Build Encrypted Chat System by using multicast technique with determine delay time

Atheer Y. Oudah
Wessam A. hamed
Hyder Y. Atwan
ThiQar University, Collage of Education for pure Sciences, Computer Department

Abstract

Multicast communications and as expected it is an effective way to send information to the largest possible number of receivers. IP multicast has several technical problems to be resolved until it is widely deployed in the Internet. These includes service model of multicast group, reliable transport, security and congestion control. In this paper, we describes the benefits of multicasting and how it can works in local area Network that connected via any server, the Class D addressing from 244.0.0.0 to 239.255.255.255 reserved for internet multicast communication to make connection between many host in the network. A prototype Multicast Chat System (MCS) has been developed to test the capability and suitability of multicasting. The prototype was developed using the Java language. The benefit for this prototype is multi diverse users can be connected without necessary needs for an Internet or Web-server, and thispaper describes the overall work for IP multicast for advantage and disadvantage based on chatting process and simple security algorithm.

Keywords: Multicast, IP Multicast, Encryption, JAVA, Delay Time.

انشاء نظام محادثه مشفر بأستخدام تقنية الارسال المتعدد مع تحديد وقت التاخير

اثير يوسف عودة
وسام عباس حمد
حيدر يحيى عطوان
جامعة ذي قار, كلية التربية للعلوم الصرفة, قسم علوم الحاسبات

الملخص:

الإرسال المتعدد هو وسيلة فعالةلإرسال المعلومات والبيانات إلى أكبر عدد ممكن من المتلقين.في هذا البحث سوف نصف فوائد الإرسال المتعدد وكيف يمكن أن يعمل في شبكة محلية دون الحاجة الى الاتصال بالانترنت .وقد تم تطوير نظام لاجراء دردشة عن طريق الارسال المتعدد (MCS) باستخدام لغة جافا .وهذا البحث يصف العمل الشامل للإرسال المتعدد عن طريق نظام دردشة مدعوم بخوارزمية تشفير بسيطة ومعرفة وقت التأخير الحاصل بين المستخدمين.

1- Introduction

There are three main types of IPv4 addresses: Unicast, broadcast, and multicast. Unicast it designed to transfer a packet between two hosts (node) in the network. A broadcast is used to send packet to sub network domain. Multicastis located between unicast and broadcast. Rather than sending data to a single host (unicast) or all hosts in a network (broadcast), multicasting delivers data only to all intended recipients. A

multicast address is designed to enable delivery of packet to the set of hosts that have been configured as group address from 244.0.0.0 to 239.255.255.255 in various subnetworks. The main disadvantages of multicast are not connection oriented. A multicast is delivered to destination group member with the same "best-effort" reliability as a slandered unicast IP [1]. The main difference between a multicast IP packet and a unicast IPpacket is the presence of a "group address" in the destination address field of the IP header.

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 physical location or how many numbers of members in a multicast group [2]. The main device in 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.For example when the host jointhe multicast group, it transmits a group membership protocol message for all groups in themulticast by join sockets group that needs to receive the packet from this host. This way hasmain advantages in Multicast capability but the maximum host in sometimes not exceed 30 hostsbut for each subnet group [3].

This research shows such IP multicasting of how create and use it in many applications. This research 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 internet by sending secure messages from one client to many recipients. Furthermore, it shows the time between many recipients for sending and receiving messages based one simple security algorithms for more security.

1-1 Advantageous of Multicast

- A multicast packet has class D multicast addresses, but it sends to a group IP hosts in one packet that will be delivered to group of receivers.
- Multicast address saves the bandwidth by sending packet to multiple hosts in the network which will receive the same multicast stream instead of individual one.
- Dynamically join a host to a group by Internet Group management Protocol (IMGP).
- The stream of data can be delivered to each multicast host of it already select before (join the group by IGMP).
- Multicast application uses in many applications such as:
    - Video conferences.
    - Live broadcasting.
    - Web TV, web radio.
    - Video-on-demand.
    - E-learning.
    - Whiteboard data change.

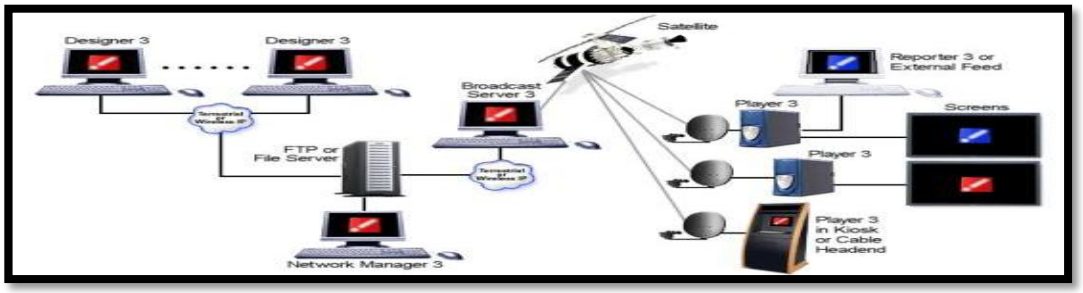

Figure 1. Usage multicast.

1-2 Disadvantages of Multicast

- Multicast protocol is not windowed flow control.
- UDP is not reliable.
- Multicasting IP is widely used in WLAN but not with interconnected WLAN's with maximum 30 host [3].
- There is no congestion avoidance mechanism.

2- IP multicast

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of recipients [4]. IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by routers enabled with multicast routing protocols, resulting in the most efficient delivery of data to multiple receivers possible.To support multicasting, ahost group should be created first and the host group must be identified by a single IP destinationaddress. The membership of a host group is dynamic, that is, hosts may join and leave groups atany time. Figure 2 illustrates the basic components of IP multicast and demonstrates how data from one sender are delivered to several interested receivers using IP Multicast [5].Therefore, IP multicasting relies on two types of protocols: multicast routing protocols to route packets efficiently to the group members and a group management protocol to establish and maintain multicast host groups.

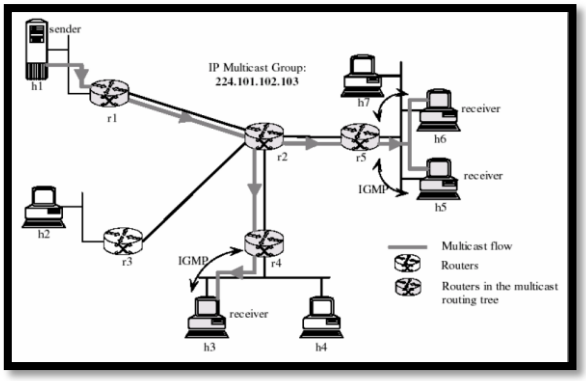

Figure 2.Block diagram shows the contents of IP multicast.

When a simulation to transmit a piece of data onto the network, it must decide what multicast group to put the data on [6]. It has basically three pieces of information that it can use to make this decision:

1. The source of the data (i.e. the place the data is coming from: either site or host or process or unit or entity). This is called source-based multicast.
2. The data contents itself (i.e. what geographic location the data fits into, or what side the producing entity is on, or what markings it has, or what entity type it is, or what acceleration it has, etc.). Any multicast scheme where the multicast group is based on the data contents fits into this category. This is called data-based multicast.
3. The destination of the data. In destination-based multicast, the data is sent onto a multicast group solely based on those hosts that are to receive that information.

3- Related Works

Multicast is an efficient communication mechanism where a source host sends the same message to a group of destination hosts denoted in the join group, Conserves network bandwidth by sending a single message along any link in the path from source to destinations. Most of the work for multicasting message in networks is focused on the network and transport layers. At the transport layer, the aim is to ensure reliable delivery of a message to all the receivers. A performance metric for these protocols is overhead communication due to packet and signaling retransmissions required to ensure reliable packet delivery. [7,8] have proposed to facilitate the loss recovery through intermediate nodes in order to avoid latency and messaging overhead. Paganiet. al. have adopted an approach that adaptively chooses flooding and recovery along routing tree based on the mobility [9].

At network layer, the aim is to design a multicast routing protocol. The multicast routing protocols can be broadly divided into two categories, namely, mesh based and tree based .The tree based routing solutions are inspired by the protocols designed for wire line networks, but have the additional capability of handling frequent topology changes. Chiang et. al. have proposed a Core based Tree (CBT) based routing protocol [10]. Here, the authors propose to divide the network in clusters and then employ hierarchical routing. In hierarchical routing, CBT is formed on a sub graph consisting of cluster-heads and gateways. Cluster-heads are responsible for routing a packet to the multicast receivers in their cluster. Chiang et. al. have also proposed an adaptive shared tree multicast routing protocol [11]. This approach adaptively chooses shared tree or source tree based on the proximity of the receiver to the source. Further, it uses two level mobility model to improve the stability of the shared tree. Wu et. al. have proposed a routing protocol that assigns sequence numbers to each node and uses them to rapidly adopt with changes in group membership and topology [12]. Gerlaet. al. have surveyed the tree based routing protocols for multi-hop wireless networks in [13].

4- Proposed Approach

We have suggested an approach to enhance security to message that sending to many hosts to protect sending message from intercept by using encryption algorithm, so that only receiver who has permission can see the original message by using decryption key to break the encrypted message. Application developed and designed by using java language, because it suitable to build this project's type and Using Java tools help to achieve flexibility for the application. The proposed approach consist of three parts , as shown in figure 3.

4-1Tentative design.

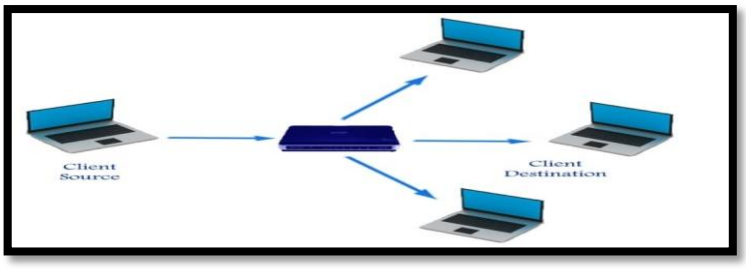

Figure 3. Show tentative design to send information between two clients (Source, Destination).

We evaluate this work by using WLAN ,so we make test for our work at WLAN network that connected with router to the internet. The first step, we send unsecure message to all clients to see the content of this message directly ,and repeat sending with 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

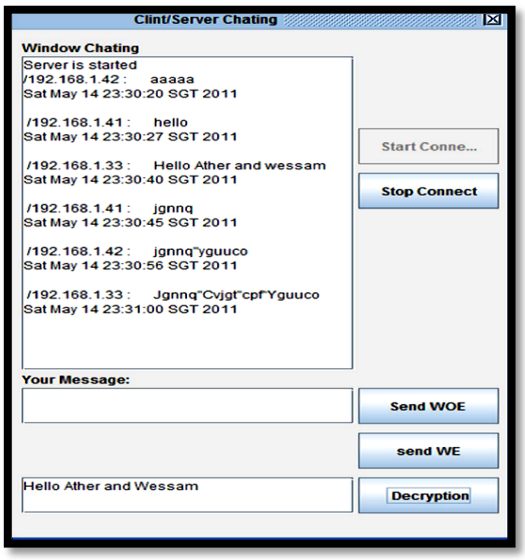

Figure 4. Send the Encrypted Message Based on Send WE command.

4-2 Proposed algorithm.

In this system we suggest an encryption algorithm for security message that sending to many hosts to protect sending process from intercept . the following piece of code explain the proposed encryption process:

```
        int i, intc; char c='a';
    char cc;
        i = 0;
        String ss="";
        // to encryption
        while (i <str.length()){
                c = str.charAt(i);
                //System.out.print(str.charAt          (i) ) ;
                intc = (int) c;
                cc = (char) (intc + 2);
                System.out.print( cc );
                ss=ss+cc;
                i++; }
        returnss;
```

4-3 Delay time.

In this system we have added one of the features that required in multicast. By adding the time of the message sent from the sender to the receiver, therefore, we will be able to know the delay time between the sender and receiver.Sample code below:

```
// This Class return the time of delivered picket on Second/ Day/ Month and year
        longcurrentTimeInMillis = System.currentTimeMillis();
```

```
        Date today = newDate(currentTimeInMillis );
    Calendar cal = Calendar.getInstance();
today = cal.getTime();
        // System.out.println( today );
        return today;
```

5- Conclusion

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 project shows such IP multicasting of how create and use it in many application. This project 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 internet 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.

References

[1]: 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.

[2]: Sajama and Z. J. Haas. Independent-tree ad hoc multicast routing (itamar).Mobile Networks and Applications, 8(5):551–566, 2003.

[3]:E. Ali, T. El-fouly and A. Bader. MESP: A Modified IPSec for secure multicastcommunication. In IEEE International Conference on ITS Telecommunications Proceedings,volume 6, pages 812–816, 2006.

[4]: S. Park and D. Park. Adaptive core multicast routing protocol.Wireless Networks, 10(1):53–60, Jan 2004.

[5]: 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.

[6]:S. Kulkarni and C. Rosenberg. Opprotunistic scheduling in wireless systems with multiple interfaces and multiple constraints. In 6th ACM Intl. Workshop on Modeling, Analysis and Simulations ofWireless and Mobile Systems (MSWim), San Diego, CA, Sep 2003.

[7]: W. Liao and M.-Y. Jiang. Family ack tree (fat): Supporting reliable multicast in mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 52(6):1675–1685, Nov 2003.

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

[9]: E. Pagani and G. Rossi. Reliable broadcast in mobile multihop packet networks. In MOBIHOC'97, pages 34–42, 1997.

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

[11]: C.-C. Chiang, M. Gerla, and L. Zhang. Adaptive shared tree multicast in mobile wireless networks. In IEEE GLOBECOM'98, 1998.

[12]: C.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.

[13]: 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.