of AODV by 82.5% or in other sense it can be also be said that latency in hybrid algorithm is near about 6 times less than the latency in AODV with source as node 1 in zone 1 and destination as node 1 in zone 3.

9.References

1.Carsten Mapple, Security and privacy in the internet of things, Journal of Cyber Policy , 2(2017) 155-184.

2.MourvikaShirode, Monika Adaling, JyotiBiradar, Trupti Mate, IoT Based Water Quality Monitoring System, International Journal of Scientific Research in Computer Science, Engineering and

Information Technology (IJSRCSEIT) | 3(2018)

3.J Sathish Kumar,Dhiren R Patel,A Survey of 8 Internet of Things: Security and Privacy Issues, International Journal of Computer Applications. 90(2014) 20-26.

4. Rosilah Hassan ,Faizan Qamar ,Mohammad Kamrul Hasan ,Azana Hafizah Mohd Aman and Amjed Sid Ahmed, Internet of Things and Its Applications: A Comprehensive Survey, MPDI Journal Symmetry, 12(2020) 1-29,doi:10.3390/sym12101674.

5.K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, R. A. Rashid, A Self-Optimized Multipath 17 Routing Protocol for Wireless Sensor Networks, International Journal of Recent Trends in Engineering, 2 (2009) 93-97.

6.Nesa Sudha, Dr. M. L. Valarmathi, T.Christopahpaul Neyandar, Optimizing Energy in WSN using Evolutionary Algorithm, IJCA Proceedings on 9 International Conference on VLSI, Communication & Instrumentation (ICVCI),2(2011) 26-29.

7. Xiao ling Wu, Jinsung Cho, Brian J. d'Auriol, and Sungyoung Lee, 16 Energy-Aware Routing for Wireless Sensor Networks by AHP, IFIP International Federation for Information Processing, (2007) 446–455.

8.Shauban Ali Solangi, Dil Nawaz Hakro,Intzar Ali Lashari, Khalil-ur-Rehman Khoumbati,Zulfiqar Ali Bhutto, Maryam Hameed, Genetic Algorithm Applications 21 in Wireless Sensor Networks (WSN): A Review, International Journal of Management Sciences and Business Research, 6 (2017) 152-166.

9. Kratika Varnshney, Sweta Tripathi and Viabhav Purvar,An Efficient and Reliable Optimized 10 Routing Protocol for IoT Network in Agriculture, IEEE International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (Bhilai,India,2021), DOI: 10.1109/ICAECT49130.2021.9392553

10. Sang-Hyun Park, Seungryong Cho, and Jung-Ryun Lee, Energy-Efficient Probabilistic Routing Algorithm 11 for Internet of Things, Journal of Applied Mathematics ,2014(2014) 1-7.

11. Ali Norouzi and A Halim Zaim, Genetic Algorithm Application in Optimization of Wireless Sensor Networks, The Scientific World Journal, (2014), https://doi.org/10.1155/2014/286575.

12. Aishwarya S Hampiholi and B P Vijaya Kumar, Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with existing protocols, 3rd International Conference on Circuits, Control, Communication and Computing (Bangalore, India 2018),

13. Amol V Dhumane,Rajesh S Prasad,Jayashree R Prasad, An optimal routing algorithm for Internet of Things Enabling Technologies, 03(2017) 1-117.

14. Roshan Lal and Kanika Sharma, GAEER: Genetic Algorithm Based Energy Efficient Routing Protocol In Wireless Sensor Network, International Journal of Scientific and Technology Research,09 (2020) 538-544.

Sources

1
https://github.com/KendallPark/genetic-algorithm
INTERNET
3%

2
https://www.mdpi.com/1424-8220/22/1/251
INTERNET
2%

3
https://www.researchgate.net/publication/353631357_A_Survey_on_Enhanced_Energy_Efficient_Routing_Protocol_of_WSN_for_Internet_of_Things
INTERNET
2%

4
https://www.researchgate.net/publication/368244093_Genetic_algorithms_theory_genetic_operators_solutions_and_applications
INTERNET
1%

5
https://en.wikipedia.org/wiki/Evolutionary_algorithm
INTERNET
1%

6
https://www.isixsigma.com/dictionary/analytic-hierarchy-process-ahp/
INTERNET
1%

7
https://www.mdpi.com/1424-8220/21/8/2681
INTERNET
1%

8
https://course.ccs.neu.edu/cs7680su18/resources/pxc3894454.pdf
INTERNET
<1%

9
https://www.ijcaonline.org/proceedings/icvci/number12/2719-1472
INTERNET
<1%

10
https://www.semanticscholar.org/paper/An-Efficient-and-Reliable-Optimized-Routing-for-IoT-Varshney-Tripathi/74c6da9fb1637e811cbd84ee78576b55da42afa9/figure/10
INTERNET
<1%

11
https://doaj.org/article/8f6cc2f03d6f43fab104cf6fbaaa1938
INTERNET
<1%

12
http://infonomics-society.org/wp-content/uploads/ijicr/published-papers/volume-6-2015/Performance-Comparison-of-Simulated-Annealing-GA-and-ACO-Applied-to-TSP.pdf
INTERNET
<1%

13
https://link.springer.com/article/10.1007/s10479-021-04432-2
INTERNET
<1%

14
https://link.springer.com/article/10.1007/s11235-017-0324-1
INTERNET
<1%

15 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9677573/
    INTERNET
    <1%

16 https://dl.acm.org/doi/10.5555/1778978.1779033
    INTERNET
    <1%

17 https://scholar.google.com.my/citations?user=M-oAwGEAAAAJ&hl=en
    INTERNET
    <1%

18 https://mail.ijstr.org/final-print/jun2020/Gaeer-Genetic-Algorithm-Based-Energy-Efficient-Routing-Protocol-In-
    Wireless-Sensor-Network.pdf
    INTERNET
    <1%

19 https://www.civil.iitb.ac.in/tvm/1100_LnTse/204_lnTse/plain/plain.html
    INTERNET
    <1%

20 https://scholar.google.com/citations?user=83CPZ0YAAAAJ
    INTERNET
    <1%

21 https://www.researchgate.net/figure/Classifiaction-of-clustering-algorithms_fig1_284097388
    INTERNET
    <1%

EXCLUDE CUSTOM MATCHES   OFF

EXCLUDE QUOTES   OFF

EXCLUDE BIBLIOGRAPHY   OFF