ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Secured Data Transmission in Mobile Adhoc Networks: An Implementation Using Java

Drashti Gautam[1], Dr. Anurag Sharma[2]

M.Tech Scholar, Dept. of Computer Science and Engineering, FET,Agra College, Agra, India[1]

Assistant Professor and Head, Dept. of Computer Science and Engineering, FET,Agra College, Agra, India [2]

ABSTRACT: MANET stands for mobile ad-hoc network. It is basically a collection of nodes where each node performs as independent router or host. Mobility is the core feature of MANET. Therefore routing protocol is needed that changes whenever topology changes. Secure data transmission is the most important issue in MANET. The emerging trends for mobile ad hoc networks and secured data transmission phase are of significant importance based upon the environments like military. In this paper, a new way to improve the reliability of data transmission is presented. In the open collaborative MANET environment, any node can maliciously or selfishly interrupt and deny communication of other nodes. Dynamically changing topologies makes it hard to determine the opponent nodes that affect the communication in MANET

KEYWORDS: Mobile Ad-hoc Network, node, data transmission, routing protocol, topology, cryptography

I. INTRODUCTION

Ad-hoc network can be explained as a temporary network set-up (short lived network)to allow mobile computer users with wireless communication devices to communicate with each other. A mobile ad-hoc network MANET is defined as a collection of mobile platforms or nodes where each node is free to move. Manet is a wireless, mobile, multi-hop, distributed network which does not hold any infrastructure except for the nodes themselves which are communicating. A manet uses the current internet technology over wireless nodes using a network cloud. A network cloud is made up of several autonomous, mobile, wireless nodes that may or may not be connected to the wired internet.
Since Ad-hoc networks for wireless communication using mobile hosts (which we call nodes) for secure data transmission. As in an ad-hoc network, there is no fixed infrastructure such as base stations or mobile switching centres. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart they transfer the packet via other nodes as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

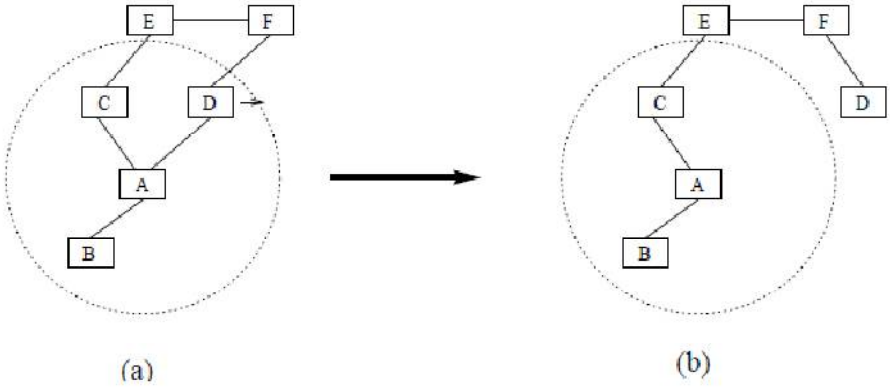

Figure 1

II. IDENTIFICATION OF NEEDS

Infra-structured Networks

The early known networks comprises of infrastructure, in these infrastructures we need to have a base station that will hand over the offered traffic from a station to another, as illustrated in Figure 2. The base-station regulate S the attribution of radio resources, for instance. When a node S wishes to communicate to a node D, the former notifies the base station, which eventually establishes a communication with the destination node. At this point, the communicating nodes do not need to know of a route for one to each other. All that matters is that both nodes source and destination are within the transmission range of the base station. If one of them fails to fulfil this, the communication will abort.

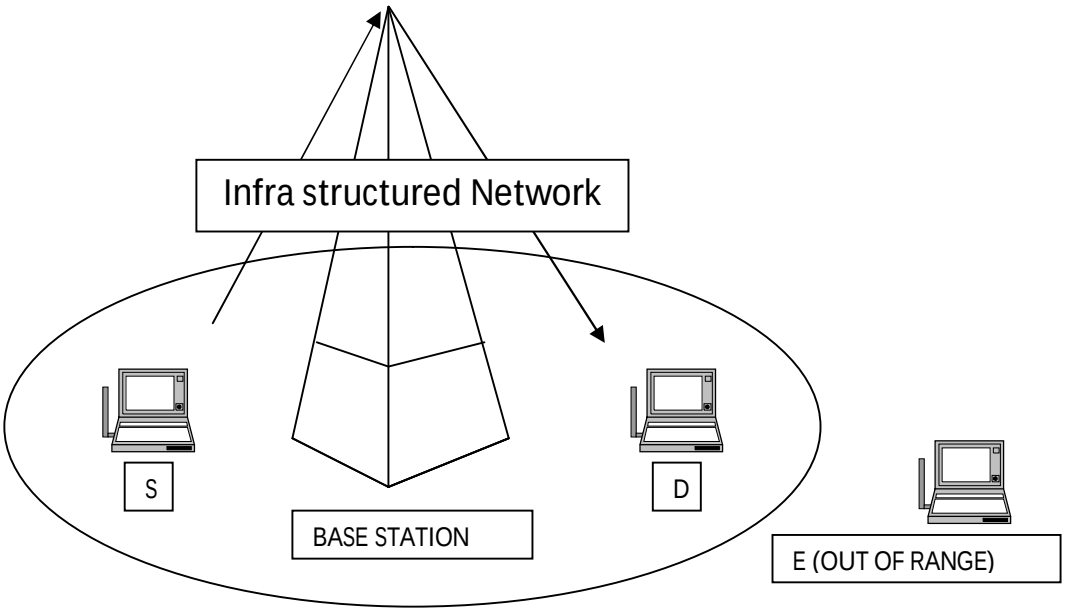

Figure 2

Here the base station's range is illustrated by the oval. The two nodes S and D which want to communicate are in the range of the base station. S send the message to the base station which in turn forwards it to destination node D. Thus communication is carried out with help of a base station. All messages have to pass through the base station. Node E is out of the range of the base station this prevents it from communicating to other nodes in the network. When node E

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

wants to communicate to any node in the network it has to contact the base station. Since it is out of range communication is not possible.
What happens if the base station is unavailable? Or what happens if we are in a situation where such an infrastructure does not exist at the first place? The answer is that we simply do not communicate! This is where the second approach is useful. Note however that this form of centralized administration is very popular among wide cellular networks such as GSM etc.

III. PROPOSED SYSTEM

Infra-structure-less Networks (Ad Hoc)
The Ad-Hoc, does not rely on any stationary infrastructure, it is devoid of any basic infrastructure. The concept behind this infrastructure less networks is the dependency between its participating members, instead of making data transit through a fixed base station, nodes consequentially forward data packets from one to another until a destination node is finally reached. Typically, a packet may travel through a number of network points before arriving at its destination.
Ad-hoc networking introduces a completely new technology of network formation. The term Ad-Hoc means, in this instance, a type temporary network connecting various mobile devices without the intervention of fixed infrastructure. The routers and hosts are free to move randomly and organize themselves in an arbitrary fashion, thus the network topology changes rapidly and unpredictably. Absence of a supporting structure in mobile ad-hoc networks, to a certain extent, invalidates almost all of the existing techniques developed for routine network controls in the existing wireless networks.
A MANET consists of mobile platforms, a router with multiple hosts and wireless communications devices herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network.

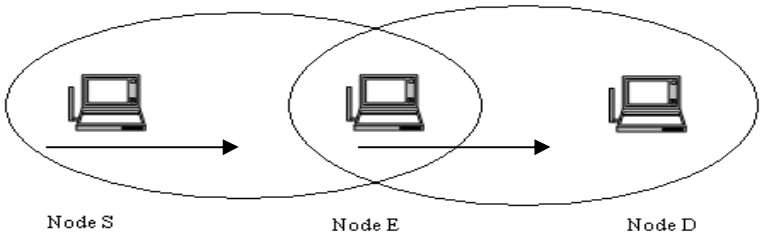

Figure 3

Infra-structure less Network

Here the node S wants to communicate to node D. The oval indicates the communication range of the node. The communication range of S does not exceed to include D. In this case routing is necessary, node E is in the range of S which has D in its range. So S in order to communicate to D, first sends the message to E which in turn forwards it to D. Thus the node E acts as a router and a node as shown in figure3. Thus in this way the Ad Hoc network co-operates to forward packets for each other to communicate without the help of a base station. But there are several issues like selfish nodes, malicious behaviour, routing challenges, security etc.

2. Routing Protocols
The primary goal of routing protocols in ad-hoc network is to create a path (minimum hops) between source and destination with minimum overhead and minimum bandwidth use so that packets are transmitted in a timely and orderly manner. A MANET protocol should function effectively over a large range of networking context from small ad-hoc group to larger mobile multi-hop networks. As Figure 4 shows, the categorization of these routing protocols.
Routing protocols, depending on the routing topology can be categorized into proactive, reactive and hybrid protocols, Proactive protocols are usually table-driven. Examples of this type of protocol are Destination Sequence Distance Vector (DSDV). Reactive or

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

source-initiated on-demand protocols, in contradictory, do not regularly update the routing information. It is distributed to the nodes only when required Example of this type of protocol is Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type of protocol is Zone Routing Protocol (ZRP).

Dynamic Source Routing (**DSR**) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. In Dynamic Source Routing, each source determines the route to be used in transmitting its packets to selected destinations. There are two main components, called Route Discovery and Route Maintenance. Route Discovery determines the optimum path for a transmission between a given source and destination. Route Maintenance ensures that the transmission path remains optimum and loop-free as network conditions change, even if this requires changing the route during a transmission.

IV. IMPLEMENTATION

Step by step Algorithm:

- Get the Destination identifier and the encrypted data to be transferred.
- Initialize the buffer with the encrypted data to be transferred.
- Setup a Request Zone.
- Build a Route Request packet having the information about the source and the Destination identifiers, and the Request Zone information.
- Broadcast the Route Request to its neighbors.
- Setup a timer for receiving Route Reply.

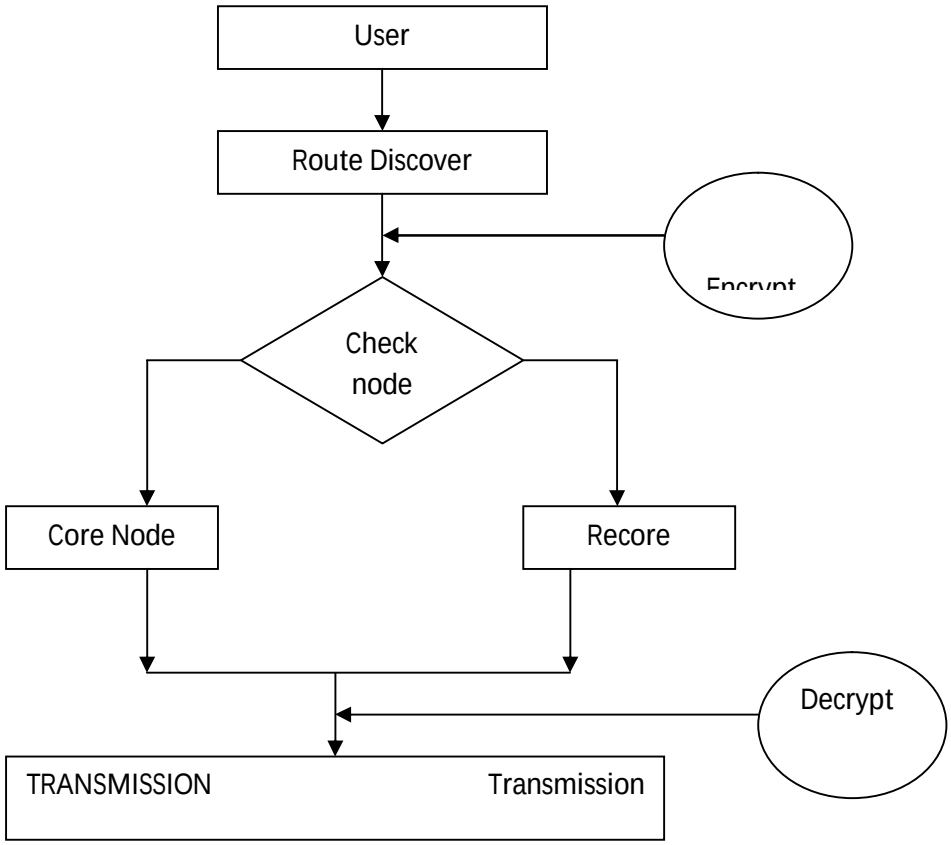

Figure 4

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Implementation is the stage in the project where the theoretical design is turned into a working system and is giving confidence on the new system for the users, which it will work efficiently and effectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the change over, an evaluation, of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The more complex system being implemented, the more involved will be the system analysis and the design effort required just for implementation. An implementation co-ordination committee based on policies of individual organization has been appointed. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system.
Implementation is the final and important phase, the most critical stage in achieving a successful new system and in giving the users confidence. That the new system will work be effective .The system can be implemented only after through testing is done and if it found to working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

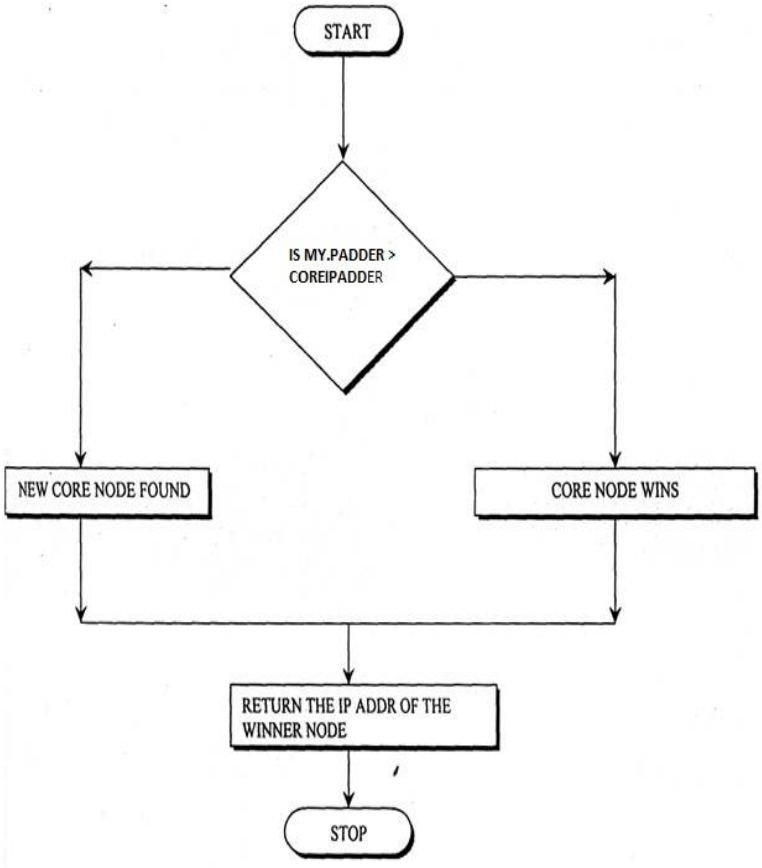

Figure 5

In figure 5 searching of address for the transmission using expand search ring method. Figure 6 is describing the process of tuning transmitter and receiver and getting acknowledgement from receiver to receive data from transmitter in the encrypted data. At the end of receiver decrypts the data for successful transmitted data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

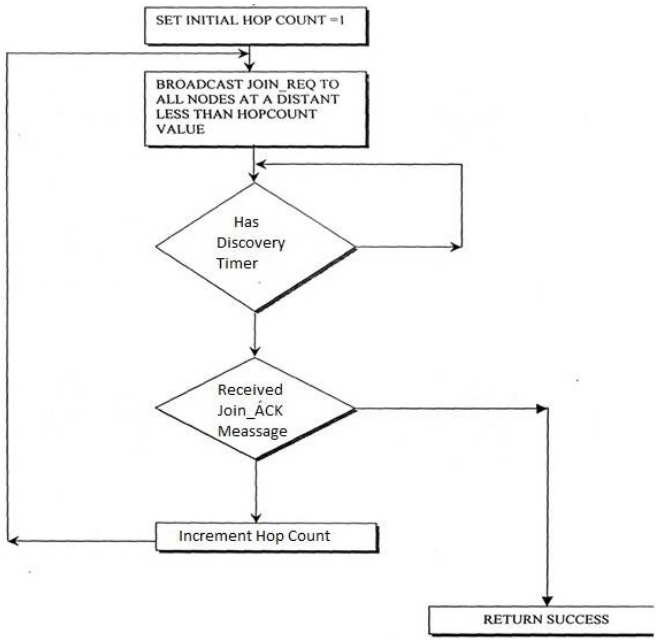

Figure 6

V. RESULTS AND DISCUSSION

Some screen shots of implemented project using java networking technique over IPv4, first we run transmitter side so we can select the file which we want to send, after that we use encryption technique to encrypt data. The encrypted data will be sending to the node which we have selected using expand ring search technique. The receiver received the encrypted data and after that it is decrypt the encrypted data which have been received by receiver from transmitter. This shows a successful secure data transmission over MANET.

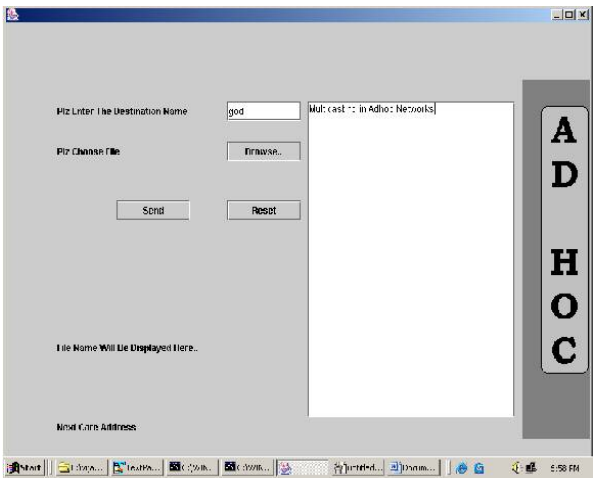

Figure 7.1 Front-end snapshot of the source node

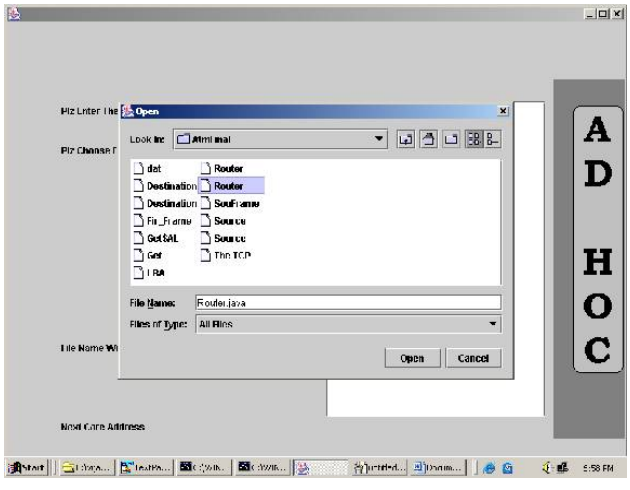

Figure 7.2 Browsing the file to be sent to destination

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

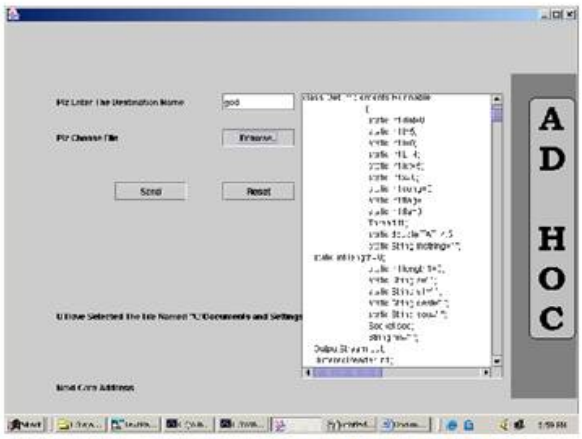

Figure 7.3 Sending selected file to destination

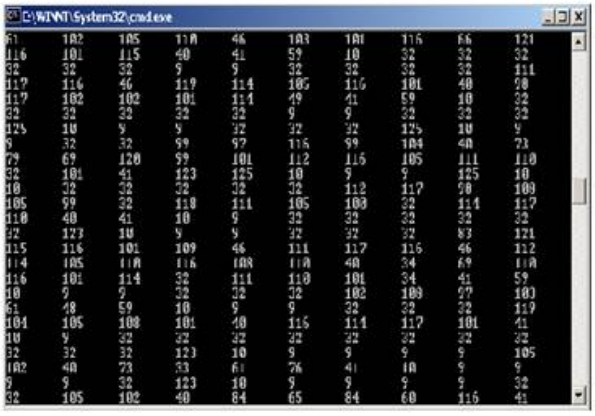

Figure 7.4 Encrypted form of the file

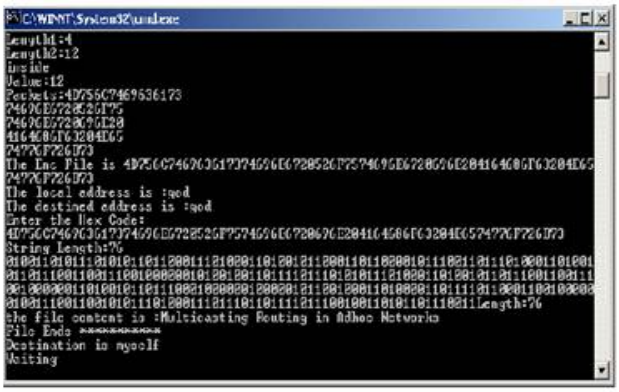

Figure 7.5 finding the core node to send data

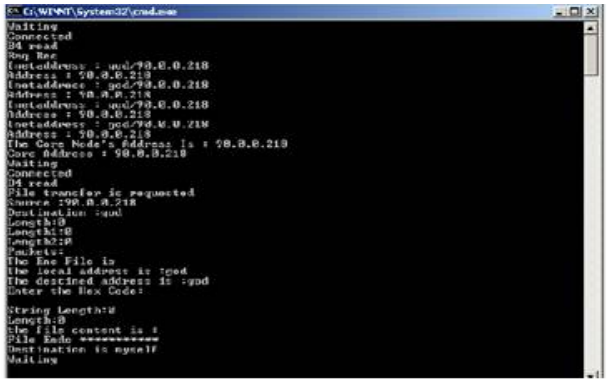

Figure 7.6 Decrypted form of the file

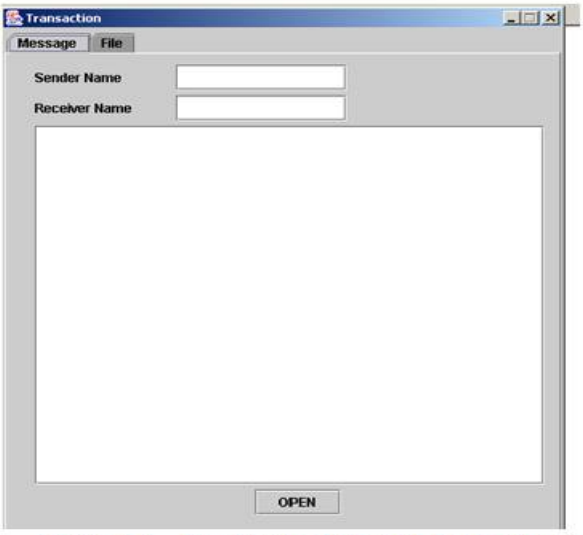

Figure 7.7 Front-end snapshot of destination node

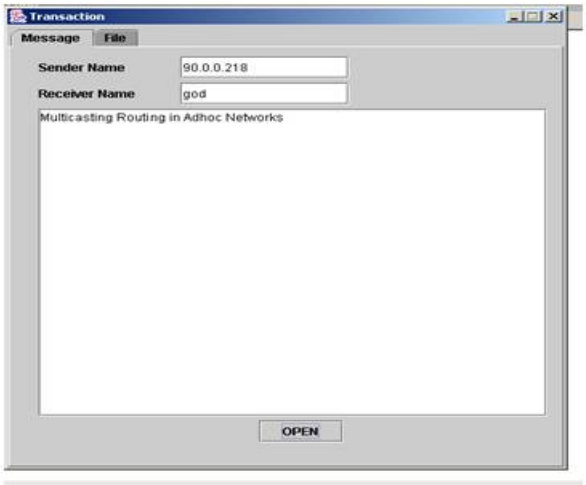

Figure 7.8 Receiving data at destination node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

VI. CONCLUSION AND FUTURE ASPECTS

It achieves its goal by combining a routing method with a link state-based mechanism. Further, it introduces the concept of anchors, which are geographical points imagined by sources for routing to specific destinations, and proposes low overhead methods for computing anchors. The successful secured data can be transmitted using encryption and decryption technique during the transmitter and receiver in Mobile Ad-hoc Network. A Mobile Gateway has been developed that uses a cellular network for the connection. It handles the challenges that had to be solved to realize this interconnection and describes a way how to connect two IPv6 networks over an IPv4 infrastructure.

REFERENCES

1. Herbert Schildt, Edition (2003) '**The Complete Reference JAVA 2'** Tata McGraw Hill Publications .
2. Michael Foley and Mark McCulley, Edition(2002) **'JFC Unleashed'** Prentice-Hall India.
3. Andrew S Tanenbaum, Edition**(2003) ' Computer Networks** '
4. P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS CNDS*, San Antonio, TX, Jan. 27–31, 2002, pp.193–204.
5. M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM WiSe*, Atlanta, GA, Sep. 2002, pp. 1–10.
6. Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM MobiCom*, Atlanta,GA, Sep. 2002, pp. 12–23.
7. K. Sanzgiri *et al.*, "A secure routing protocol for ad hoc networks," in *Proc. ICNP*, Nov. 2002, pp. 78–87.
8. P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *Proc. IEEE CS Workshop on Security and Assurancein ad hoc Netw.*, Orlando, FL, Jan. 2003, pp. 379–383.
9. Y. Hu, A. Perrig, and D. B. Johnson, "Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–190, Jul. 2003.
10. P. Papadimitratos and Z. J. Haas, "Secure QoS-aware route discovery in ad hoc networks," in *Proc. 2005 IEEE Sarnoff Symp.*, Princeton, NJ, Apr. 2005, pp. 176–179.
11. "Secure on-demand distance-vector routing in ad hoc networks," in *Proc. 2005 IEEE Sarnoff Symp*., Princeton, NJ, Apr. 2005, pp. 168–171.
12. S. Kent and R. Atkinson, "Security architecture for the Internet protocol," IETF, RFC 2401, Nov. 1998.
13. "IP authentication header," IETF, RFC 2402, Nov. 1998.