International Journal of
Advanced Science Computing and Engineering

Journal Homepage www.ijasce.org/index.php/ijasce

Genetic Algorithm based Secure Hybrid Routing Technique for IoT Framework

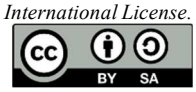
Rakesh Kumar [a,*]

[a] *Department of Electronics and Communication Engineering, IKGPTU, Kapurthala, Punjab, 144603, India*
Corresponding author: [*]drrakeshbanga@gmail.com

***Abstract*— Internet is gaining new heights in today's technological environment. Internet of things (IoT) is a new class of Internet-based heterogeneous networked application systems that uses various types of sensors/detectors and devices for the exchange and collection of data. Due to their applications in situations such as building home automation, emergencies, crisis management, energy management, and healthcare, path optimization and message security becomes of topmost importance in IoT. An optimized routing scheme using intelligent mathematical techniques including Genetic Algorithms (GA) and Analytical Hierarchy Process (AHP), is proposed here and an optimized route can be encrypted using cryptographic techniques. From the simulation results, it has been found that the overall efficiency of the IoT system can be greatly improved with the proposed model. A comparison is also provided in the discussion section which demonstrates that hybrid algorithms developed for IoT systems perform much better than traditional routing algorithms.**

***Keywords*— AHP; cryptographic techniques; GA; IoT; WSN.**

Manuscript received 15 Feb. 2024; revised 20 Mar. 2024; accepted 2 Apr. 2024. Date of publication 30 Apr. 2024.



I. INTRODUCTION

IoT is the 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 the 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 Centre 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 computers to manage and invent the devices if they are equipped with certain kinds 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 the internet, and cloud service can be used to collect, store and investigate the data collected by various sensors deployed in IoT environment for further processing [2].IoT involves the use of smart objects which possess smart features so that they can be easily identified and smart features include sensing abilities, physical shape, unique identity, processing powers, unique address, and communication capabilities. Fig 1shows the future projections by the IoT.

A. 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 human interventions were possible by WLAN and doing this can cause a breach of security of the IoT system and there are the following major security issues in IoT [2]

B. Front End Sensors and Equipment

1. Unauthorized access to data
2. Threats to Internet

3. DoS attack
4. Attacks and Privacy analysis of M2M or contact information.
5. Attacks to availability of M2M or contact information

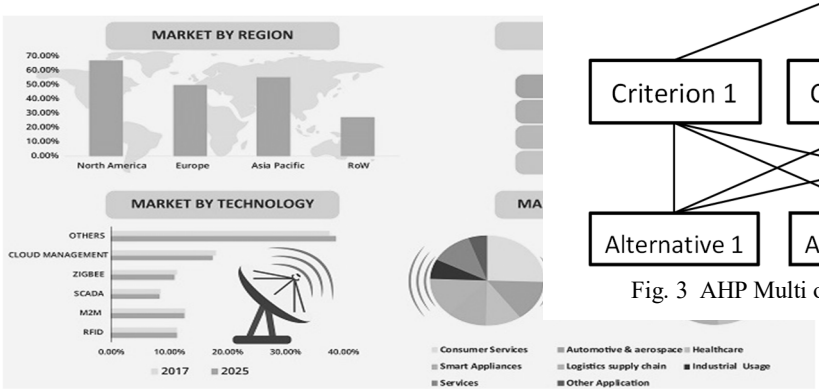


Fig. 1 Global IoT Market Forecast 2017-2025

C. Network

1. Unauthorized access to data
2. Unauthorized access to service
3. Virus or Malware attacks

D. Front End Sensors and Equipment

1) Safety management of code resources

2) Front-end Sensors and Equipment accept 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 applications 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 as unauthorized access to data, threats to the Internet, and denial of service attacks.

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

4) 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 an IoT system can be defined through several terms which include privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality, and availability at any time [3].

E. Literature Review

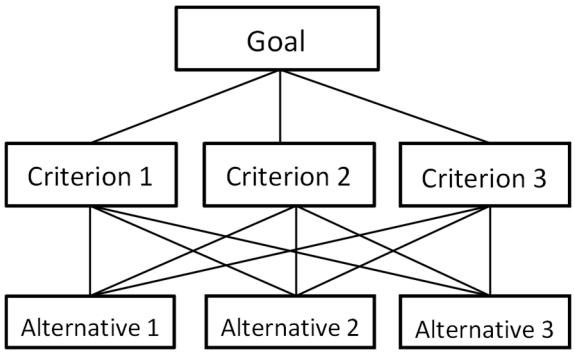


Fig. 3 AHP Multi objective Selection Criteria[16]

Internet of things finds its applications in various domains including environmental, commercial, industrial, smart cities, healthcare, traffic monitoring, urban computing, smart homes, security and emergencies and infrastructure [4]. A number of challenges, like route security and parameter optimization, are being faced while deploying IoT framework to achieve its applicability in the real world. 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 the 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 lifetime can be maximized. GAs can also be used to optimize the minimum cost function and a 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 a lifetime of a node in a wireless network. Analytical hierarchy process can be used to design an energy-aware geographical multipath

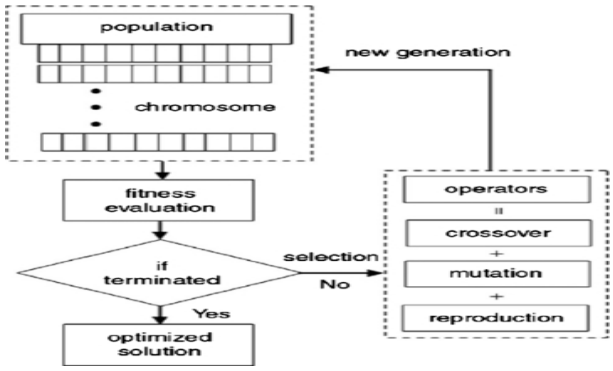


Fig. 2 Genetic Algorithm Flow Chart

routing scheme for WSN which can further reduce the distance to the 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 lifetime are very vital concerns 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 lifetime 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 result in JPAC, MATLAB, and NS are compared with present protocols, and optimization of the network lifetime and energy consumption can be achieved [11]. A new genetic algorithm-based routing technique called MEGA (Maximum Enhanced Genetic Algorithm) which uses the local search mechanism and sleep wake-up mechanism can also optimize the network lifetime and energy consumption constraints in deploying the WSN [12]. In IoT, sensor nodes can be clustered which can perform on the basis of the energy of sensor nodes and genetic algorithms can be used to optimize the 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 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. GAEER improves stability period and network lifetime by 26.6%, 67.7% and 76.8%, 173.6% as compared to GADALEACH, and GAOC, respectively [14].

II. Material and Methods

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 human interventions were possible by WLAN and doing this can cause a breach of security of the IoT system and there are the following major security issues in IoT [2]

A. Problem Formulation

The main objective of this routing model is to select an optimized and secured route among the different zones and each zone has a 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 secured by transposition ciphers with a message divided into various packets (letters) and then the encrypted message will be transmitted through the selected route. On the other side, each letter is decrypted according to the agent code or key and the original message is retrieved. 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 the optimal route i.e. Latency, Power Consumption, and Network Congestion. All these parameters shall be given different priorities according to the AHP scale. The design and development of this routing protocol shall make use of three techniques which are Genetic Algorithms, Analytical Hierarchy Process, and Encryption algorithms.

B. Genetic Algorithm (GA)

The Genetic Algorithm (GA) is a search heuristic that is based on the theory of evolution, stressing the survival of the fittest, inspired by crossover, mutation, recombination and selection operators [15]. Candidate solutions to the problems of optimization play the role of individuals in a population, and the cost function calculates the quality of the solution. Natural selection of the population then takes place after the repetitive application of the GA operators. Genetic algorithms are best suited for approximation solutions 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 the following steps until the new population is complete.

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

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

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

4) [Replace] Use the 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.

C. Analytical Hierarchy Process (AHP)

The Analytical Hierarchy Process (AHP) is a decision-making procedure that 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 the next hop transfer. The following three steps can be utilized to get the solution in this process.

1) Information is gathered and the next-hop routing nodes selection problem is formulated as a decision hierarchy of independent factors.
2) Calculate the relative local weights of decision factors.
3) Processing the values got in the results from the above steps to attain the overall weight of each alternative node and choose the nodes with the largest weight values which will be eligible for the next-hop relay nodes[16]

D. Encryption Algorithm

Following are steps involved in encryption –

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

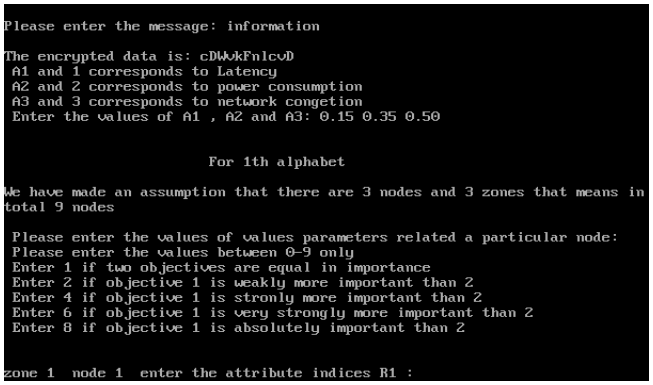


Fig. 4 AHP Multi objective criteria

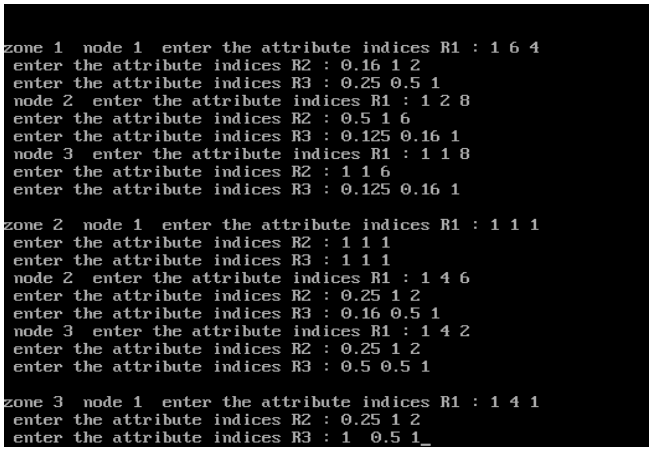


Fig. 5 Input values for zone 1 to formulate comparison matrix

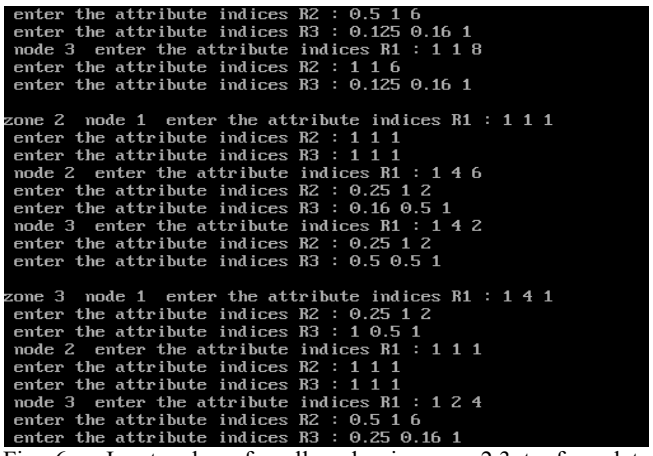


Fig. 6 Input values for all nodes in zone 2,3 to formulate comparison matrix

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

3) When the packet arrives at receiving side it gets decoded and the original message is received.

III. Simulations and Results

Simulation is done for various zones (the user defines the number of zones) and the optimized routing is determined by the value of the cost function. The optimized route is selected with the use of an analytical hierarchy process and genetic

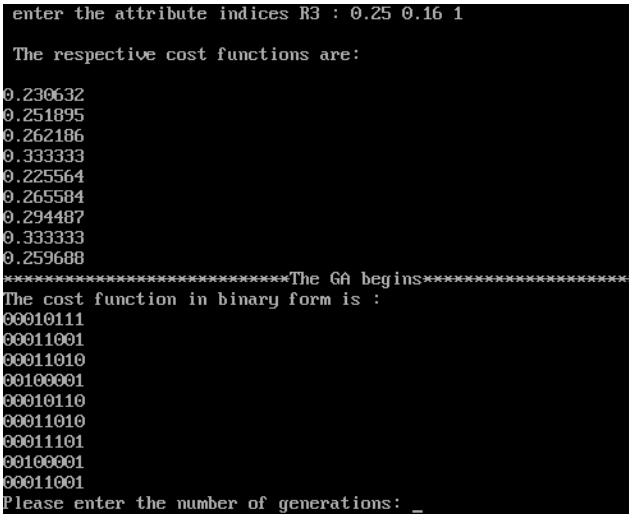


Fig. 7 Cost functions of comparison matrix in binary form

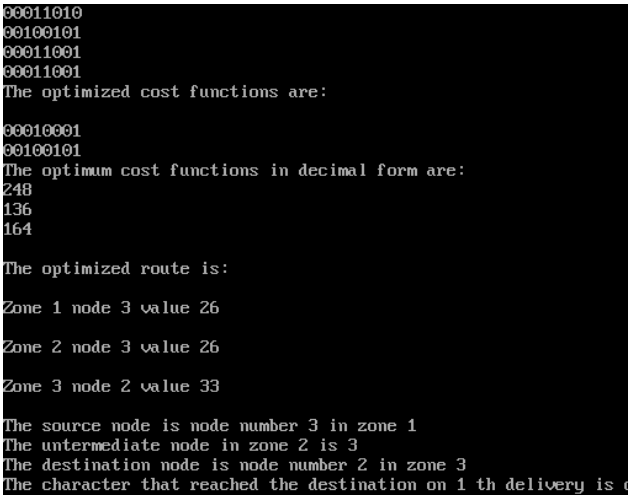


Fig. 8 Delivery of 1st character of encrypted message

algorithm. We took three parameters in our study, namely Latency, Power Consumption and Network congestion. The universal set will include three parameters {L,PC,NC}, Let Q be the input set of parameters and U be the universal set and A1, A2 and A3 are input choices, then below table lists out the dependency of the objective function as per the algorithm chosen to optimize the path.

TABLE I
PARAMETER SELECTION CRITERIA FOR DIFFERENT ALGORITHMS

AODV	AHP	GA
F {Q(i) < U} : L	F {Q(i) < U} : $A_1 * Q(i)$	F {Q(i) ∩ U = 1} : $A_1 * L + A_2 * PC + A_3 * NC$

Once the optimized route is selected, the encryption algorithm is applied to make the routing secure.

Enter the agent code: - r,

Enter the message: - information

Enter the encrypted message: - cDWvkFnlcvD

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

Performance indices for AHP are as follows: -
1 - Equally important
2 - Moderately important
4- Strongly important
6- More strongly important
8- Most strongly important

The following tables will generate the weights associated with each node in the three regions: -

For Zone 1
Node 1:

TABLE II
COMPARISON MATRIX FOR NODE 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 III
COMPARISON MATRIX FOR NODE 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 IV
COMPARISON MATRIX FOR NODE 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 V
COMPARISON MATRIX FOR NODE 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 VI
COMPARISON MATRIX FOR NODE 2 IN ZONE 2

Attributes	Latency	Power Consumption	Network Congestion
Latency	1	4	6
Power Consumption	0.25	1	2
Network Congestion	0.16	0.5	1

Node 3:

TABLE VII
COMPARISON MATRIX FOR NODE 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 VIII
COMPARISON MATRIX FOR NODE 1 IN ZONE 3

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

Node 2:

TABLE IX
COMPARISON MATRIX FOR NODE 2 IN ZONE 3

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

Node 3:

TABLE X
COMPARISON MATRIX FOR NODE 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 for the first alphabet: -
0.230632

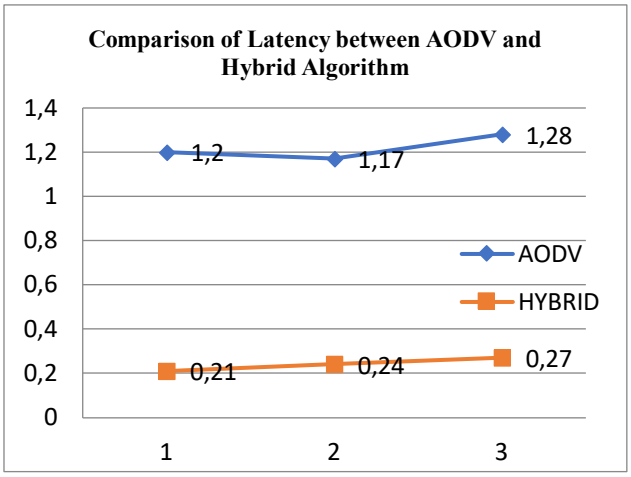


Fig. 9 Comparison of Latencies between AODV and Hybrid Algorithms

0.240936
0.262186
0.333333
0.225564
0.265584
0.294487
0.333333
0.259680
Cost functions in binary form are as follows:
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 are as follows
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 show the result of simulations. Due to space constraints, simulations for the optimal route for only first alphabet are shown here

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 under user priority depending upon 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 the AHP scale. In one case, the user can assign the highest priority to latency and lower to network congestion as well as power consumption whereas in the second case, the highest priority can be assigned to network congestion and lowest to latency and power consumption and similarly, there can be other combinations too. So, the use of the adaptive techniques give an optimized route that is further secured by cryptographic techniques, which can be easily seen in the simulation results. In this proposed model 3 nodes have been considered in each zone and the zones are source zone, intermediate zone, and destination zone. This algorithm calculates the results based on the theoretical backgrounds of EA, AHP, and Encryption techniques used, and code is developed in a 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

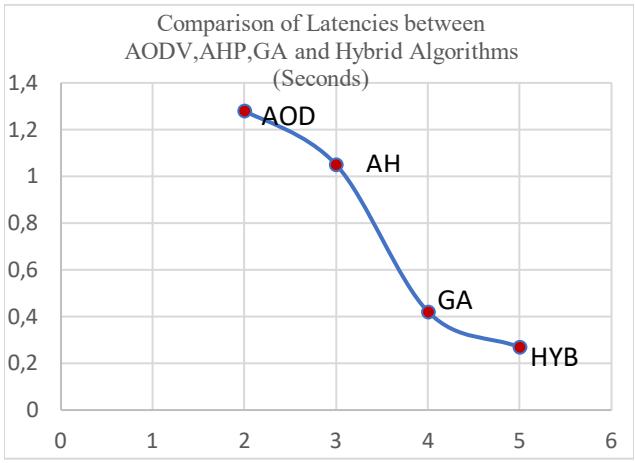


Fig. 10 Comparison of Latencies between AODV, AHP, GA and Hybrid Algorithms

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 the case of a hybrid algorithm as compared to AHP, GA and AODV. Similarly, latency was seen lesser in the case of hybrid algorithms and was more in the case of AODV. The remaining bandwidth was available more in hybrid algorithms as compared to AHP, GA, and AODV. Fig 10 and 11 are representing latencies in seconds along 'x' coordinates. A consolidated comparison of the three algorithms has been given in the Table XI.

TABLE XI
CONSOLIDATED COMPARISON OF ALGORITHMS

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

IV. CONCLUSION

By using genetic algorithms (GA) and the 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 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 a 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 a 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.

REFERENCES

[1] Carsten Mapple, "Security and privacy in the internet of things," Journal of Cyber Policy , vol 2, no. 2,pp. 155-184,August 2017.

[2] Mourvika Shirode,Monika Adaling, JyotiBiradar, Trupti Mate, "IoT Based Water Quality Monitoring System," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3,pp.1423-1428,January-February 2018.

[3] J Sathish Kumar,Dhiren R Patel, "A Survey of Internet of Things: Security and Privacy Issues," International Journal of Computer Applications, vol 90, no.11, pp. 20-26,March 2014.

[4] Rosilah Hassan,Faizan Qamar ,Mohammad Kamrul Hasan ,Azana Hafizah Mohd Aman and Amjed SidAhmed, "Internet of Things and Its applications: A Comprehensive Survey," MPDI Journal Symmetry, vol.12, no.10, pp 1-29,October 2020.

[5] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, R. A. Rashid, "A Self Optimized Multipath Routing Protocol for Wireless Sensor Networks", International Journal of Recent Trends in Engineering, vol.2, pp 93-97,November 2009.

[6] Nesa Sudha,M. L. Valarmathi,,T.Christopahpaul Neyandar. "Optimizing Energy in WSN using Evolutionary Algorithm," IJCA Proceedings on International Conference on VLSI, Communication & Instrumentation, vol 2, pp 26-29,2011.

[7] Xiao ling Wu, Jinsung Cho, Brian J. d'Auriol, and Sungyoung Lee, "Energy-Aware Routing for Wireless Sensor Networks by AHP," IFIP International Federation for Information Processing,LNCS 4761, pp 446– 455,2007.

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

[9] Kratika Varnshney, Sweta Tripathi and Viabhav Purvar, "An Efficient and Reliable Optimized Routing Protocol for IoT Network in Agriculture," Proceeding of IEEE International Conference on Advances in Electrical, Computing Communication and Sustainable Technologies, Bhilai, India, February 2021.

[10] Sang-Hyun Park, Seungryong Cho, and Jung- Ryun Lee, "Energy-Efficient Probabilistic Routing Algorithm for Internet of Things," Journal of Applied Mathematics vol. 2014, pp 1-7,April 2014.

[11] Ali Norouzi and A Halim Zaim, "Genetic Algorithm Application in Optimization of Wireless Sensor Networks," The Scientific World Journal, vol. 2014, pp 1-15, February 2014.

[12] Aishwarya S Hampiholi and B P Vijaya Kumar, "Efficient routing protocol in IoT using modified Genetic Algorithm and its comparison with existing protocols," Proceeding of 3rd International Conference on Circuits, Control, Communication and Computing, Bangalore, 2018.

[13] Amol V Dhumane,Rajesh S Prasad,Jayashree R Prasad, "An optimal routing algorithm for Internet of Things Enabling Technologies," International Journal of Rough Sets and Data Analysis vol.04, issue 3, pp 1-16,July 2017.

[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, vol.9, pp 538-544,June 2020.

[15] Sourabh Katoch, Sumit Singh Chauhan and Vijay Kumar, "A Review on Genetic Algorithm:past present and future" Multimedia tools and Applications, 80, pp:8091–8126,Oct 2021.

[16] Hameed Taherdoost, "Decision Making Using the Analytic Hierarchy Process (AHP); A Step by Step Approach," International Journal of Economics and Management Systems,vol.2,pp 244-246,January 2017