INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SIMPLE PACKET TRANSMISSION SCHEME FOR WIRELESS DATA OVER ROUTING PROTOCOLS – A SURVEY

M.Mayilvaganan[1], S.Dhivya[2]
[1] *Associate Professor, Dept of CS, PSG College of Arts and Science, Coimbatore, India,*
mayil24_02@yahoo.co.in
[2] *Research scholar, Dept of CS, PSG College of Arts and Science, Coimbatore, India,*
dhivya.selvaraj69@gmail.com

Abstract

Data in networks is transmitted in packets, which are sequences of octets. In some reason it is cheaper to deal with failure or altered form of small packets than with long full messages; easier to share communication channels between synchronized communicating entities since there are no long messages for whose transmission all have to wait. In this paper, we proposed packets are transmitted from one node to another node with different packet size; time may be varied from packet range. Sometimes the packets might be fatalities due to high rate of recurrence. With high rate of recurrence nodes, packets can improve network scalability, connectivity, and broadcasting robustness. We premeditated this with recent proposed protocols.

Keywords*:* Packet Transmission, Communication, Packet Size, Protocols

1. Introduction

Computer networking is one of the most existing and important technology. Computer networks can be seen as the collection of interconnected and all together independent. Computer systems mainly for the purpose of allocation computer resources and communication. The recrudescence of computer networks and its attendant unprecedented advantages led to its increasing use in today's communication system. It offers reliable data, voice, and video communication, which is the prime expectation of its users at both ends of the network. Computer networks can span local areas such as buildings to form Local Area Networks (LAN) or wide areas such as countries forming Wide Area Networks (WAN).

The Internet is the most popular type of computer network because it gives reliable and efficient transfer of information – data, voice, and video. The quest for reliable data transfer necessitated the concept of routing, which is the process of finding a path from the source to a destination system in the network. It allows users in the furthest part of the world to get to information and services provided by computers wherever in the world.

Routing makes networking and internetworking at large supernatural. It allows voice, video and data from different location in the world to be sent to multiple receivers around the world. The concept of routing addresses such intricacies like selection of paths that span the world, adaptation of routing system to failed links, path selection criteria such as least delay, or least cost or most available capacity links. However, the performance of routing depends on the routing algorithms adopted. Routing is accomplished by means of routing protocols that establish mutually consistent routing tables in every router or switch controller in the network.

Routers build routing tables that contain collected information on all the best paths to all the destinations that they know how to reach. A routing table contains at least two columns: the first is the address of a destination endpoint or a destination network, and the second is the address of the network element that is the next hop in the “best” path to this destination. When a packet arrives at a router, the router consults the routing table to decide the next hop for the packet.

A packet is a basic unit of communication over a digital network. A packet is also called a datagram, a segment, a block, a cell or a frame, depending on the protocol. When data has to be transmitted, it is broken down into similar structures of data, which are reassembled to the original data chunk once they reach their destination.Transmission of standardized packets of data over transmission lines rapidly by networks of high speed switching Computers that have themessage packets stored in fast access core memory.

Packet transmission charge are exciting on the basis of the quantity of data packets transmitted (one packet = 128 bytes). Therefore, as in the case of accessing a website with images, transmitting/receiving E-mail with an attached file, and downloading data, the larger the volume of data transmitted is, the more expensive the transmission charges become. If the transmission charges become excessively expensive, there may be some cases in which the line will be temporarily suspended. Even when data is not received properly due to reception conditions or content of data, packet transmission charges may still be charged. Because packets are transmitted on a "best effort" basis, transmission rates fluctuate depending on the congestion level of the line used.

2. Communication

2.1 Packet Delivery Time

The packet delivery time or latency is the time from the first bit leaves the transmitter until the last is received. In the case of a physical link, it can be expressed as:

Packet delivery time = Transmission time + Propagation delay

In case of a network connection mediated by several physical links and forwarding nodes, the network delivery time depends on the sum of the delivery times of each link, and also on the packet queuing time (which is varying and depends on the traffic load from other connections) and the processing delay of the forwarding nodes. In wide-area networks, the delivery time is in the order of milliseconds.

2.2 Roundtrip Time

The round-trip time or ping time is the time from the start of the transmission from the sending node until a response (for example an ACK packet or ping ICMP response) is received at the same computer. It is affected by packet delivery time as well as the data processing delay, which depends on the load on the responding node. If the sent data packet as well as the response packet have the same length, the roundtrip time can be expressed as:

Roundtrip time = 2 * Packet delivery time + processing delay

In case of only one physical link, the above expression corresponds to:

Link roundtrip time = 2 * packet transmission time + 2 * propagation delay + processing delay

If the response packet is very short, the link roundtrip time can be expressed as close to:

Link roundtrip time ≈ packet transmission time + 2 * propagation delay + processing delay

2.3 Throughput:

The network throughput of a connection with flow control, for example a TCP connection, with a certain window size (buffer size), can be expressed as:

Network throughput ≈ Window size / roundtrip time

In case of only one physical link between the sending and transmitting nodes, this corresponds to:

Link throughput ≈ Bitrate * Transmission time / roundtrip time

The *message delivery time* or *latency* over a network depends on the message size in bit, and the network throughput or effective data rate in bit/s, as:

Message delivery time = Message size / Network throughput

2.4 Transmission Delay

In a network based on packet switching, transmission delay (or store-and-forward delay, also known as packetization delay) is the amount of time required to push all of the packet's bits into the wire. In other words, this is the delay caused by the data-rate of the link.

Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits,

It is given by the following formula:

$$D_T = N/R \text{ Seconds}$$

Where

D_T is the transmission delay in seconds
N is the number of bits, and
R is the rate of transmission (say in bits per second)

Most packet switched networks use store-and-forward transmission at the input of the link. A switch using store-and-forward transmission will receive (save) the entire packet to the buffer and check it for CRC errors or other problems before sending the first bit of the packet into the outbound link. Thus store-and-forward packet switches introduce a store-and-forward delay at the input to each link along the packet's route.

2.4.1 Packet transfer delay

Packet transfer delay is a concept in packet switching technology. The sum of store-and-forward delay that a packet experiences in each router gives the transfer or queuing delay of that packet across the network. Packet transfer delay is influenced by the level of network congestion and the number of routers along the way of transmission.

- There are four sources of packet transfer delay:
  1. Nodal processing:
     1. Check bit errors
     2. Determine output link
  2. Queuing:
     1. Time waiting at output link for transmission
     2. Depends on congestion level of router
  3. Transmission delay:
     1. R=Link bandwidth (bit/s)
     2. L=Packet length (bits)
     3. Time to send bits into link = L/R

2.5 To calculate packet transmission time and delay in networks

2.5.1 Transmission Time

The **transmission time**, is the amount of time from the beginning until the end of a message transmission**.** The packet transmission time in seconds can be obtained from the *packet size* in bit and the bit rate in bits

Packet transmission time = Packet size / Bit rate

2.5.2 Propagation Delay

The transmission time should not be confused with the propagation delay, which is the time it takes for the first bit to travel from the sender to the receiver (During this time the receiver is unaware that a message is being transmitted). The propagation speed depends on the physical medium of the link (that is, fibre optics, twisted-pair copper wire, etc.) and is in the range of $2 * 10^8$ meters/sec for copper wires and $3 * 10^8$ for wireless communication, which is equal to the speed of light. The propagation delay of a physical link can be calculated by dividing the distance (the length of the medium) in meter by its propagation speed in m/s.

Propagation time = Distance / propagation speed

3. Network packet Terminology

A network packet is a formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users than if the network were circuit switched. A packet consists of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

In the seven-layer OSI model of computer networking, packet strictly refers to a data unit at layer 3, the Network Layer. The correct term for a data unit at Layer 2, the Data Link Layer, is a frame, and at Layer 4, the Transport Layer, the correct term is a segment or datagram. For the case of TCP/IP communication over Ethernet, a TCP segment is carried in one or more IP packets, which are each carried in one or more Ethernet frames.

3.1 Packet framing

Different communications protocols use different conventions for distinguishing between the elements and for formatting the data. For example in Point-to-Point Protocol, the packet is formatted in 8-bit bytes, and special characters are used to delimit the different elements. Other protocols like Ethernet, establish the start of the header and data elements by their location relative to the start of the packet. Some protocols format the information at a bit level instead of a byte level. A good analogy is to consider a packet to be like a letter: the header is like the envelope, and the data area is whatever the person puts inside the envelope.[1] A network design can achieve two major results by using packets: error detection and multiple host addressing. A packet has the following components.

3.2 Network address

Modern networks usually connect three or more host computers together; in such cases the packet header generally contains addressing information so that the packet is received by the correct host computer. Typically, two addresses are included, the destination address, which is where the packet is intended to go, and the transmitter's address which is necessary if there is to be a reply sent. In addition, other fields may be present, to identify the particular applications that are running on the network host that are sending and waiting for packets.

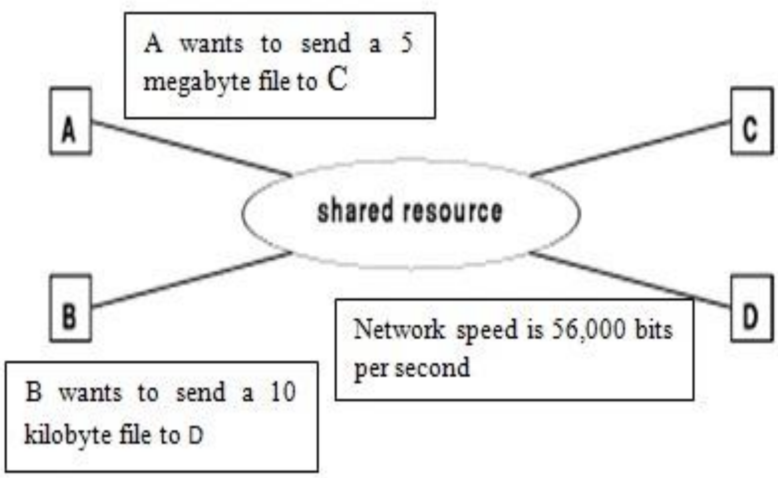

Figure 1: Packet transfer through networks

3.3 Error detection and correction

Network packets often contain a checksum, parity bits or cyclic redundancy checks to check for errors that occur during transmission. At the transmitter, the calculation is performed before the packet is sent. When received at the destination, the checksum is recalculated, and compared with the one in the packet. If discrepancies are found, the packet may be corrected or discarded. Any packet loss is dealt with by the network protocol. In some cases routine modifications of the network packet can occur while routing. In that case recalculation may be required.

3.4 Hop counts

Under fault conditions packets can end up traversing a closed circuit. If nothing was done, eventually the number of packets circulating would build up until the network was congested to the point of failure. A time to live is a field that is decreased by one each time a packet goes through a network node. If the field reaches zero, routing has failed, and the packet is discarded. Ethernet packets have no time-to-live field and so are subject to broadcast radiation in the presence of a switch loop.

3.5 Packet length

There may be a field to identify the overall packet length. In some protocols, the length is implied by the duration of transmission.

3.6 Class/priority

Some networks implement quality of service which can prioritise some types of packets above others. This field indicates which packet queue should be used; a high priority queue is emptied more quickly than lower priority queues at points in the network where congestion is occurring.

3.7 Payload

In general, payload is the data that is carried on behalf of an application. It is usually of variable length, up to a maximum that is set by the network protocol and sometimes the equipment on the route. Some networks can break a larger packet into smaller packets when necessary.

4. Conclusion

In these paper, we deliberate a few protocol used to implement for packet transmission. Some of the protocols for transfer packet from one node to another node require elevated rate of recurrence.

REFERENCES

1. Andrew s. Tanenbaum, computer networks,5th edition
2. http://www.cis.temple.edu/~giorgio/cis307/readings/packettrans.
3. F. Adler, "Minimum energy cost of an observation," IRE Trans. Inform. Theory, vol. IT-2, pp. 28–32, 1955.
4. N. Bambos, "Toward power-sensitive network architectures in wireless communications," IEEE Personal Commun., vol. 5, pp. 50–59, June 1998.
5. N. Bambos and S. Kandukuri, "Power control multiple access (PCMA)," Wireless Networks, 1999.
6. N. Bambos and G. Pottie, "Power control based admission policies in cellular radio networks," in GLOBECOM '92.
7. D. Rajan, A. Sabharwal, and B. Aazhang, "Delay and Rate Constrained Transmission Policies over Wireless Channels," Proc. Globecom 2001, San Antonio, November 2001
8. W. Fleming and H. Soner, Controlled Markov Processes and Viscosity Solutions, Springer-Verlag, 1993.
9. M. Davis, Markov Models and Optimization, Chapman and Hall, 1993.
10. B. Oksendal, Stochastic Differential Equations, Springer, 5th edn., 2000