Using IP Multicast Distribute Encryption Message

Maha SabriAltememe
Computer Science Department, College of Science
Kerbala University ,Kerbala, Iraq
Email :maha.sabri@uokerbala.edu.iq

Abstract

There are many aspects have been discussed in this study for IP multicasting. It can be used in many applications such as chatting in local area network, marketing and also can be used in educational services. This paper shows such IP multicasting of how create and use it in many application. This paper also discussed many issues for IP multicast such as adding and leaving the join group, advantages and disadvantages of IP multicasting. The prototype has been applied in WLAN by sending secure messages from one client to many recipients. Furthermore, it shows the time between many recipients for sending and receiving such messages based one simple security algorithms for more security.

Keyword : Encryption Message, Client Server , Distributed System, Information Technology.

1. Introduction

Distributing , as a word it used with a different term such as distributed system, distributed programming and distributed algorithm, in fact it referred to computer networks. Where computers are physically distributed individually within some geographical area and make a connection between them. Nowadays these terms are used in a much wider sense, even referring to independent processes that run on the same computer and interact with each other by sending messages[2].Generally, the communication between two computers (client and server) needs to be reliable. Therefore, every device connected to a distributed systems network is assigned a unique number known as an Internet Protocol (IPv4 or IPv6) address. The IP is part of the communication protocols that allow communicating between the devices on the networks[1].

There are three main types of IPv4 addresses: Unicast, broadcast, and multicast. Unicast id designed to transfer a packet between two hosts (node) in the network. A broadcast is used to send packets to sub network domain. A multicast address is designed to enable delivery of packets to the set of hosts that have been configured as a group address from 244.0.0.0 to 239.255.255.255 in various sub networks. The main disadvantages of multicast are not connection oriented[12]. A multicast is delivered to destination group member with the same "best-effort" reliability as a slandered unicast IP. The main difference between a multicast IP packet and a unicast IP packet is the presence of a "group address" in the Destination Address field of the IP header[2].

Each host is free to join or leave using a datagram socket as a join group at any time. That's mean no restriction on the physical location or how many numbers of members in a multicast group. The main device on the internet is router that uses the group membership protocol to learn about the existing of hosts in the network that attached in its sub network[15].

Processes that work between one sender and one recipient ,Browsing Systems and email Is an example of online applications. another field It requires the latest applications, One user (sender) sends data to a number of

receivers at a same time. This application will use to optimize to ability of organization ability to Collaboration and communication with information, Increasing the importance of using networks. This feature in IP Multicast is an important advance in IP networking .The use of multicast feature can be applied to easy work and we have added a simple security encryption package to send to number of receives to make it more secure for data exchange or for future development.

One of the main challenges that face the time needing to send messages from one sender to group those receive this message, this way by using unicast takes more time for sending to the group because it needs to send one message at each time to each one of the group. So when sends message to group contain five clients, it will need to send this message five times. On the other hand, with IP Multicast it would be easy to support many of the recipients. By multicast will reduce time so it can pervious message send only one, and another challenge to ensure securing multicast communication is confidential information that is transferred or receive enable data multicasting to verify, that the data contained originated should be sent to the user without another ,problem becomes more complex in common, in other word encryption of a document in a secret key constitutes a signature strong authentic ation of document and weak against repudiation , in particular send to a group of recipients .

The objective of this paper proposes distribute encryption message based on IP multicast .with IP multicast it would be easy to support many of recipients as it achieved the speed and secrecy in the transfer of information. The main research objectives of this study are: To measure the performance for the group hosts based on response time between the sender and the many receivers, To implement the secure packet for sending the encryption messages between many hosts using some encryption algorithm and to understand the difference between broadcast, multicast, and unicast and how the Protocol Independent Multicast Protocols (IMP) to join the new client with a group.

This study provides an executive introduction to IP Multicast to be used among many groups. It presents the basic concept for IP multicast; highlights its advantages and disadvantages, and provides implemented to secure sending packet based on encryption algorithms. It also shows network performance by joining and adding new users simultaneously and the algorithm can show the efficient response time among many hosts even in a second or mill i-seconds. Whether one is a user of TCP/IP-based technologies or an organization interested for implementing or taking advantages of IP Multicast within product or service, this study will be beneficial and lucrative for all of them. This study shows "administratively scope of IPv4 multicast space" to be in the range of IPv4 from 239.0.0.0 to 239.255.255.255. The application has been applied practically using local area network connected with the internet. The application put into use the safe type language “Java programming” to operate the whole program.

2. Literature Review

2.1 Multicast Protocols

The most frequently used transport layer protocol to employmultiple addressing is the User Datagram Protocol (UDP). By nature, UDP is not dependable—loss of messages and delivery that is out of order are quite possible. Dependable multicast protocols, e.g. Pragmatic General Multicast (PGM) have been evolved to add loss detection and retransmission to IP multicast.

IP multicast is commonly utilized in businesses, stock exchanges, and networks sending multimedia material. A frequentbusinessemployment of IP multicast is for IPTV applications such as distance learning and televised company meetings [30].

Liao et al. and Wu et al. have offered to make the loss retrieval easier via intermediate nodes so as to shun latency and messaging overhead [1,2]. Xu et al. have exploited a technique to provide quality of service to video applications [3].
Pagani et al. have applied a method that adaptively selects flooding and retrieval along routing tree based on the mobility [4]. A lot of scholars like Alperton et al. evolve a technique which employs flow control to guarantee dependability [5].

2.2 Privacy in Multicast

One of the most important security concerns in multicast is maintaining privacy of communication. How do multiple network users who are in the same multicast "group" exchange data such that no one outside the group can decipher what is being sent? A natural way to guarantee this would be to have users share a common key, called the group key, and to require that all multicast transmissions from any user within the group be encrypted using that key. If they are guaranteed that the group key is known only to group members, then such an encryption protocol would trivially solve the privacy problem [28, 30].In Figure1 this would mean transmitting to all nodes in network. In Figure 2 illustrates transmitting to all nodes but privacy in multicast.

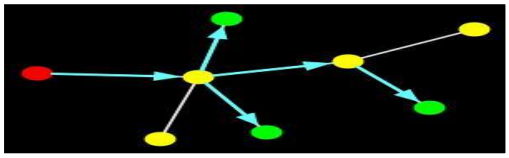

Figure 1.Transmitting to multiple recipients using Multicast

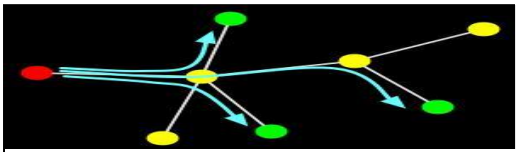

Figure2. Transmitting to multiple recipients using privacy in multicast

Example researches, Brooks's et.al (2009) applied Multicast Encryption Infrastructure for Security in Sensor Networks. Designing secure sensor networks is difficult. They propose an approach that uses multicast communications and requires fewer encryptions than pair wise communications. The network is partitioned into multicast regions; each region is managed by a sensor node chosen to act as a key server. The key servers solicit nodes in their neighborhood to join the local multicast tree. The key server generates a binary tree of keys to maintain communication within the multicast region using a shared key .This approach supports a distributed key agreement protocol that identifies the compromised keys and supports membership changes with minimum system over head. They evaluate the overhead of this approach by using the number of messages and encryptions to estimate power consumption. Using data from field tests of a military surveillance application, they show that this multicast approach needs fewer encryptions than pair-wise keying approaches. They also show that this scheme is capable of thwarting many common attacks [29].

Duan and Canny (2006) presented a general framework for constructing effective multicast cryptosystems with provable security and show that a line of previous work on multicast encryption are all special cases of this general approach. They provided new methods for building such cryptosystems with various levels of security (e.g., IND-CPA, IND-CCA2).The results they obtained enable the construction of a whole class of new multicast schemes with guaranteed security using a broader range of common primitives such as OAEP. Moreover, they were show that multicast cryptosystems with high level of security (e.g. IND-CCA2) can be based upon public key cryptosystems with weaker (e.g. CPA) security as long as the decryption can be securely and effectively "shared". This constructions feature truly constant-size decryption keys whereas the lengths of both the encryption key and cipher text are independent of group size [24].

3. Methodology

The methodology for this work contains four phases including State problem, Sending Message, Pre-processing message and Evaluation of Model. We follow this methodology because each phase in this methodology is related to the research and scope .it is a very flexible in implementation and it will be suitable for our work. The steps of the data process are illustrated in Figure 3.

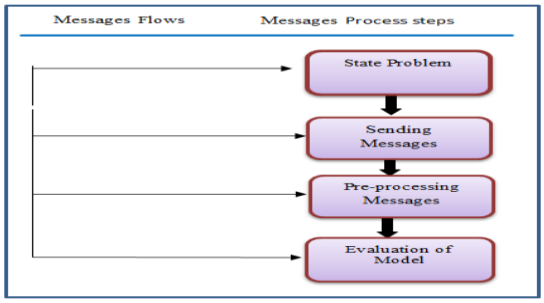

Figure3.MessagesProcess Representation

3.1 State problem

The first step in general methodology is awareness of the problem. The information about problem come from many sources: new developments in industry or in a reference discipline. For this study the awareness of the challenges that face the time needing to send message from one sender to group those receive this message, this way by using unicast takes more time for sending to group because it needs to send one message at each time to each one of group . So when send message for group contain five clients, it will need five once send message .On the other hand, with IP Multicast it would be easy to support many of recipients. By multicast will reduce time so it can pervious message send only one. Also we have suggested her to send messages in more securely.

3.2 Sending Messages

The second phase of the methodology suggested adding security to message that sending to many hosts to protect sending message from intercept by using encryption algorithm, the encryption key can be extracted from the mathematical formula in Figure 4 shows that, the Java code of the encryption algorithm is given as Figure 5.

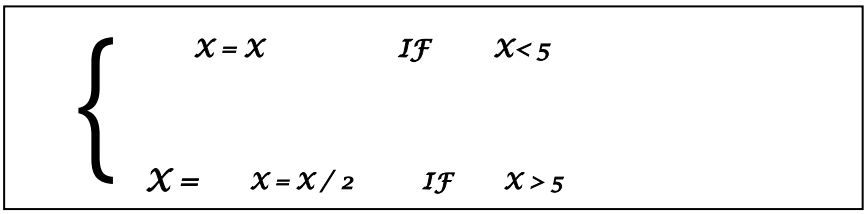

Figure4.mathematical formula for extracting the encryption key

```
396          public String kaserEn(String str){
397              // Effect:  returen encryption str
398              // Require: str
399              // Modify:  str
400                          int i, intc; char c=' '; char cc;
401                          i = 0;
402                          // to create encryption key
403                          int x = str.length();
404                          while (x>5){
405                              x = x/2;
406                          }
407                          String ss="";
408                          // to ncryption
409                          while (i < str.length()){
410                          c = str.charAt(i);
411                          intc = (int) c;
412                          cc = (char) (intc + x);
413                      ss=ss+cc;
414                          i++; }
415                          return ss;
416                  }
```

Figure5. Java code for encryption algorithm

This formula will receive the total length of the string (text message) from the method , and if the total number more than Five it will start divide it by Two until be less than Five. Finally the result from the formula will consider as the encryption key, and this technique ensures the changeable key, so that only receiving who has authentication can see the original message by using decryption key to break the encryption message. An application developed and designed by using the Java language, because it's suitable to build this project type and Using Java tools help to achieve flexibility for the application.

3.3Pre-processing message

We develop this project by using the Java language, to show an advantage and dis-advantage for IP multicast with a simple encryption algorithm.

3.4Evaluation of Model

We evaluate this work by using LAN, so we makes test for our work on LAN network that connected with router to the internet. The first step, we send message that no need to be secure (without encryption) ,all clients see the content message directly ,and repeat sending without secure (with encryption) that one client want only one client read his message and no one from the other will read the content of the message .It was successful test ,after send message with encryption that was seen for all client but no one can read the content because the encryption ,the target client was enabled to read content message after make decryption to the message.

3.5 Simulation model

In this methodology we will propose our work mechanism model to show message sending process from sender to group of receivers, moreover the process of sending and receiving encryption message between many hosts .Sending and receiving blind text: Sending unencrypted message to group of receivers, as well as every host receiving the message at the same time .The java code of this part of the application is presented in Figure6.

```
331
332          public void SendRequest(){
333             // Effect: send the blind text
334             // Require: the connction is enable
335          try{
336               add = InetAddress.getByName("224.0.0.0");
337               MulticastSocket socket = new MulticastSocket();
               byte[] buffer = new byte[65535];
339               String mess = jTextField2.getText()+":"+ area.getText();
340               buffer = mess.getBytes();
341               DatagramPacket packet = new DatagramPacket(buffer,buffer.length, add, 6789);
342               packet.setData(buffer);
343               socket.send(packet);
344               area.setText("");
345               socket.close();
346                  }
347                catch(IOException io){}
348                 }
```

Figure 6. Java code for sending blind text

Sending and receiving encrypted text: Sending encryption message to a group of receivers as Figure 7shows, as well as every host receiving the encryption message at the same time as Figure8shows. The java code of this part of the application is presented in Figure 9.

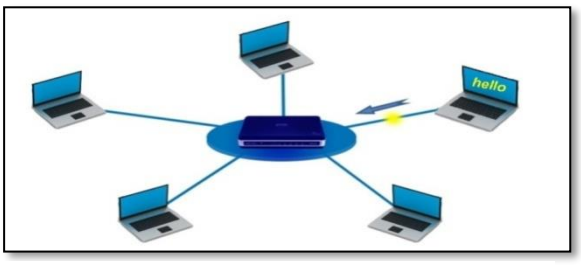

Figure 7.explains encryption sending the message

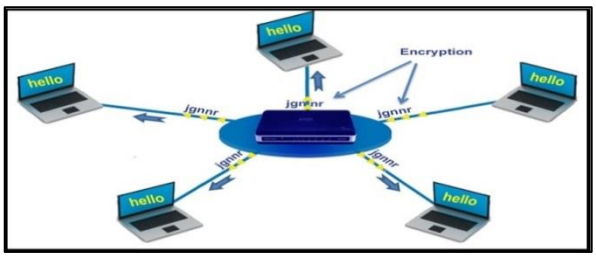

Figure8.explains receiving the encryption message

```
375          public void    SendEnRequest(){
376          // Effect:  send the encryption message
377          // Require: the connection is enabled
378          try{
379               add = InetAddress.getByName("224.0.0.0");
380               MulticastSocket socket = new MulticastSocket();
381               socket.joinGroup(add);
382               byte[] buffer = new byte[65535];
383               String mess1 =  area.getText();
384               String mess=kaserEn(mess1);
385               String mess2 = jTextField2.getText()+":"+ mess;
386               buffer = mess2.getBytes();
387               DatagramPacket packet = new DatagramPacket(buffer,
388               buffer.length, add, 6789);
389               socket.send(packet);
390               area.setText("");
391               socket.close();
392               }
393                catch(IOException io){}
394                          }
```

Figure 9. Java code for sending encryption message

The user can send and receive the blind text as well as the encryption text as Figure10 process of sending and receiving the message between any two hosts.

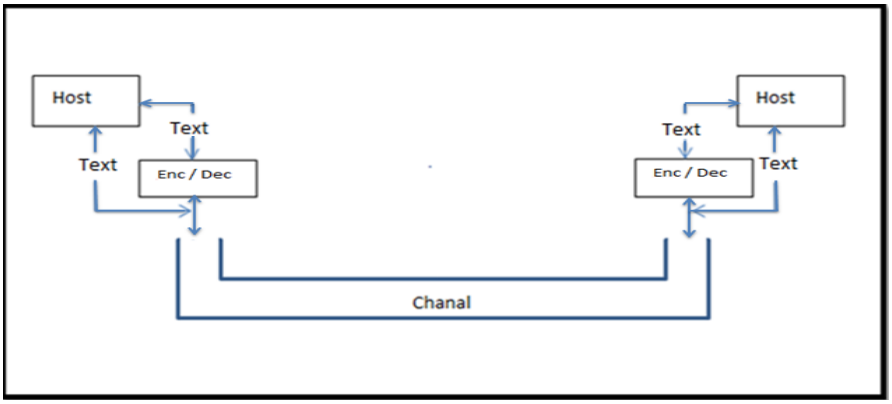

Figure 10.sending encryption message

3.6 Experimental Steps

In this part we are going to illustrate application mechanism that consists of two steps (login window and chat window) that shows as below:

3.6.1 Login window

Main login interface as in the Figure11.This application requires the user to perform an authentication procedure whereby they are required to insert a user name and password in order to use this chat application. The application will be launched when the user entered the correct username and password. However, if the user entered the wrong combination of username and password, the program will immediately show error box that contain a message to inform the user to correct the inserted username and password.

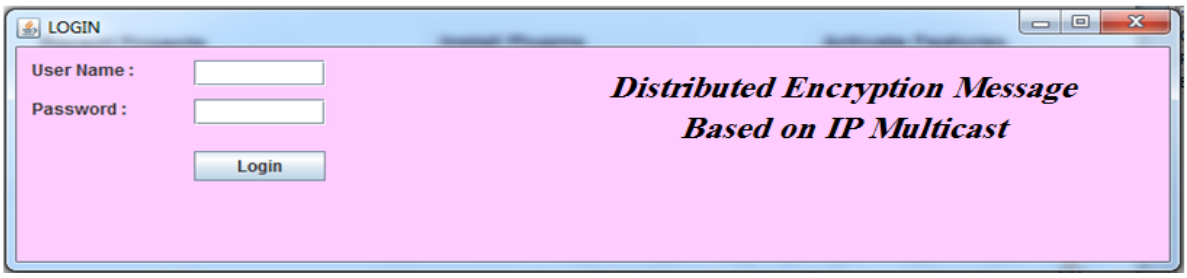

Figure 11.login

3.6.2 Chat Window

Figure 12 presents the main user interface for our chat application. The interface includes labels and buttons that increase the application's usability and ease of use.

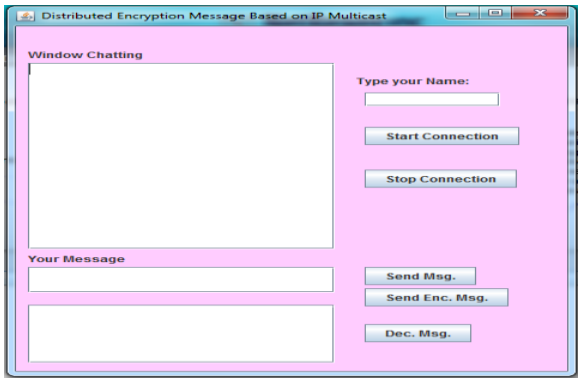

Figure12.application windows

But, if the user didn't type any name to join the chat group and try to start a connection, the application will show error box that contains message to ask him to type his/her name .Users may connect to the server simply by clicking on the 'Start Connect' button provided on the main interface. When the connection successfully done, the window chatting will display "Server is started". Once a connection with the server is established, a user may have the option to continue on using text chatting by writing their message in the 'Your Message' textbox area show that in Figure 13.

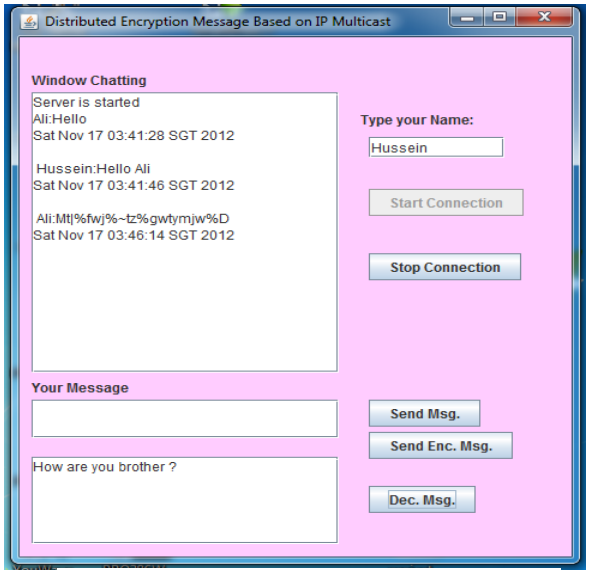

Figure13. Appear Message and Time

Also, once connection with the server is established, a user may have the option to continue on using text chatting by writing their message in the 'Your Message' textbox area. After that, the user is able to use "Send Enc. Msg." to send encryption message. Every encryption message will display in window chatting. The message will not appear same once that write on the text area "Your Message" because it will encrypt in our Algorithm. Also, the encrypted message will display on the all hosts in the same samples as a Figure 14 showing that approach.

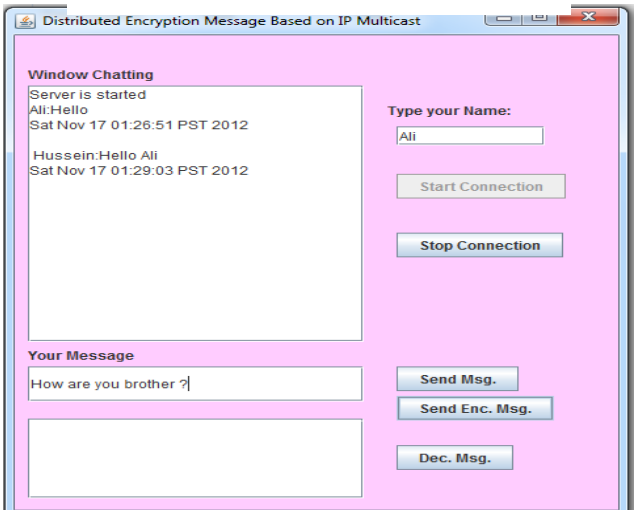

Figure 14. Appear Encryption Message on X Host

3.7 Program setup

Installation for computer program is the procedure of action the program ready to work .Some computer programs can be operated by only copying them into a folder stored on a computer and operating them. Other programs are supplied in a mode that cannot be immediately executed and thus require a setup procedure. When installed, the program can be operated repeatedly, needing no reinstallation prior to each operation.

The chat application requires two principal things to operate correctly. Firstly, the application is constructed using the Java programming language; hence, the user has to install Java Runtime Environment (JRE) and the Java Development Kit (JDK). Next, the application can operate with no error at all. Nevertheless, the program still requires to be connected to the network for linking with a set of IP.

3.8 Tools

Customarily, most computers used to communicate using the Network Protocol; consequently a network socket is point ending between two operation connection stream across network for computer. the application of socket API is interface application API generally supplied by the operating system, that permits application programs to control and use network sockets.

Network socket APIs generally conform to the Berkeley sockets standard. A socket address consists of an Internet Protocol address and a port number, just like one end of a phone connection which consists of a phone number and

some extension. Using this address, network sockets send received data to the suitable application operation or thread.

Java is a language used in object-oriented programming. It has anion-built application programming interface (API) that can tackle images and user interfaces and that can be employed to devise new applications or applets. Due to its diverse collection of API's, like Macintosh and Windows, and its platform independence, Java can further be considered as a platform on its own. In addition, it has standard libraries for doing math's, not to mention Java including numerous libraries. The java net pack purveys two classes--Socket and Server Socket--that execute the client part of the connection and the server part of the connection, respectively.

3.9 Platform

Net Beans IDE is original for free java when most developers for systems , this Net Beans IDE support of many language such as JavaScript, PHP,C++ and JavaFX.Net Beans is an open-source project dedicated to providing rock solid software development products (Net Beans IDE and Net Beans Platform) that address the needs of developers.

4. Finding Results and Conclusion

The objective of this project was to design and implement a chat application based on the multicast technology, which allows sending and receiving instant messaging and sending the encryption messages between many hosts using some encryption algorithm. All these operations were under wireless local area network (WLAN). The application client side was implemented on the windows platform using the Java language and the Socket library file, while the chat application was implemented on Net beans IDE 7.1 using a Java language. [17]

The main results that we obtained in this project; it is success to send and receive the message based on IP multicasting technique . The message can be send from one client to group of receivers, as well as anyone can join the multicast group by getting the application.

Moreover, the security issue is a second object that we have achieved in this project. Where, the clients can receive cipher text, but who can send that text and decrypting it just that who has the application that we have suggested as clearly shown in Figure 15. This application contain encryption algorithm to provide high secure level for top secrete text.

There are many aspects have been discussed in this study for IP multicasting. It can be used in many applications such as chatting in local area network, marketing and also can be used in educational services. This paper shows such IP multicasting of how create and use it in many application. This paper also discussed many issues for IP multicast such as adding and leaving the join group, advantages and disadvantages of IP multicasting. The prototype has been applied in WLAN by sending secure messages from one client to many recipients. Furthermore, it shows the time between many recipients for sending and receiving such messages based one simple security algorithms for more security.

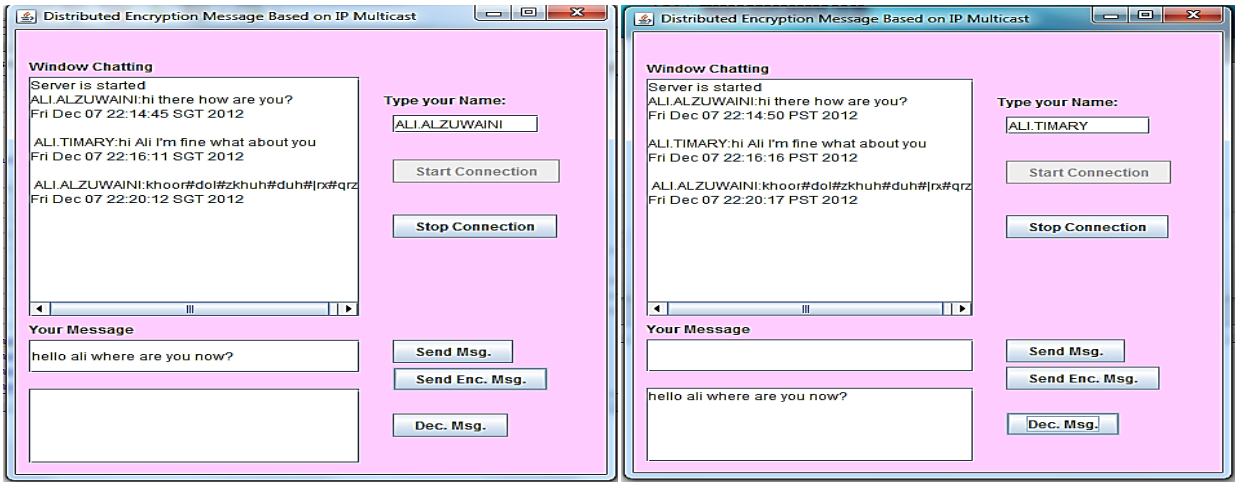

Figure 15. Send and Receive Encrypted Message

References

[1]. *W. Liao and M.-Y. Jiang. Family ack tree (fat): Supporting reliable multicast in mobile ad hoc networks. IEEE Transactions on Vehicular Technology, Vol 52.No6,1675–1685, Nov 2003.*

[2]. *S. Wu and C. Bonnet. Multicast routing protocol with dynamic core (mrdc). In International Symposium on Telecommunications (IST01), Tehran, Iran, Aug 2001.*

[3]. *D. Xu, B. Li, and K. Nahrstedt. Qos-directed error control of video multicast in wireless networks. In 8th IEEE International Conference on Computer Communications and Networks (IEEE ICCCN '99), pages 257–262, Boston-Natick, MA,Oct 1999.*

[4]. *E. Pagani and G. Rossi. Reliable broadcast in mobile multihop packet networks. In MOBIHOC'97, 1997.*

[5]. *K. Almeroth, K. Obraczka, and D. Lucia. A lightweight protocol for interconnecting heterogeneous devices in dynamic environments.In IEEE ICMCS'99, 1999.*

[6]. *R. Chandra, V. Ramasubramanian, and K. Birman. Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks. In The 21st International Conference on Distributed Computing Systems (ICDCS), Phoenix, Arizona, 2001.*

[7]. *C.-C. Chiang and M. Gerla.Routing and multicast in multihop, mobile wireless networks.In IEEE ICUPC'97, 1997.*

[8]. Hoda A. Abdel Hafez, " Big Data in Smart Cites: Analysis and Applications in Arab World",Egyptian Computer Science Journal, Volume 41, Issue 1, January 2017.

[9]. *W.Wu and Y. C. Tay. Amris: A multicast protocol for ad hoc wireless networks. In Military Communications Conference (AIILCOM 1999), pages 25–29, 1999.*

[10]. *M. Gerla, C.-C. Chiang, and L. Zhang. Tree multicast strategies in mobile, multihop wireless networks. ACM/Baltzer Journal of Mobile Networks and Applications (MONET), 1999.*

[11].*Sajama and Z. J. Haas.Independent-tree ad hoc multicast routing (itamar). Mobile Networks and Applications, vol8, No5:551–566, 2003.*

[12]. *P.-J. Wan, G. Calinescu, X.-Y.Li, and O. Frieder. Minimum-energy broadcasting in static ad hoc wireless networks. Wireless Networks,vol8, No6:607 – 617, Nov 2002.*

[13].*J. Wieselthier, G. Nguyen, and A. Ephremides. Energy-limited wireless networking with directional antennas: The case of session-based multicasting. In INFOCOM' 02, New York, NY USA, 2002.*

[14].*S. Guo and O. Yang. Antenna orientation optimization for minimum-energy multicast tree construction in wireless ad hoc networks with directional antennas. In the 5th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc04), Roppongi Hills, Tokyo, Japan, 2004.*
[15].*S. Guo and O. Yang. Minimum energy multicast routing for wireless ad-hoc networks with adaptive antennas. In ICNP 2004, Berlin, Germany, 2004.*
[16]. *K. Wang, C. F. Chiasserini, R. R. Rao, and J. Proakis. Rise: Reducing interference and saving energy through multicasting in ad hoc wireless networks. In IEEE*
MILCOM 2002, Anaheim, CA, USA, 2002.
[17].*C. Hu, Y. Hong, and J. Hou. On mitigating the broadcast storm problem with directional antenna.In ICC'03, 2003.*
[18]. *A.K. Das, R.J. Marks II, M.A. El-Sharkawi, P. Arabshahi, and A. Gray. Maximization of time-to-first-failure for multicast applications in wireless networks: optimal solution using milp. In IEEE Milcom, Monterey Conference Center, Monterey, CA,Oct 2004.*
[19].*C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol (fgmp) for multihop, mobile wireless networks. Cluster Computing: Special Issue on Mobile Computing,vol1.1, No2:187–196, 1998.*
[20].*R. Vaishampayan and J.J. Garcia-Luna-Aceves. Efficient and robust multicast routing in mobile ad hoc networks.In 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Fort Lauderdale, Florida, 2004.*
[21].*J.J. Garcia-Luna-Aceves and E.L. Madruga.A multicast routing protocol for ad-hoc networks. In IEEE INFOCOM '99, New York, New York,, 1999.*
[22].*S. Park and D. Park. Adaptive core multicast routing protocol. Wireless Networks, vol10. No1:53–60, Jan 2004.*
[23].*S. Singh, C. S. Raghavendra, and J. Stepanek. Power efficient broadcasting in mobile ad hoc networks. In PIMRC'99, 1999.*
[24].*H. Zhou and S. Singh. Content-based multicast for mobile ad hoc networks.In Proc. Mobihoc 2000, August 2000.*
[25].*J. Kuri and S. Kasera. Reliable multicast in multiaccess wireless lans. Wireless Networks, pages 359–369,, Jul 2001.*
[26].*M. Nagy and S. Singh. Multicast scheduling algorithms in mobile networks.Cluster Computing, 1998.*
[27].*S. K. S. Gupta, V. Shankar, and S. Lalwani. Reliable multicast mac protocol for wireless lans. In IEEE International Conference on Communications (ICC'03),volume 1, pages 93–97, 2003.*
[28].*L. Tassiulas and A. Ephremides. Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. IEEE Transactions on Automatic Control, vol 37, No12:1936–1948, Dec 1992.*
[29]. *L. Tassiulas and A. Ephremides. Dynamic server allocation to parallel queues with randomly varying connectivity. IEEE Trans. Info. Theory, vol30, No2:466–478, Mar 1993.*
[30]. *C. Diot, B. N. Levine, B. Lyles, H. Kassem, and D. Balensiefen, Deployment issues for the IP multicas service and architecture. IEEE Network, vol14, No1:78–88, 2000.*
[31].*R. R. Brooks, BrijeshPillai, Matthew Pirretti ,And Michele C. Weigle, Multicast Encryption Infrastructure For Security In Sensor Networks,2009.*