Agents-Secured Rural Communication Development Using Mobile Ad-Hoc Network

Jasleen Kaur[1] Dr. Rajesh Gargi[2]
[1]M.tech Student [2]Professor
[1,2]Geeta Engineering College

Abstract— Rural areas where resource of communication lacks and the area like earthquake zone require a strong communication channel. India is one of the fastest growing countries in the world but fact is there are more than 600 villages still lack the proper communications. Mobile ad-hoc network is one of the networks which often requires seamless ubiquitous network, which can be utilized to structure the wireless mode of communication, for the transmission of strategic information among mobile agents in areas where no rigid infrastructure can be set up for a network. Mobile ad-hoc network is best suited for this kind of situation because of the flexibility and scalability it offers. No central administration is required for such network, as it works on temporary connection links, making the network ubiquitous. The prime challenge in implementing such network with multi-agent communication is the need of an efficient routing protocol for multi-hop connectivity, frequently changing topology and dynamic routes. This paper proposes a new multi-agent based routing algorithm to facilitate the reliable communication in rural areas network. The proposed algorithm is named as Ant Algorithm for Mobile Ad-hoc Network. The proposed algorithm is inspired from the ant colony optimization metaheuristic and is based on swarm intelligence, uses simple node-level management with probabilistic multi-path routing which highly resembles to the behavior of real world harvester ants to find the shortest path between their nest and the food source. This paper will discuss about the security ethics of the Adhoc network. Techniques that will make MANET more secure and Algorithms for security in MANET.

***Keywords**:* Mobile Ad-hoc network, Rural Communication Issue, Ant Colony Optimization, Multi-agent network, multi-path routing, Security Ethics

I. Introduction

Wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet),which evolved into the survivable adaptive radio networks. (J.A. Freebseryser, 2001). Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge.

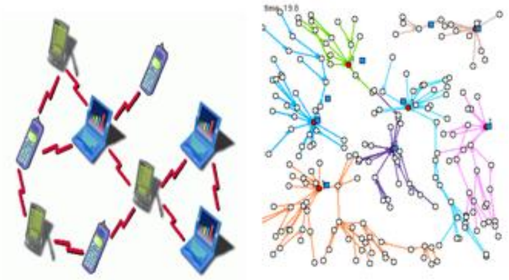


Fig. 1.1**:** Mobile Ad-Hoc Network Structure (Q.Fang)

II. Mobile Ad-Hoc Network Structure

In MOBILE AD-HOC NETWORK, nodes within each other's wireless transmission ranges can communicate directly.

In recent years, Mobile Adhoc Network (MOBILE AD-HOC NETWORK) has received marvelous attentions due to self-design, self-maintenance, and cooperative environments. (Bing Wu, 2006)In MOBILE AD-HOC NETWORK, all the nodes are mobile nodes and the topology will be hanged rapidly. The structure of the MOBILE AD-HOC NETWORK is shown in Figure1.1.

III. Basics And Background

A. *Ant algorithm Basics*

The idea of the ant algorithm is inspired from real world ants observing the ways ants work in their colonies to search for food. Ants searching for food travel towards food and when they reach an intersection, they have to decide a branch or route to travel forward. This decision is based on the concentration of pheromone trail left by ants while traveling. Pheromone is a volatile substance left behind by ants while traveling on a path. Ants are biologically blind in nature. Therefore, they leave behind the pheromone trail to mark the path they travel and create the routes which they are able to smell. Concentration of pheromone on a path depicts the frequency of usage of the path. Paths with higher pheromone concentration are more likely to be chosen by an ant. Since, the pheromone is a volatile substance, the intensity of pheromone decreases with time due to diffusion. Diffusion of pheromone adds dynamics to the route searching and decision making process.

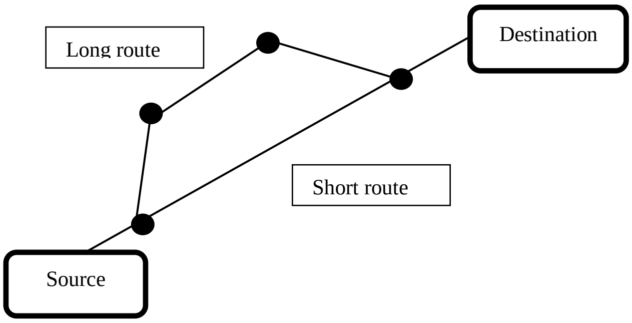


Fig. 3.1: Longer And Shorter Path From Source To Destination.

In figure 3.1, assume that there are two paths from source (nest) to destination (food). Say, a group of n ants, travelling from source to destination, reach the first intersection. Let's assume that (n/2) number of ants chose the longer path and the other (n/2) number of ants chose the shorter path. While returning back, ants again have to make the decision to choose the route back home. Since, the path chosen by the ants is shorter, ants traveling from shorter path will deposit pheromone on the shorter path more rapidly while traveling back and forth, compared to the ants choosing the longer route. Whereas, the pheromone trail of longer path diffuses away with time, decreasing its chances to be chosen by new ants.Eventually, the pheromone intensity on shorter path will be higher than that of alternative longer path and all the ants will chose the shorter path. (Dorigo, Maniezzo, & Colorni, 1996)

This approach used by ants can be used to design an algorithm with probabilistic multi-path routing which can fit best in situations where the existence of links are not assured and link changes are frequent. Example: MOBILE AD-HOC NETWORK.

B. Ant Colony Optimization metaheuristic algorithm

Assume a graph G = (M, N), where M = number of nodes and N = Number of edges, be the connected graph with *n* number of nodes where *n* = | M |. $v_s$be the source node and $v_d$be the destination node on the graph G. Path length be the total number of nodes on the path between v_s and v_d.

Each path*e* (*i*, *j*) ϵ Nof graph G connecting the nodes v_i and v_j has an artificial pheromone concentration value; say,$P_{i,j}$. The value is modified each time the ants travel that path. Value $P_{i,j}$ reflects the frequency of usage of the path in the graph .If S_i is the set of one-step neighboring nodes of $v_i$and v_j is one of the neighbor of v_i (i.e. v_j ϵ S_i), then the ant located at node v_i uses the pheromone concentration value of the path *e*(*i,j*) (i.e. $P_{i,j}$)to determine the probability of visiting the node v_j as next node (Jawahar, 2005). If $\boldsymbol{Prob.}\mathbf{v_j}$ be the probability of visiting the node $\mathbf{v_j}$ then, the equation can be represented as:

$$\textbf{Probability of visiting node } \mathbf{v_j}\ (\boldsymbol{Prob.}\mathbf{v_j}) = \frac{\boldsymbol{P_{i,j}}}{\sum_{j\in S_i}\boldsymbol{P_{i,j}}}$$

Whereas, if node $v_j$is not the one-step neighbor of node $v_i$then, the probability of visiting v_j becomes 0. This means that the ants can only travel to their one-step neighboring nodes.

If$\boldsymbol{j} \notin \boldsymbol{S_i}$ then, $\boldsymbol{Prob.}\mathbf{v_j}$ = 0

The probabilities choosing the next hope must satisfy the constraint:

$\sum_{j\in S_i}\boldsymbol{Prob.}\mathbf{v_j}$ = 1, provided that $\boldsymbol{i} \in |\mathbf{1}, \boldsymbol{S}|$

An ant deposits a constant amount of pheromone (say, $\Delta\boldsymbol{P}$) each time it travels via edge. So, while transiting from node $\mathbf{v_i}$ to $\mathbf{v_j}$, the pheromone concentration on the edge *e*(*i, j*) changes as follows:

$\boldsymbol{P_{i,j}} \coloneqq \boldsymbol{P_{i,j}} + \Delta\boldsymbol{P}$ …………………. Equation (i)

In a simple ant colony metaheuristic, the pheromone trail diffuses away with time. If we consider ants living in environment where time is discrete, then the diffusion of the pheromone takes place exponentially. The equation can be represented as:

$\boldsymbol{P_{i,j}} \coloneqq \boldsymbol{P_{i,j}}\,.(\mathbf{1} - \boldsymbol{C})$, where$\boldsymbol{C} \in (\mathbf{0}, \mathbf{1})$ …. Equation (ii)

(Gunes & Udo Sorges, 2002)

IV. PROPOSED ROUTING ALGORITHM

The proposed routing algorithm, Ant Algorithm for Rural Communication MOBILE AD-HOC NETWORK (AAMM), consists of 3 major phases. Following section describes the AAMM and adaptations from ant colony optimization metaheuristics.

A. Route Discovery

In this phase, new routes are created using the control packets before the transmission of data packets. Forward ant (FANT) and backward ant (BANT) are used for this purpose. FANT is an agent which helps in tracking the source node whereas; BANT helps in tracking the destination node. FANT is a small packet which stores a unique sequence number, used along with the source address, by the nodes to identify the duplicate. Duplicate packets are destroyed by the nodes.

FANT is first broadcasted to all the one-hop neighbors and if the destination is not found the neighbors forward the FANT to their neighbors and so on. The whole process goes on until the destination is found. Each node also stores the recently forwarded packet details in its buffer to prevent the loops. A node which receives the FANT for the very first time, adds a record in the routing table. The record consists of 3 attributes viz. destination address, next hop and pheromone value. Source address of FANT is interpreted as the destination address, the previous node is interpreted as next node and the pheromone value is calculated using the number of nodes the FANT travelled to reach that particular node.

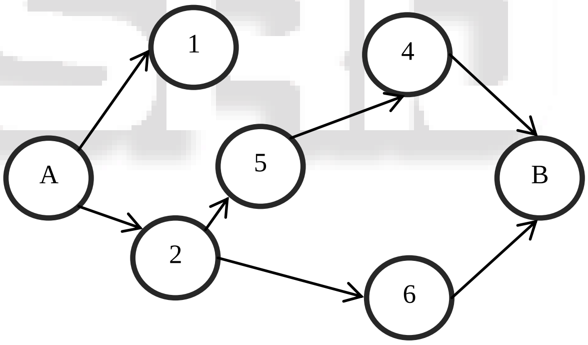


Fig. 4.1(A):Transmission Of Fant From Source Node A To Destination Node B

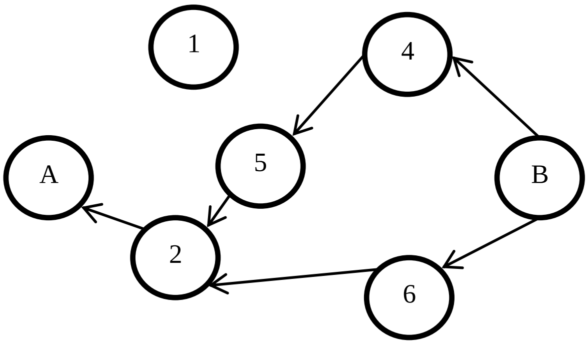


Fig. 4.1 (B) .Transmission Of Bant From Destination Node B To Source Node A

After the FANT reaches the destination, the information is extracted and the FANT is destroyed. The destination node creates a BANT and sends it back to the source node. BANT travels in network similar to FANT, creating routes from destination to source. After, the sender receives the BANT from the destination nodes, the route is formed and transmission of data packets is possible. (Subha & Anitha, 2009)

Figure4.1(a), shows the process of route discovery where each nodes broadcast FANT to one-hop neighboring nodes until it reaches destination. In Figure 4.1 (b), BANT is transmitted back to source node creating multiple routes for data transmission which shows that AAMM supports the multi-path routing.

B. *Route Maintenance*

Once the routes are formed between source and destination using FANT and BANT agents, the second phase of algorithm will be to improve the routes during the transmission of packets. AAMM algorithm does not need to transmit special packets to maintain the network traffic. The data packets transmitted by end-users are enough to perform the route maintenance. The pheromone values for the path keeps on changing as the data packets travel via the path updating the artificial pheromone concentration based on equation (i). Similarly, the pheromone concentration for a route also decreases with time using equation (ii). This way, the data packets behave like natural agents (ants) and keep optimizing the routes as they travel in network and the most optimal path is opted by data packets with the time.

To prevent the disappearance of the alternative routes, which may lead to saturation mode of network, AAMM uses an agent called update ants (UANT) to update the network in timely manner. This keeps the network from getting saturated and updates the pheromone values for all the alternative routes as multiple routes are very crucial for dynamic network like MOBILE AD-HOC NETWORK. Alternative routes can come handy during the breakdown of the route as it saves from the overhead of initiating the route discovery phase. (Sethi & Udgata, 2010)

C. *Link Failure Handling*

Due to the mobile nature of nodes in MOBILE AD-HOC NETWORK, sometimes the routes may be interrupted or the position of nodes may change. AARM can identify the failure in root when it receives the error message for a certain link while broadcasting the data packets. This kind of link failure is handled by deactivating the link, ceasing its pheromone value to NULL which means no further transmission takes place via that node.

Alternative link is searched using the routing table, and upon the discovery of alternative link the data packets are forwarded via alternative path. Else, neighboring hops are informed for local transmission. Using neighboring hops ensures that unsuccessful data packets are re-routed using neighboring nodes instead of original sending nodes reducing the delay in process. In case both the alternatives do not work, and the transmitting node receives the negative acknowledgement (NACK), the new route discovery phase is initiated.This approach of local transmission saves end-to-end delivery time.

V. Comparison with Similar Existing Algorithms

	AAMM	**ARA**	**AODV**
Local Transmission	Yes	No	No
Pheromone update mechanism	Yes	Yes	No
Multipath transmission	Yes	Yes	No
Automatic New route discovery	Yes	No	No

Table 5.1: Comparison Of Aamm With Ara And Aodv (Sethi & Udgata, 2010)

Table5.1 shows the comparison of AAMM with similar nature of algorithms namely Ad-hoc On-Demand Distance Vector Routing (AODVC) and Ant colony based Routing Algorithm (ARA).AAMM provides the local transmission facility which saves the end-to-end delivery time in network. In a dynamic nature of network such as MOBILE AD-HOC NETWORK with high node mobility, the frequency of failure of links is high. Thus, with the local transmission mechanism AAMM proves to be better in cutting down the network overhead compared to other two algorithms. AAMM also has an upper hand on automatic route discovery as it uses the new kind of ants namely Update Ants (UANT) for preventing the network from being saturated. The pheromone update mechanism and multi path transmission are present in dynamic algorithms like AAMM and ARA but not in traditional algorithms like AODV. (Sethi & Udgata, 2010)Presence of all these features makes AAMM an appropriate routing algorithm for MOBILE AD-HOC NETWORK with reduced overhead and high reliability.

VI. Security And Ethics

Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes.

A. *Criteria For Protecting Ad Hoc Networks*

1) *Physical security*

In ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the adhoc networking approach and the environment in which the nodes operate

2) *Security of Network Operations*

The security of ad hoc networks can be based on protection in the link or network layer.In some ad-hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers. Most MANET routing protocols seem to handle the rapid changes to the networking environment rather well, as stated in [15]. As the routing protocol is responsible for specifying and maintaining the necessary routing fabric for the nodes, the protocol must be protected from any attack against confidentiality, authenticity, integrity, non-repudiation and availability.

3) *Security of Key Management*

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As ad hoc networks significantly vary from each other in many respects, an environment-specific and efficient key management system is needed.

To be able to protect nodes e.g. against eavesdropping by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumptions about a priori negotiated secrets

VII. Security in Ad Hoc Networking Proposals

A. DDM

Dynamic Destination Multicast protocol (DDM) is a multicast protocol that is relatively different from many other multicast-based ad hoc protocols. In DDM the group membership is not restricted in a distributed manner, as only the sender of the data is given the authority to control to which the information is really delivered. In this way the DDM nodes are aware of the membership of groups of nodes by inspecting the protocol headers.

The DDM approach also prevents outsider nodes from joining the groups arbitrarily. This is not supported in many other protocols directly; if the group membership and the distribution of source data have to be restricted, external means such as the distribution of keys have to be applied.

B. OLSR

Optimized Link State Routing protocol (OLSR), as defined in [13], is a proactive and table driven protocol that applies a multi-tiered approach with multi-point relays (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes. Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kinds of environments. The MPRs are chosen so that only nodes with one-hop symmetric

C. AODV and MAODV

Ad Hoc On-Demand Distance-Vector routing protocol (AODV), defined in [11], is an unicast-based reactive routing protocol for mobile nodes in ad hoc networks. It enables multi-hop routing and the nodes in the network maintain the topology dynamically only when there is traffic. Currently AODV does not define any security mechanisms whatsoever.

D. Encryption Algorithm

RSA is perfectly suitable and effective for Military Mobile Ad-hoc network. RSA algorithm is an asymmetric key cipher; most widely used public cryptography algorithm .Public key encryption has rapidly grown in popularity and controversy because it offers a very secure encryption method that addresses the privacy concerns. RSA keep the data 1,024 to 4,096 bit typical the largest encrypted data in comparison any algorithm and hard to break.

1) Encryption

Calculate the cipher text CT from the plain text PT as follows: CT = PTE mod N

Then send CT as the cipher text to the receiver.

2) Decryption

For decryption, calculate the plain text PT from the cipher text CT as follows: PT = CTD mod N

VIII. Literature Review

Title	Author	Year	conclusion
Wireless Ad-hoc Networks	Lu Han	October 8, 2004	explains what is Mobile Ad-hoc networks and it's character
The Ant System: Optimization by a colony of cooperating agents	Marco Dorigo	1996	The research paper explains the way ant colonies function.
Mobile Ad hoc Networks: Challenges and Future	Kavita Taneja R. B. Patel	2007	demonstrate the challenges and Future of the system
Swarm intelligence for routing in mobile ad hoc networks	Gianni Di Caro	2005	The Paper explains the routing algorithm for the system.

Table 8.1: List Of The Research Paper Used ((J.A. Freebseryser, 2001)

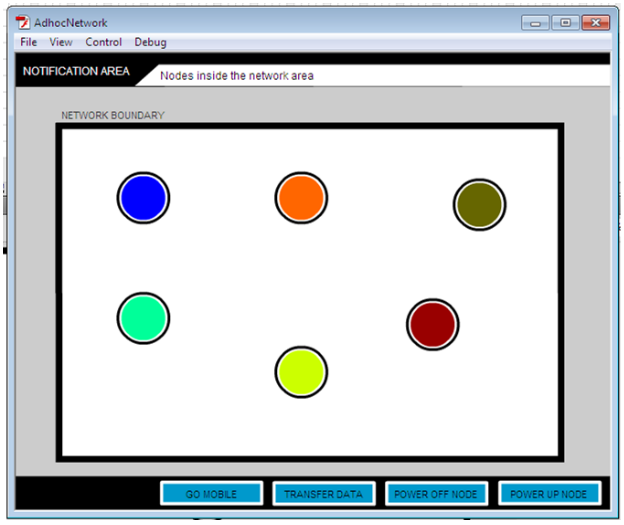
IX. Simulation Output

To perform simulation we have assume some facts. The assumptions are as follows:

(1) Node 1 has been taken as the user node.
(2) The network boundary has been pre defined.
(3) When automatic route detection and management will be done then no nodes will be mobile

A. Automatic Distance Calculation

Every node in the first scenario is mobile it can move from one place to another, means it can change its location. In this we can calculate distance from our user node to another node.

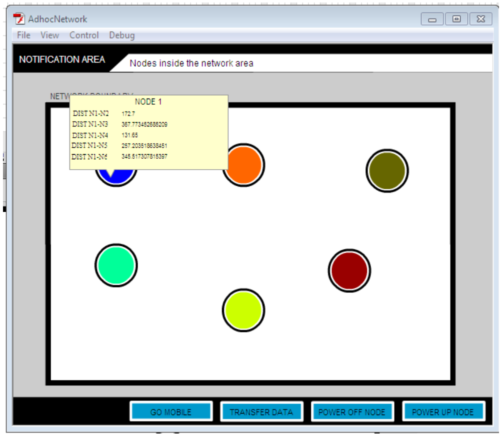


Nodes inside the network area

Fig. 9.1: Assumed Scenario

(1) During movement the distance is calculated dynamically and displayed as the tooltip of that node. As the node moves from one place to another the distance between the User node and other nodes are calculated and displayed.

(2) In our simulation we have used formula for calculating the distance between the User node and the other nodes. The formula is taken as follow:



NODE 1

DIST N1-N2	172.7
DIST N1-N3	367.77345268209
DIST N1-N4	131.65
DIST N1-N5	257.203518638451
DIST N1-N6	345.517307815397

Fig. 9.2: Automatic Distance Calculation.

c = _root.b1;

a. s = _root.b2;

b. deltaX = c._x-s._x;

c. deltaY = c._y-s._y;

_root.tooltip.dist=Math.sqrt((deltaX*deltaX) + (deltaY* deltaY));

Where **C** is the variable which stores the current position of the **node 1** named b1 in the simulation.
S is the variable which stores the current position of node 2 named b2 in the simulation.
deltaX is the variable which stores the difference of X value of both of the nodes
deltaY is the variable which stores the difference of Y value of both of the nodes
dist is the variable which stores the exact distance between the two nodes

(3) This value is used in the route management of the nodes to detect the shortest path between the nodes.

B. Route Management

(1) In this Scenario the users see the shortest route possible for communication or data transfer. We are using shortest path so that we can transfer our data as soon as possible to our destination.

(2) The user gets four different routes .The four routes are shown in below figure , these four route shows the path from source node to destination node to transfer data. From that four route the system select the shortest path between source to destination for data transfer.

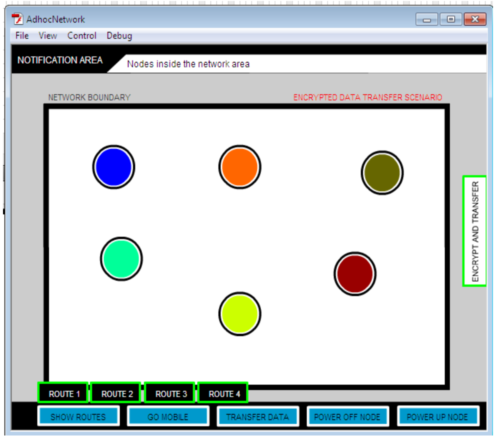


Fig. 9.3 (A): Route Management Between Source And Destination.

(3) In below figure a line is present that represent the shortest path between Source and destination. Based on the algorithm the shortest route is selected to transfer or to send the data.

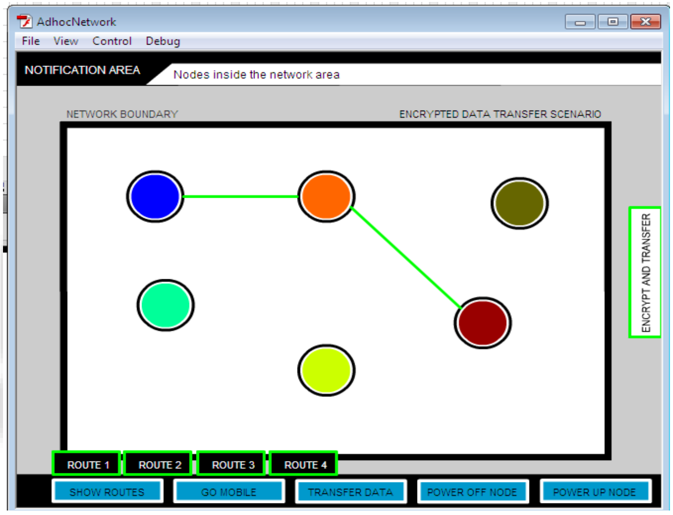


Fig. 9.3 (B): Route Management Between Source And Destination.

C. Communication

Communication is a process by which information is exchanged between individuals. To have successful communication between source and destination , the data have to be transferred in encrypted form .Encryption is required so that unauthorized person cannot read or change the original text .And at the receiver side that data is decrypted and converted into original text or a readable form.

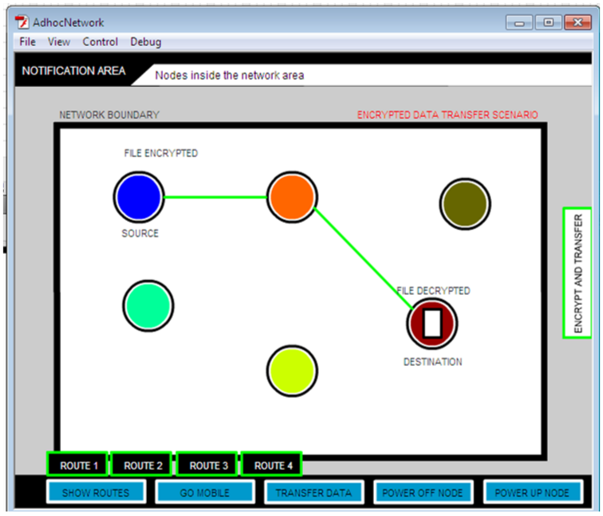


Fig. 9.4: Show Communication Between Source And Destination.

X. CONCLUSION

The paper introduced the new approach for secure routing in MOBILE AD-HOC NETWORK blending together the widely used ant colony optimization meta-heuristic and some intelligent techniques like local transmission and automatic route discovery using UANT. Introduction of the new artificially intelligent techniques in existing approach like ACO resulted in the modeling of the new multi-agent based algorithm which can be implemented in Rural Communication MOBILE AD-HOC NETWORK for transmission of critical Rural Communication information. The algorithm, on comparison, proved to be better than the similar existing algorithms like ARA and AODV in terms of dynamicity, error handling and reducing overhead. The algorithm proposed is robust, dynamic, scalable and flexible and thus, can be used in Rural Communication and defense sector with high degree of reliability. The communication among the nodes will be more secure because of the proposed encryption technique selected.

REFERENCE

[1] Bing Wu, J. C. (2006). A Survey on Attacks and Countermeasures in mobile addhoc network. *WIRELESS/MOBILE NETWORK SECURITY* , 2-6.
[2] G.Varaprasad. (2005). New security algorithm for mobile adhoc networks using zonal routing protocol. *Ieee journal*. 2-4.
[3] Haas, Z. J. (2002). Secure Routing for Mobile Ad hoc Networks. *distributed Network and simulation conference,1-2.*
[4] J.A. Freebseryser, B. L. (2001). A DoD perspective on mobile ad hoc networks. *Ad hc networking* , 29-51.
[5] Pietro Michiardi, R. M. (2010). Ad hoc networks security. *Security in Networks* , 1-2.
[6] Shuyao Yu. (2010). A security architecture for Mobile Ad Hoc Networks. Security Architecture,2-4.
[7] Jacquet, P. et al. Optimized Link-State Routing Protocol (OLSR).IETF draft,18July,2000.
[8] Ji, L. and Corson, M. S. Differential Destination Multicast Specification (DDM). IETF draft, 12 July2000.

Image Reference

[1] Q.Fang. (n.d.). Retrieved from http:/ /graphics.stanford.edu/projects/lgl/papers/fzg-lscptea-2003/image .gif.
[2] Figure:1.1http://www.google.co.in/imgres?hl=en&client=firefox-a&hs=SAM&sa=X&rls=org.mozilla:en-US:official&biw=1366&bih=665&tbm=isch&prmd=imvnsb&tbnid=T_7qAWCKRc2BuM:&imgrefurl=http://mudji.net/press/%3Fp%3D166&docid=uKzEEGQj7YP0HM&imgurl= http://mudji.net/press/wpcontent/uploads/2006/11/rsa-encrypt.JPG&w=500&h=350&ei=dWRXUIzdA8fYrQfq8oDIDw&zoom=1&iact=hc&vpx=777&vpy=282&dur=223&hovh=188&hovw=268&tx=134&ty=87&sig=106410129848198221949&page=2&tbnh=131&tbnw=187&start=18&ndsp=24&ved=1t:429,r:21,s:18,i:213