Optimized Routing in Mobile Ad hoc Networks

Rakesh Kumar
IK G, Punjab Technical University Bhikhiwind Campus, Punjab, India

Summary:
A mobile ad hoc network is type of wireless network without any infrastructure and it has a fast changing network topology, as a result of which new mobile nodes frequently gets added and move away from the radio range of network. Due to frequent movement of nodes in the network, this network can have hostile attacks from the external unauthorized nodes which temper the secure communication between the nodes, due to this security becomes a very vital factor which hinders the performance of network. In this paper, first a brief introduction of mobile ad hoc network and its routing protocols is given, and after that implementation results of a secured routing protocol by using intelligent mathematical techniques along cryptographic techniques is presented which can be effectively used in securing the MANETs.

Keywords:
MANET, Routing Protocol, Security and Cryptographic Algorithms.

1. Introduction

Mobile ad hoc network is a collection of mobile nodes forming short lived or temporary networks without the aid of any centralized equipment. Mobile ad hoc network has its roots associated with U.S defence agency DARPA, which is also known as Defence Advanced Research Project Agency, which initiated research on the viability of using packet- switched radio communications to provide reliable computer communications and came up with packet radio network in 1973, also known as DARPA PRNET. The routing protocols used in PRNet were designed to enable reliability, speed and correctness and also included network management facilities. These packet radio networks were known as first generation packet radio networks. After the first generation, second generation survivable adaptive radio networks(SURAN) evolved in around 1980s which provided packet switched networking environment to the mobile battlefield elements in infrastructure- less situations and it was the second generation of MANETs. In 1990 and onwards with the invention of notebook computers and viable communication devices based on radio waves, concept of commercial ad-hoc networks arrived and it was the start of third generation ad hoc networks. .At the same time two new technologies named Bluetooth and Ad hoc sensors were also evolved.[3].Routing in ad hoc networks is a very important issue ,which if not addressed properly may affect severely the throughput of the network. Routing protocols for the MANETs can be classified into three categories which are reactive, proactive and hybrid routing protocols. One other important factor that affects the secure delivery of data to the destination node in the ad hoc network is the Security. It deals with confidentiality, authorization and authentication. The major challenges that are being identified in the MANETs are the insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security. There is limitation of MANETs that protocols used in wired network can't be used for MANETs, as they operate in highly dynamic environment and due to this they are the perfect candidates for numerous provisions.

2. Routing Protocols

For communication within a network, a routing protocol is required to produce reliable and effective routes between a pair of nodes so that data may be transmitted between them efficiently and number of routing protocols have been proposed for these ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols and development of new routing algorithms have been an active area of research for many years. Many protocols have been suggested. Basically, routing protocols can be broadly classified into two types as (a) Table Driven Protocols or Proactive Protocols and (b) On-Demand Protocols or Reactive Protocols. In this paper more stress is given on reactive routing protocols

Proactive (Table Driven) Routing: This approach is similar to the connectionless approach of traditional datagrams networks and nodes based on periodic update process attempt to compute a priori and provide consistent and up to date routing information to every other node in network. The approach is called proactive the nodes calculate all possible paths to all destinations independently of their effective use. Some of the proactive protocols are DSDV,WRP and OLSR

Reactive (on demand) Routing: These protocols evaluate the network on as needed basis and create routes only when there is a need for carrying the traffic. Some of the reactive protocols are AODV, TORA, SSR, DSR,ABR.

Manuscript received December 5, 2016
Manuscript revised December 20, 2016

2.1 Proactive Routing Protocols

2.1.1 Destination-Sequenced Distance-Vector Routing (DSDV)

A table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm .In his protocol every mobile node in network maintains a routing table in which all of the possible destinations within the network and number of hops to each destination are recorded. Each entry is marked with a sequence number generated by destination node. The sequence number enable the mobile nodes to differentiate stale routes with new ones thereby avoiding the formation of new loops. Routing table updates are periodically transmitted throughout the network in order to maintain the table consistency .If a node receives new information, and then it uses latest sequence number. If sequence number is same as one already in table, then the route with better metric will be used. The main source of inefficiency in this is that the DSDV requires regular updates of its routing tables, which uses up battery power and small amount of bandwidth even when the network is idle.

2.1.2 Wireless Routing Protocols

This is again a table driven protocol with goal of maintaining routing information among all the nodes In this protocol ,each node maintains four tables named distance table, routing table ,link cost table and message retransmission list table(MRL).Each entry of MRL table contains the sequence number of update message, a retransmission counter ,an acknowledgement required vector with one entry per neighbour and list of updates sent in update message.MRL is used to store the identification of the nodes that have not acknowledged a route update.MRL records which updates in an update message need to be retransmitted and which neighbours should acknowledge the retransmission. Main drawback of WRP is the requirement for nodes to maintain four routing tables. This can be lead to substantial memory requirements when numbers of nodes in the network are large[1]

2.1.3 Optimized Link State Routing(OLSR)

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad-hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad-hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. The key idea behind OLSR is to reduce the duplicate broadcast packets in the same region and this is achieved by multipoint relay (MPR) nodes and the idea behind the multipoint relay principle is to achieve efficient flooding.

2.2 Ad hoc On Demand Routing Protocols

2.2.1 Ad hoc On-Demand Distance Vector (AODV) Routing

Routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the internet are proactive, meaning they find routing paths independently of the usage of the paths.But AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing. AODV routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed.

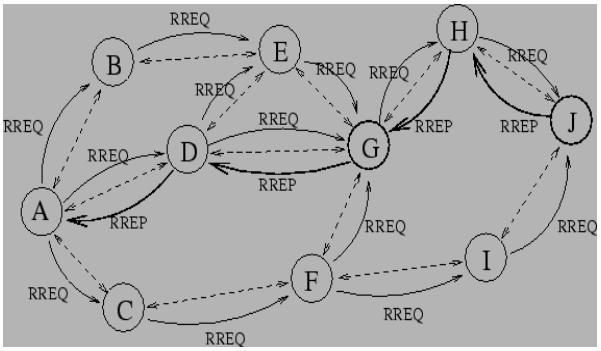

Fig.1 RREQ packet propagation in AODV.

Route Discovery Process

For route discovery, data source node will flood the network with route request (RREQ) packet. If a reply is not received after flooding the whole network with RREQ within some specified time, then source node will rebroadcast RREQ or it may perceive that no route exists between source and that destination from which it has not received any RREP.AODV ensures that all routes are loop free and not stale, so AODV uses destination sequence numbers. Like DSDV, AODV also maintains its sequence number for a node and a broadcast ID. Whenever a node receives a RREQ message then it will check whether it has

seen the RREQ message before by noting the source address and broadcast ID pair. It will discard the request, if so. Otherwise it sets up reply path pointing toward the data source. In AODV, intermediate nodes can also reply to RREQ only if there exists a route to destination. Fig 1 shows an example of route discovery in AODV.A node updates its path information only if the Destination Sequence number of the current packet received is greater or equal than the last Destination sequence number stored at the node with smaller hop count.

2.2.2 Dynamic Source Routing

It is similar to ad hoc on demand vector driven routing protocol and is based on the concept of source routing .In source routing each packet carries in its header, the complete ordered list of nodes the packet should pass through the network.

Route discovery and route selection

Route discovery and route election process in DSR is based on flooding the network with route request(RREQ) packet. An RREQ message includes sender address, target address, a unique number to identify the request and route record, listing the addresses of each intermediate node through which RREQ is forwarded. On receiving RREQ control packet, an intermediate node can do the following

i) Reply to query source node with route reply ,if valid path to destination is stored in its cache
ii) Discard the packet, if same RREQ is already received and to limit number of route request, node only forward route request if same request has not been forwarded again.
iii) Append its own ID into route record and relay packet to its neighbours.

DSR uses key advantage of source routing to learn routes by scanning the routing information in the header of received packet. This form of active learning can be very efficient and reduce the network overhead .This is so because intermediate nodes do not need to maintain up to date routing information to route packets as packets themselves already contain all routing information.DSR allows nodes to keep multiple route to destination in their cache. Hence when a link on route is broken, the source node can check its cache for another route .If such a route is found in cache, route reconstruction does not need to be reinvoked, thereby saving network bandwidth as well as reducing route acquisition latency. One of the main benefit of DSR protocol is that there is no need to keep routing table so as to route a given data packet as the entire route is contained in the packet header. The limitations of DSR protocol is that this is not scalable to large networks and even requires significantly more processing resources than most other protocols[1]

2.2.3 Signal Stability Routing (SSR)

This protocol performs the on demand route discovery by selecting a long lived routes based on signal strength and location stability. Signal strength criteria allows the protocols to differentiate between strong and weak channels. Each channel is characterized as strong or weak by the average signal strength at which packets are exchanged between the hosts at the either end of the channel.

Route discovery and route selection process

In this node starts route discovery by broadcasting a route request packet (RREQ) throughout the network. A node that receives an RREQ to relay, forwards RREQ only if it is received over a strong channel, otherwise RREQ is dropped. If the route discovery initiator receives no route reply within some time out, it starts a new route discovery process. When a failed link is detected, the intermediate nodes send a route error message back to source indicating the link in error.The source then initiates a new route discovery process to find a new path to destination.

2.2.4 Associativity Based Routing(ABR)

In this routes are chosen based on their longevity and this is the fundamental objective of ABR to derive longer lived routes and this metric is known as degree of association stability. The brief functioning of the technique is as follows: node periodically broadcasts a HELLO message to signify its existence. Nodes counts these HELLO messages received from neighbours to update their associativity ticks. For each beacon received, the associativity tick of the current node w.r.t. beaconing node is incremented. Associativity ticks are reset if beacon signal is not received for certain period of time.

Route discovery and route selection process

A data source node acquires a new route by broadcasting a route request control packet and as the packet is propagated, intermediate nodes append their own ID. The destination node waits for a suitable period of time so as to receive other request packets forwarded along other paths .The destination is then able to select the best route by examining the associativity ticks along each of the paths .Once a route is selected ,the destination sends a route reply control packet through the selected route .As the route reply is propagated backwards to data source, intermediate nodes involved in its retransmission are able to set up a route entry for the destination and activating a forward path to the destination in a hop by hop fashion. Major advantage of the ABR relies on the longevity concept of routes .Stable routes with a long life result in fewer route reconstructions.

3. Problem Formulation

From all the protocols described above it can be concluded that no routing protocol offers security and privacy to the data being transmitted in the MANETs and in addition to this route is not optimized to provide the maximum throughput. To overcome this, intelligent mathematical techniques like evolutionary techniques and analytical hierarchical process are used in conjunction with cryptographic techniques and substitution ciphers are used to encrypt the optimized route. In the next section all these techniques will be discussed one by one and after that implementation results are presented.

3.1 Genetic Algorithms in MANETs

The wireless sensor network technology has been gaining tremendous importance in recent years. Network lifetime is one of the important parameters to optimize as energy resources in a WSN are limited due to battery operated nodes. Replacing or recharging of battery in the network may be infeasible. Though the overall function of the network may not be hampered due to failure of one or few nodes of the network as neighboring nodes may take over, but for optimum performance the network density must be high enough. Network connectivity which depends upon the communication protocol is another WSN design issue.
The mentioned issues call for simultaneous optimization of more than one nonlinear design criteria, and the underlying challenge is to find as many near-optimal and non-dominant solutions as possible in unimpeachable computational constraints. Several interesting approaches like Neural Networks, Artificial Intelligence, Swarm Optimization, and Ant Colony Optimization have been implemented to tackle such problems.The genetic algorithm (GA) is a search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problems. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. The GA repeatedly modifies a population of individual solutions. At each step, the genetic algorithm selects individuals at random from the current population to be parents and uses them to produce the children for the next generation. Over successive generations, the population "evolves" towards an optimal solution. GAs can be applied to solve a variety of optimization problems that are not well suited for standard optimization algorithms, including problems in which the objective function is discontinuous, non-differentiable, stochastic, or highly nonlinear.

3.2 Analytical Hierarchical Process (AHP)

The Analytical Hierarchy Process (AHP) is a multiple criteria decision-making method which decomposes a complex problem into a hierarchy of simple sub problems, synthesizes their importance to the problem, and finds the best solution. AHP is used to determine the nodes which are eligible to be selected as next hop relay. It is carried out in three steps like Information is collected and the next hop routing nodes selection problem is formulated as a decision hierarchy of independent factors. Secondly calculate the relative local weights of decision factors or alternatives of each level and thirdly, synthesize the above results to achieve the overall weight of each alternative node and choose the nodes with largest weight as the eligible next hop relay nodes.

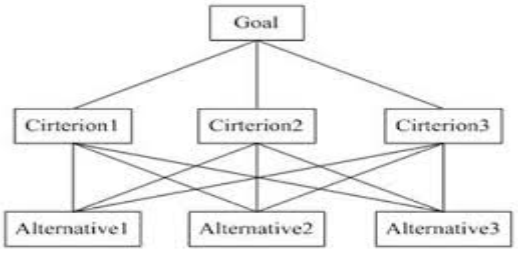

Fig. 2 Analytical Hierarchical Process Selection Criteria

3.3 Evolutionary Algorithms

EA as the name suggests takes the evolution of the species into picture and applies the similar concepts on the problems related to optimization. The main concept of this algorithm revolves around selecting the best next alternative taking into account the fitness function. However, evolutionary algorithm involves altogether different concept than AHP. Here the nodes in zone 1 are considered to be the parents who will be evolving into the children. Now as the species evolve and the feature of the children is determined by the genes of the parents, similar concept follows here known as crossover.
The various steps involved in evolutionary algorithm are as follows –
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 chance to be selected
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 the parents.

c. [Mutation] with a mutation probability 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 step2.

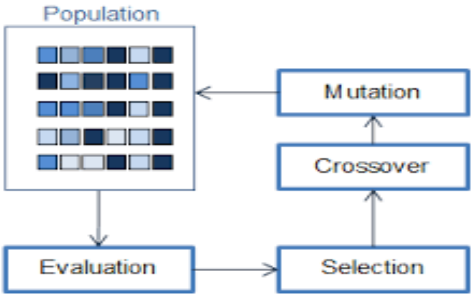

Fig 3.Evolutionary Algorithm

3.4 Encryption Algorithm

Cryptographic algorithms plays a very important part by securing the routes for the transmitting the data in wired/wireless communication. In this paper, message to be send is encrypted before sending through the communication nodes and also the optimized intermediate node which forms the optimized route determined by intelligent mathematical techniques is encrypted
a. Enter the agent key which will decide the encryption 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 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. Once each of the packet reaches to the receiving side it gets decrypted and the original message is received.

4. Simulation and Discussions

The simulation is done in C++ language for various 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 and the Ceaser cipher encryption algorithm is applied to make the routing secure. The source node is considered in the first zone whereas destination is considered to be present in the third zone. Evolutionary algorithm takes all three parameters into consideration when it comes to optimize the path from source to destination. We took three parameters in our study, namely Energy, Latency and Bandwidth and the different priorities for these parameters are a, b and c, which are assigned by the user and similarly assigned values of Energy, Latency and Bandwidth to the different nodes in the zone 1 are E,L and B

Cost Function= a*E +b*L +c*B

In AHP, objective function is dependent on any one among the energy, latency and bandwidth of the nodes at one time, and in EA, objective function is dependent upon all the parameters which are energy, latency and bandwidth .The main assumption while doing crossover which has been taken is that if one node takes the three-fourth (75%) of the feature then the other nodes takes remaining one-fourth (25%). For instance, if node number 1and 2 of zone 2 has evolved from the zone 1as parents (namely node 1 and node 2), then if three-fourth of the energy level from node 1 in first zone is transferred to node 1 in the second zone then second children in zone 2 will get remaining one-fourth energy and if node 1 and node 3 has been selected as parents in zone 1 ,then node 2 in zone 2 will be child after crossover and it will utilize 50% energy of node 1 in zone 1 and 50% energy of node 3 in zone 1.In this work there are three zones and each zone is having three nodes.
The technique developed here is a hybrid which is a combination of analytical hierarchy process (AHP), evolutionary algorithms (EA) and an encryption algorithm. If routing algorithm is implemented using only AHP then we have to assign different priorities to parameters that are energy, latency and bandwidth as per the need of importance and also we have to fix the source and destination node in zone 1 and zone 3 respectively and this algorithm will determine best node in zone 2. If routing algorithm is implemented using only EA then we have to assign equal priority to all the parameters that are energy, latency and bandwidth and here we have to fix only destination node in zone 3 and this algorithm will determine best node in zone 2 with use of EA parameters. If hybrid algorithm incorporating the AHP, EA and encryption algorithm is implemented then the best nodes in zone 1 will be determined by the use of AHP and source node too and the nodes in the zone 2 will be determined by the use of EA with the effective use of its parameters and the optimized route will be secured with the use of encryption algorithm. The simulation results of the hybrid algorithm using high level language C++ are presented here.

4.1 Simulation Results

Case 1: When destination is node 1 in zone 3

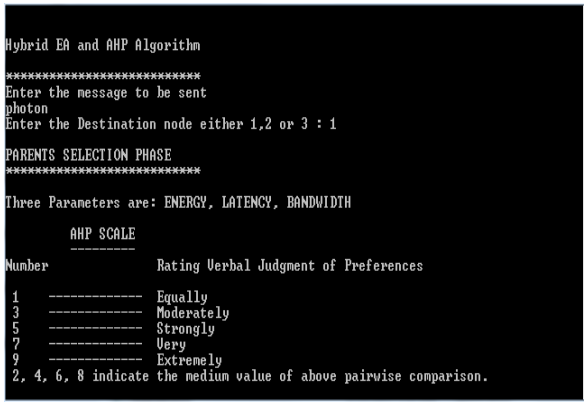

Fig.4Simulation results for Hybrid Algorithm with destination 1

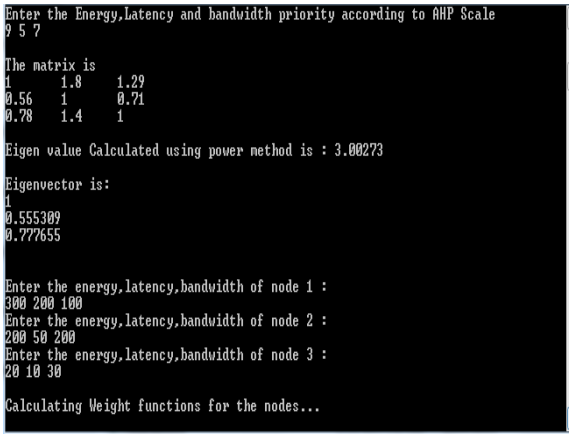

Fig.5 Design of comparison matrix using AHP and assigning different weights to nodes

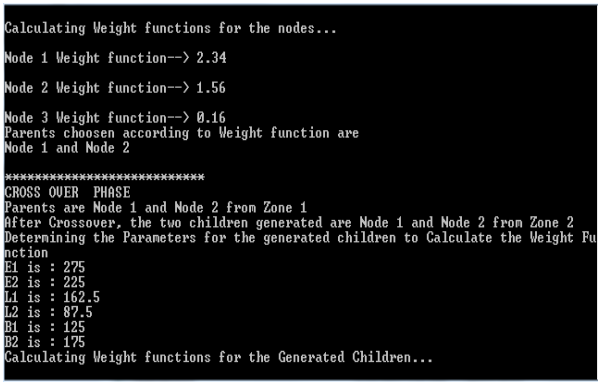

Fig. 6 Crossover phase using EA

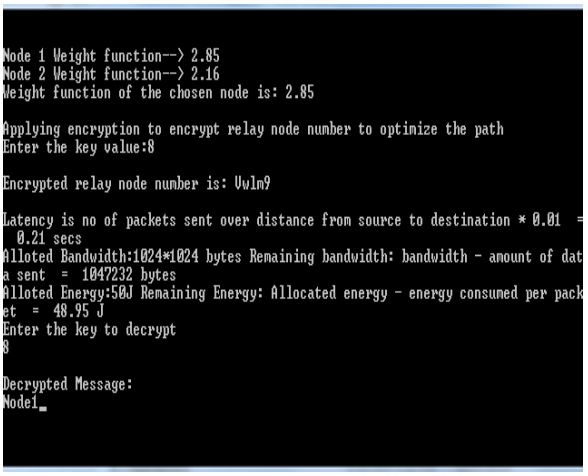

Fig.7 Final calculated values of Energy, Latency and Bandwidth and decrypted message

In the first case of the hybrid algorithm, we fix the Node 1 in Zone 3 as the destination node and AHP priority is assigned as 9 5 7 to Energy, Latency and Bandwidth with the initial values of nodes same as assumed in the earlier cases. It was observed that the weight function of the nodes were calculated as 2.34, 1.56 and 0.16.As the weight functions of the nodes 1 and 2 are higher than that of 3rd ,so nodes 1 and 2 will be selected as parents in zone 1.Now after the crossover the parameters of the generated children were calculated as under.

[275 162.5 125] & [225 187.5 175].

The weight function of the generated children were calculated as under 2.85 and 2.16.Now it is evident from the calculations that node 2 is higher weight function and hence will get selected as best child in the zone 2 and hence the best node for optimized routing as this node assumed the features of EA and AHP. In a similar way results of the second case where destination is taken as node 3 in zone 3 can also be explained whose simulation results are given below.

Case 2: When destination node is node 3 in zone 3

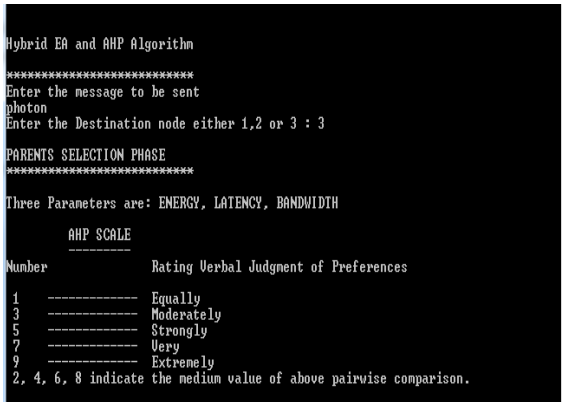

Fig 8 Simulation results for Hybrid Algorithm with destination 3

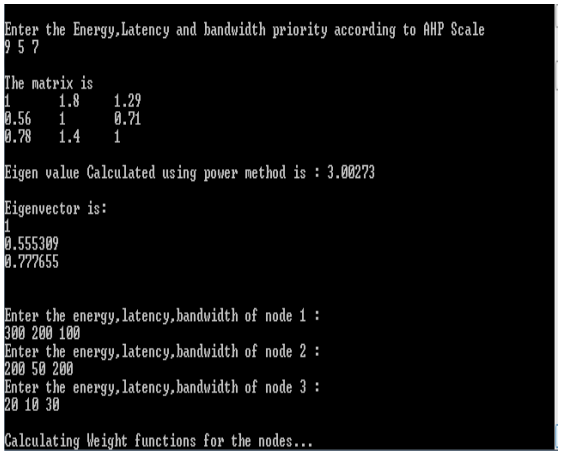

Fig.9 Design of comparison matrix using AHP and assigning different weights to nodes

Fig. 10 Crossover phase using EA

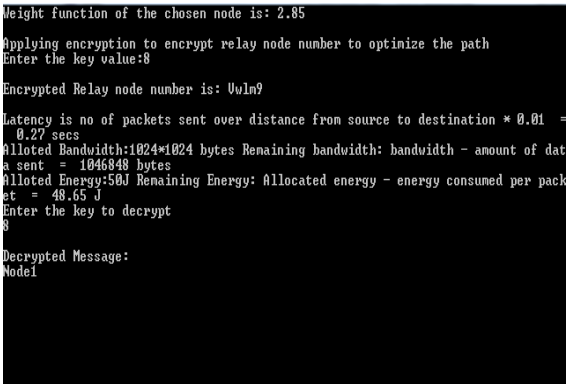

Fig.11 Final calculated values of Energy, Latency and Bandwidth and decrypted message

5. Conclusion

From the simulations and discussions presented in this paper it can be concluded that hybrid algorithm which is a combination of analytical hierarchy process and evolutionary algorithms performs better for routing in mobile ad hoc networks in terms energy, latency and bandwidth of nodes in comparison to classical routing protocols used in MANETS. After the application of hybrid algorithm to MANET, all the parameters of the network are having the optimized and secured values which are the major requirements of any network for their better performance. At the same time if we talk about networking simulator tool NS-2 which is used to simulate the mobile ad hoc networks and to carry about various studies of networking parameters, then it has been observed that delay and energy consumed in network is calculated to be 0.024 seconds and 0.88joules and value got of latency in our case is 0.24 sec and we can say that the values got from hybrid algorithms and NS-2 tool are comparable with each other.

References

[1] Rakesh Kumar, Dr Push Verma, Dr Yaduvir Singh "A Review And Comparison Of MANET Protocols With Secure Routing Scheme Developed Using Evolutionary Algorithms" International journal of computer Engg and technology, Volume 3, Issue 2, July- September (2012), pp. 167-180

[2] Rakesh Kumar, Dr Push Verma, Dr Yaduvir Singh, "An Efficient Routing Scheme for MANETs" IEEE International Conference on Computational Intelligence and Computing Research 2014, 978-1-4799-3972-5/14, pp 36-42.

[3] Humayun Bakht "History of mobile ad hoc networks" ppt availableon internet, pp1-16.

[4] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-HocNETworks (MANET)" International Journal of Information and Education Technology, Vol. 3,No.1,February2013,DOI: 0.7763/IJIET.2013.V3.223, pp 1-5

[5] Abolhasan, M., Wysocki, T. & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2,(1), 2004,pp1-22.

[6] Z. J Haas and M. R. Perlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," IETF Internet draft, draft-ietf-manet-zone-zrp-01.txt, Feb, 1999.

[7] Elizabeth M Royer,Chai Keong Toe, "A review of current routing protocols for ad hoc mobile wireless networks,IEEE Personal Communications,1999,pp46-55.