

Data Communications
Prof. A. Pal
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 22
Congestion Control

Hello and welcome to today's lecture on congestion control in packet switched network. In the last two lectures we have discussed about the routing techniques used in packet switched network. So, after routing another very important aspect that has to be considered is the congestion in the packet switched network. Here is the outline of today's talk.

(Refer Slide Time: 1:46)

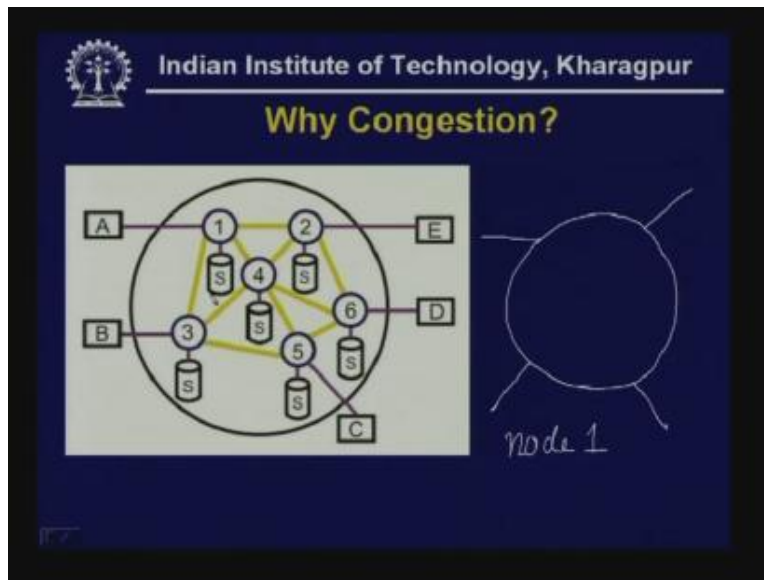


First we shall discuss about why congestion rather why congestion arises at all then the common causes of congestion or in other words the sources of congestion and we will also discuss about what are the effects of congestion on the packet switched network whenever congestion takes place. Then we shall discuss about two basic approaches for controlling congestion. One is open loop technique and another is close loop technique.

Under the open congestion control technique we have two important algorithms; one is known as the Leaky Bucket Algorithm and another is the Token Bucket Algorithm. We shall discuss a number of close loop congestion control techniques such as admission control, weighted fair queuing related to admission control, resource reservation which is known as the RSVB then the use of choke packet, load shedding and so on. Finally we shall close our discussion by considering a comparison between congestion and flow control.

On completion of this lecture the students will be able to explain the causes for congestion, understand the effects of congestion, what happens when congestion take place, understand various open loop and close loop congestion control techniques such as Leaky Bucket Algorithm, Token Bucket Algorithm and so on then they will be able to distinguish between flow and congestion control. So with this background let us start our discussion about why congestion.

(Refer Slide Time: 3:24)



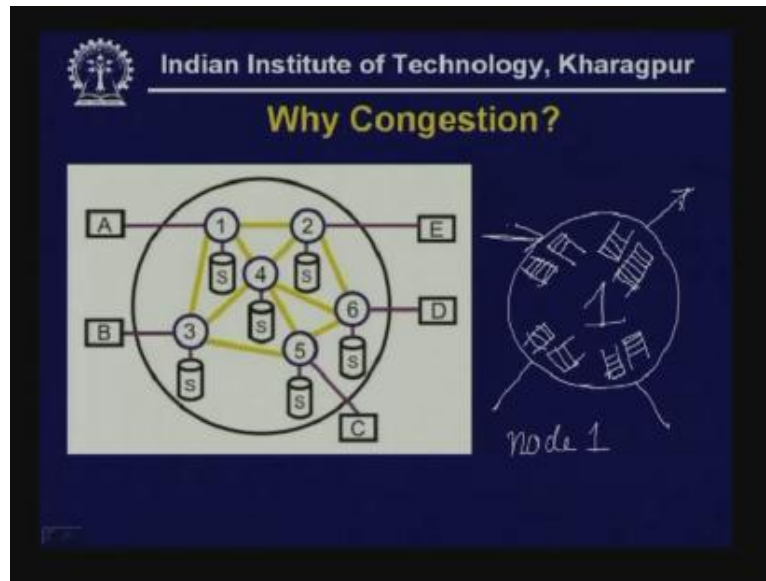
So here is schematic diagram of a packet switched network. Let us have a closer look of a particular node. So here I have considered a bigger view of a particular node. Let us consider the node 1, this is the node 1. As we can see node 1 has got 1 2 3 4 so four links coming from either the host or the station or connected to some other nodes so it has got four nodes. And also it has some storage, so how this storage is used? This storage is used to maintain queues, it can be considered as input queue and also output queue which stores the packets which are used as packet buffer. So queue of packets are present on each node as shown here (Refer Slide Time: 4:28) where the packets are buffered before they can be transmitted through the links, and it has got four links so here is node number 1.

Now let us assume it has got certain number of packets in the queues in this particular node. What happens in normal situation? In normal situation a packet which is introduced into the network gets delivered to the destination if the network is not heavily loaded. That means all the packets which are entered from this station say from station A into the network may be temporally stored in this buffer then it is sent to a proper output link through some buffer and then it is transmitted towards the destination.

In the last two lectures we have discussed about the routing techniques and also discussed about how it is sent towards the destination, that is the normal situation but what happens when the traffic increases suddenly. We know that the data communication network is

bursty in nature. As a consequence what can happen is suddenly the load can increase within a short period of time. What happens in such a situation? In such a situation one situation is that the buffer may get filled up and whenever there is no more storage available here the packet gets discarded. That means the buffer becomes full there is no empty space in the storage then the packet is discarded that is one possibility.

(Refer Slide Time: 6:50)



Another possibility is that whenever there is a big queue at the output nodes suppose it is going in this direction then what can happen is the particular packet takes very long very time to reach the front of the queue that means before transmission it spends a long time in the buffer and as a consequence delay increase significantly and whenever delay increases significantly the source node after waiting for sometime does not get an acknowledgment and as a consequence it retransmits the same packets which also in turn increases the load of the network. These two things happen and as a result whenever the packets do not get delivered the delay increases to a large extent resulting in congestion. So congestion arises because of heavy load in the network and for various other reasons also.

Once again to summarize what we can say is, as packets arrive at a node they are stored in an input buffer if packets arrive too fast because of bursty nature and incoming packet may find that there is no available buffer space that is one possibility of a packet getting discarded.

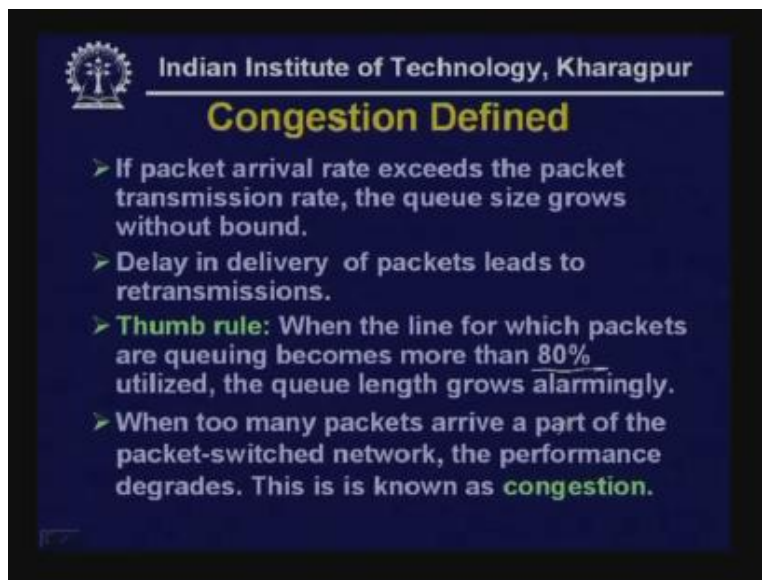
Another possibility is that even very large buffer cannot prevent congestion because of delay, timeout and retransmissions. As I have mentioned one can argue that since the buffer space is insufficient why not you increase the buffer space. But increasing the buffer size will increase the size of the queue and the packet which is at the end of the queue will take the long time to reach the front of the queue before it gets transmitted and this will lead to timeout, lead to retransmissions which will increase the traffic in the

network and which in other words contribute towards congestion. Then the slow processors may also be responsible for congestion.

The slow processors may take very long time although the link may be of high speed but the slow processors may take very long time to process a packet so it has to do the buffer management, it has to do some housekeeping and for all these things the processors will take sometime. If the processor is slow that may take quite sometime to do this processing. As a result that may delay a packet leading to congestion.

Then the low bandwidth line may also lead to congestion. As we know the network may have links of various data rates or line capacity and as a consequence if the bandwidth of a particular link is small even that can lead to the increase in congestion because the buffer size will increase and the packet may not be delivered. These are some of the common causes for congestions. And as we discuss we shall see how the effect of these causes can be minimized. Now we can define congestion. Now we are in a position to define congestion.

(Refer Slide Time: 10:25)



Indian Institute of Technology, Kharagpur

Congestion Defined

- If packet arrival rate exceeds the packet transmission rate, the queue size grows without bound.
- Delay in delivery of packets leads to retransmissions.
- **Thumb rule:** When the line for which packets are queuing becomes more than 80% utilized, the queue length grows alarmingly.
- When too many packets arrive a part of the packet-switched network, the performance degrades. This is known as **congestion**.

If packet arrival rate exceeds the packets transmission rate the queue size grows without bound.

Delay in delivery of packets leads to retransmissions.

Whenever these two things happen the thumb rule says: When the line for which the packets are queuing becomes more than 80% that means its original capacity may be 100% but whenever it becomes more that 80% utilized the queue length grows alarmingly. That means if the utilization of a link increases more than 80% that means the network has become overloaded and we can say that the network is in congestion. There

will be a port and when too many packets arrive at the port the performance degrades in the packet switched network, this is known as congestion.

So we can say that, because of overload the delay increases and the network is not able to handle the packet it has received and as result the packets do not get delivered to their destination. This is called congestion. Now let us see what is the effect of it.

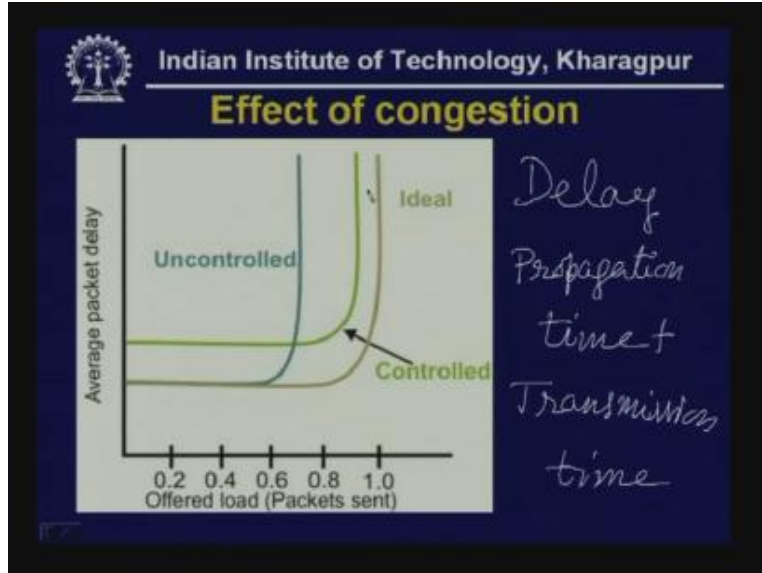
As you can see this greenish curve corresponds to uncontrolled that means no controlled measure has been taken for overcoming congestion. In such a situation initially as the offered load or the number of packets introduced in the network increases all the packets gets delivered that means the throughput follows linearly. That means if it is 0.2% of the total capacity then here also it is 0.2% so it rises linearly. But as you can see when it crosses 0.6 to 0.8 mark there is delay and that delay leads to retransmission and as a result the throughput decreases and the rate of increase decreases initially then the throughput suddenly drops although the offered load increases and at certain point it becomes 0 which is known as thrashing situation.

In thrashing situation although the stations introduce the packets in the network but not a single one is delivered because of long delay and retransmission and various other problems and that situation is known as thrashing. Thrashing occurs when the throughput becomes 0. Now ideally it should follow this curve (Refer Slide Time: 12:45) if there is no congestion but because of congestion it behaves in this manner. And by taking suitable congestion control approaches the congestion can be controlled. In such a situation the behavior of the network will be somewhat like this.

As you can see the throughput is less than the ideal curve. That means there is some overhead for implementing congestion control and because of that overhead the throughput is less because there are some overhead packets which are also transmitted resulting in a decrease in throughput but it will not drop like the congested network. As a result although the throughput is less it will never reach the thrashing situation. This is the effect of congestion on throughput both in controlled and uncontrolled situations as discussed.

Now let us see the other parameter known as delay. Delay is a very important parameter and as you can see in the ideal situation as long as the offered load is within the capacity of the network the delay is very small which is decided only by the propagation time.

(Refer Slide Time: 14:18)

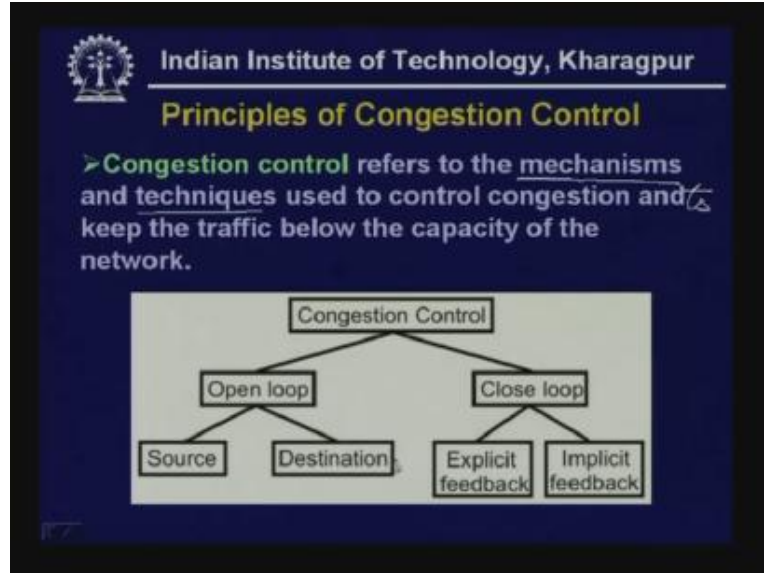


Propagation time and the transmission time of the packet is the only delay and there is no other delay in the network. However, suddenly whenever congestion occurs whenever we know that traffic is more than the capacity of the network then the delay will increase because they will be buffered around 0.8% or so.

Now, in the uncontrolled case as you can see delay can be very high compared to the ideal situation so you see that the delay is very high in the uncontrolled network. On the other hand, by using control although the over all delay increases ultimately it can sustain very high offered load compared to the uncontrolled situation. So we see that how the delay parameter is affected in all the three conditions ideal, uncontrolled case and whenever congestion control measures are taken. This curve shows how delay is affected.

Therefore we have seen two important effects of congestion, one on throughput and another on delay. Now let us see what are the techniques we can use to control congestion.

(Refer Slide Time: 15:49)



The basic principle of congestion control refers to the mechanisms and techniques used to control congestion and to keep the traffic below the capacity of the network. That is the basic objective of the congestion control. So, basic objective is to keep the traffic within certain limit such that congestion does not work or whenever congestion works we have to overcome that. That is why congestion control technique basically can be categorized into two types; one is open loop congestion control and another is close loop congestion control.

You may be familiar with control **theory**; this can be explained in terms of control theory. There are two basic techniques; one is open loop control and another is close loop control.

The open loop congestion control can be further divided into two types; one is based on source and another is based on destination. That means who does the control, it can be done by the source that means source will try to control the congestion by introducing traffic in a controlled manner or it can be implemented at the destination, the destination will take suitable measure it will inform the source such that the traffic is reduced. So who controls is further decided by the two different types under open loop congestion control technique.

Then under the category of close loop we have got two different types. As we know in close loop case there is some kind of feedback. That means when the network is monitored it checks whether control has taken place or not which is not done in case of open loop. in open loop case there is some feedback from the system. There is some way of checking the status of the network as whether it is congested or how much congested it is and so on. Therefore in such a situation there can be two different mechanisms; one is explicit feedback, another is implicit feedback.

In case of explicit feedback some of the nodes usually switches or nodes they will detect congestion then inform the source or the one who controls. That means it will go to the source or sources of the packet. This is explicit feedback. Another is based on implicit feedback.

Implicit feedback is based on the fact that whenever a packet is transmitted into the network a particular source may wait for the acknowledgment and by monitoring the delay in receiving the acknowledgment the source may decide whether the network is congested or not. If the delay is small which is essentially the propagation time plus transmission time then the source may say that the network is not congested. On the other hand, if delay is very high in such a case the source or the station gets some implicit feedback that means that acknowledgment accesses an implicit feedback which can be used for controlling congestion. So based on this the close loop can be divided into two different types.

Now, the basic objective of the open loop congestion control is by adopting suitable policies such that the congestion does not take place in the first place that means to prevent congestion. As you know prevention is better than cure so this is the policy adopted for open loop congestion control.

(Refer Slide Time: 20:18)



 Indian Institute of Technology, Kharagpur

Open Loop Congestion Control

- The basic objective is to prevent congestion by adopting suitable policies for:
 - Flow control
 - Acknowledgement
 - Retransmission (Timeout interval)
 - Caching
 - Packet discard
 - Routing
- Traffic Shaping:
 - The leaky bucket algorithm
 - The token bucket algorithm

For that purpose suitable policies can be adopted while doing various functions such as flow control. When flow control is done there are various techniques used in flow control such as stop-and-wait, go-back-N or sliding-window protocol is used for flow control. Now, whenever you are using sliding window protocol the number of packets in the network will depend on the window size. So if window size restricted to small numbers as 7 or 3 then the traffic on the network will be small. On the other hand, if a large window size is used the number of packets in the network will be high before acknowledgments are received. Hence that flow control may help in preventing congestion. By adopting suitable policies for flow control congestion can be prevented.

Then we have the acknowledgment policy. **as you know** a particular destination node can send explicit acknowledgment packet which will reach the source station. Another possibility is that whenever full-duplex communication is going on there is traffic in both directions then the destination node can send the acknowledgment in the form of piggybacking. We already discussed the piggybacking approach. Thus if piggybacking approach is used for acknowledgment then the number of traffic in the network is reduced which in turn helps in preventing congestion.

Then we have the retransmission policy. The retransmission policy essentially discusses the timeout interval. If the timeout interval is small then many retransmission will take place before acknowledgment is received. On the other hand, if the retransmission time is longer that means the timeout interval is longer there is a possibility that the number of packets that is the acknowledgment is received before timeout takes place so retransmission will not take place. That is why the retransmission policy particularly the timeout interval will help in preventing congestion.

Now let us see the caching policy. We have seen that there are two approaches.

Whenever automatic repeat request technique is used for error control we know that we can use either go-back-N ARQ or we can use repeat request protocol. So whenever it is repeat request then we know that we have to do some kind of caching of the frames. So whenever it is being done then you do not have to retransmit a number of packets which have been received correctly by the destination. So this caching also helps in reducing the number of packets in the network. Then we have the packet discard. The discard policy will also decide how to control congestion. **We shall discuss this later on.**

We have discussed the routing techniques. For example, flooding increases the number of packets in the network. The traffic increases in an unbounded manner. So, if flooding is used for routing then it may lead to congestion. Therefore by adopting suitable policy in routing congestion can be prevented.

(Refer Slide Time: 24:14)

Indian Institute of Technology, Kharagpur

Open Loop Congestion Control

- The basic objective is to prevent congestion by adopting suitable policies for:
 - Flow control ✓
 - Acknowledgement ✓
 - Retransmission (Timeout interval) ✓
 - Caching ✓
 - Packet discard ✓
 - Routing ✓
- Traffic Shaping:
 - The leaky bucket algorithm
 - The token bucket algorithm

Open Loop Control

Now let us consider two important techniques of open loop control. One is Leaky Bucket Algorithm and the other is Token Bucket Algorithm.

(Refer Slide Time: 24:17)

Indian Institute of Technology, Kharagpur

The Leaky Bucket Algorithm

Bursty flow

Leaky bucket

Fixed flow

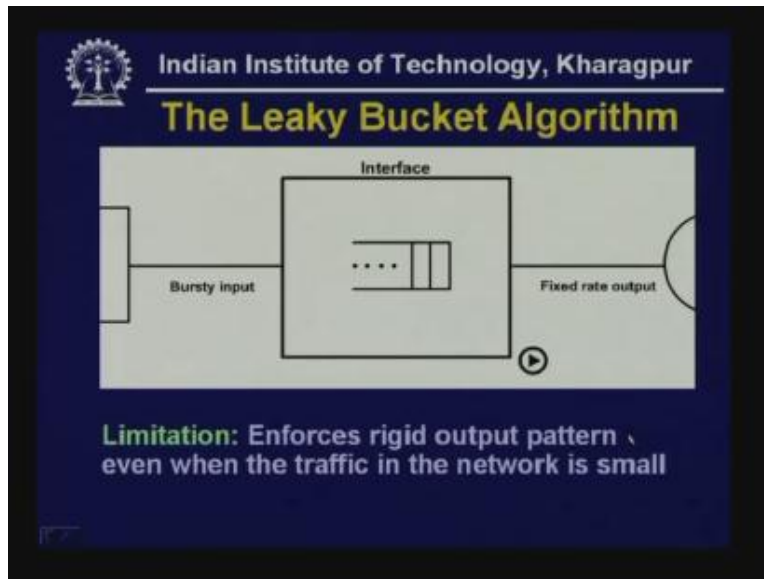
10 Mbps

2n

Here what is being done is some kind of traffic **safety is done** so that the network is not congested. **Let us see how it is being done.** Here this is basic philosophy. You can see here that the bucket is getting filled up and here you have got some kind of bursty flow but there is a fixed flow at the output. Here whenever the bucket gets filled up (Refer Slide Time: 24:40) leading to what is known as packet discarding. Thus what it essentially does is suppose the input packet generated by the source node is like this

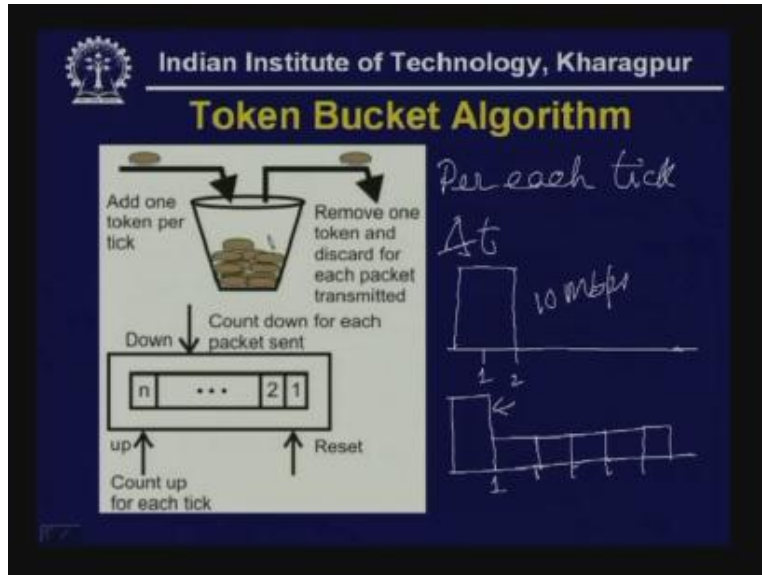
suppose it generates at the rate of 10 Mbps per 2 second and then for 2 seconds it sends at the rate of 10 Mbps so here it is bursty in nature and what the leaky bucket will do is it will smooth out and send it at the rate of 2 Mbps for 10 seconds. So, for 10 seconds it is sent in the uniform rate. So as a result as you can see the traffic is at a fixed rate throughout the 10 second period. This is what is being done by this approach.

(Refer Slide Time: 25:47)



So what it does is it shapes bursty traffic into fixed rate traffic however it has the disadvantage that packets are dropped when the bucket is full. When the bucket is full the packet gets dropped in this particular type of algorithm. One another important drawback of this technique is that whenever the network is not congested there are few packets in the network and even under that situation it reduces traffic rather controls the packet in the same manner. So whether the network is congested or not, whether there are many packets or smaller number of packets at a uniform rate the packets are introduced which is not necessary. When you have got less number of packets in the network the packets may be introduced at a higher rate and that is precisely what is done in this Leaky Bucket Algorithm. Therefore in the Leaky Bucket Algorithm the input is again bursty in nature and as we have already discussed the leaky bucket is generated in a uniform manner. So this is the limitation even in the beginning and at the end as it generates at a uniform rate. This limitation can be overcome by using the Token Bucket Algorithm as we shall see.

(Refer Slide Time: 28:35)



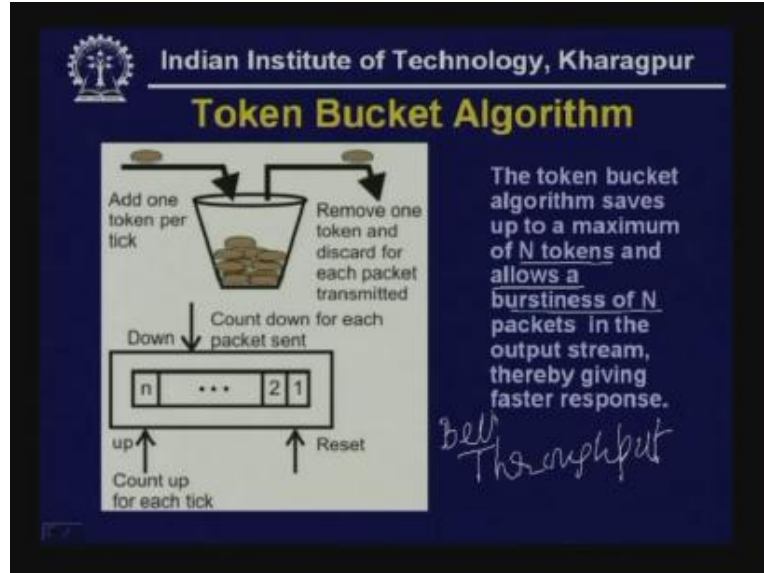
As I already mentioned this enforces rigid output pattern even when the traffic in the network is small. Now let us see what is being done Token Bucket Algorithm.

In Token Bucket Algorithm it is done in a different way. Here you have got some kind of a counter and per each tick say (Δt) a token is added to the bucket. And whenever packets come if you have got enough number of tokens accumulated then it allows the traffic to be sent at the rate in which it has come.

After all the tokens are exhausted it will then introduce the packets at the rate of one token per tick. That means it will become the same as the Leaky Bucket Algorithm. So let us consider the same example. Suppose it has received at the rate of 10 Mbps for two second this is one this is two because of the bursty nature of traffic therefore in case of token bucket what will be done is may be for one second it will send at the rate of 10 Mbps and assuming that five tokens were stored and after that for five more seconds 1 2 3 4 5 that means in six seconds all the packets are transmitted.

Therefore as you can see, initially for this part there were accumulated tokens and because of that the data is transmitted at the rate which it has been introduced into the network and after that it is transmitted. Both these Leaky bucket and Token Bucket Algorithms can be implemented by the operating system or by a network interface chord which is connected to the network and as you can see it is implemented with the help of a counter which initializes to 0 in the beginning and per tick the counter is incremented.

(Refer Slide Time: 31:20)



On the other hand, whenever each packet is sent the counter is decremented. In other words countdown for each packet sent and **count of it performs** for each tick and in this way the counter is maintained to implement the Token Bucket Algorithm so it can be implemented either by hardware or by the operating system of the host.

We have seen that the Token Bucket Algorithm saves up to a maximum of N tokens and allows a burstiness of N packets in the output stream thereby giving faster response. We have already seen that the time taken for introducing the packets in the network is smaller than the Leaky Bucket Algorithm in Token Bucket Algorithm so it increases throughput compared to the Leaky Bucket Algorithm thereby providing you better throughput.

Now, to make the traffic shaping approaches successful it is necessary to specify the requirement in a precise manner known as flow specification. That means traffic shaping can be done very effectively if the flow specification is provided by the source node in a proper manner and its requirement is specified in a proper manner. What are the things to be specified let us see.

(Refer Slide Time: 32:20)

Indian Institute of Technology, Kharagpur

Flow Specification

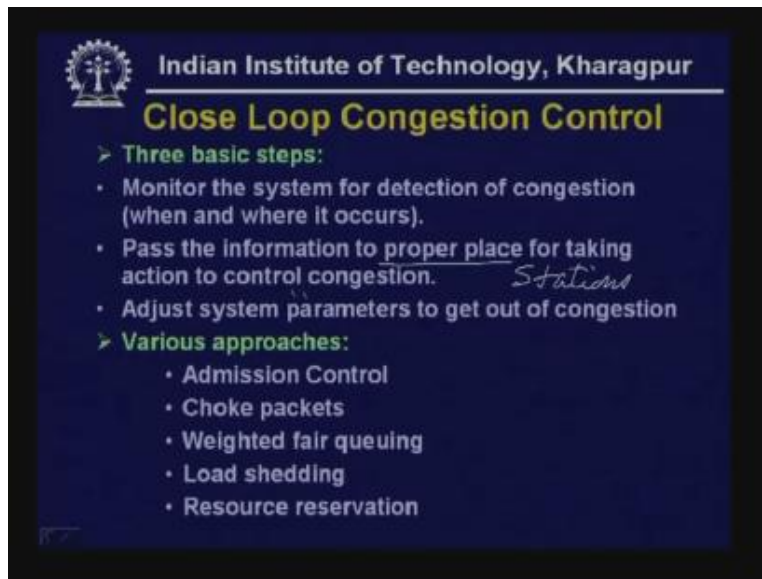
➤ To make traffic shaping approaches successful, it is necessary to specify the requirement in a precise manner known as **Flow Specification**.

➤ Input characteristics:	➤ Services desired
➤ Maximum packet size <i>kbits</i>	➤ Reliability ✓
➤ Token bucket rate <i>Mb/sec</i>	➤ Delay ✓
➤ Token bucket size <i>GB</i>	➤ Jitter ✓ <i>Variation of Delay</i>
➤ Maximum transmission rate	➤ Bandwidth

first one is input characteristic that means the maximum packet size in terms of may be kilobits or megabits or whatever it may be then the token bucket rate it can be say megabit per second the maximum rate at which the packet can be sent then token bucket size it can be megabyte or gigabyte and the maximum transmission rate that can be done. These are the four input characteristic to be specified. On the other hand, services required desired by the host must also be specified like what is the reliability desired, what is the delay in sending a packet is desired, and what is the delay it can tolerate for a particular application that has to be specified depending on the nature of traffic whether it is data or voice or video.

Hence whenever you are sending voice or video another important parameter is not the delay but the variation of delay and that has to be specified properly. So the variation of delay needs to be properly specified that is expressed in terms of jitter. Also, it is necessary to specify the bandwidth required for a particular application. So obviously for sending speech or music the bandwidth required is smaller compared to bandwidth required for sending video. These are the services desired that must be specified so that traffic shaping can be done properly. With this we come to the end of open loop congestion control technique. Now let us focus on the close loop congestion control technique.

(Refer Slide Time: 34:30)



The slide features the IIT Kharagpur logo in the top left corner. The title 'Close Loop Congestion Control' is displayed in a large, bold, yellow font. Below the title, the content is organized into two main sections: 'Three basic steps' and 'Various approaches', both marked with a green arrow icon. The 'Three basic steps' section contains three bullet points, with the second point including a handwritten note 'Stations' in blue ink. The 'Various approaches' section lists five techniques as bullet points.

Indian Institute of Technology, Kharagpur

Close Loop Congestion Control

➤ Three basic steps:

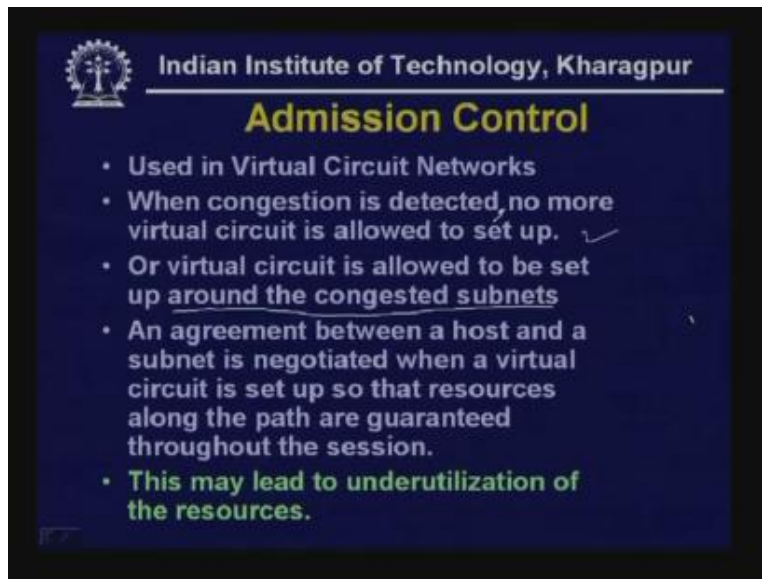
- Monitor the system for detection of congestion (when and where it occurs).
- Pass the information to proper place for taking action to control congestion. *Stations*
- Adjust system parameters to get out of congestion

➤ Various approaches:

- Admission Control
- Choke packets
- Weighted fair queuing
- Load shedding
- Resource reservation

In close loop congestion control technique there are three basic steps. First one is monitor the system for detection of congestion. That means monitoring of the status of the network is necessary and usually it is done by the nodes or the switches they will monitor and decide based on the delay, based on queue length and various other parameters and then that has to be informed to the place where the action is taken. That means pass the information to the proper place for taking action to control congestion. Usually this action has to be taken by the stations or the source nodes. So information has to be passed on to the stations for taking action to control congestion. Then the source will adjust system parameters to get out of congestion. That means the close loop congestion control techniques are used when the network is really in congestion may be it is in light congestion mode or it is heavily congested whatever it may be both will be detected. Here we have various approaches used for congestion control.

(Refer Slide Time: 35:22)



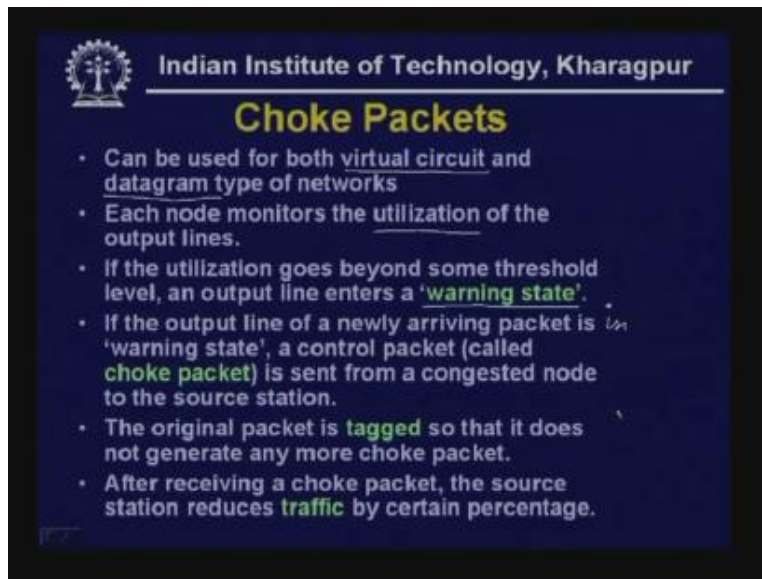
First let us consider the admission control. This admission control technique is used in virtual circuit networks. So, when congestion is detected no more virtual circuit is allowed to be set up. That means whenever congestion has already taken place the network will not allow setting up any more virtual circuit. That is the basic approach of admission control. This is one policy.

Another is, the virtual circuit is allowed to be set up around the congested subnets. That means may be the congestion has affected or the traffic has increased significantly in one portion of the network and not throughout the network. So, if the packet can be sent around the congested subnets and not through the congested subnet then this is also part of the admission control. That means the virtual circuit is allowed to be set up around the congested subnet and not through the congested subnet that can be done as part of the admission control.

So an agreement between a host and a subnet is negotiated when the virtual circuit is set up so that resources along the path are guaranteed throughout the session. That means whenever a virtual circuit is set up the required bandwidth, required buffer space are all negotiated between the source node and the subnet so that the congestion is overcome. Therefore this particular approach is known as admission control approach.

However, this may lead to underutilization of the resources. Since the source node is negotiating and locating some kind of bandwidth and resources still it is not utilized and because of bursty nature of traffic it is underutilized that is one limitation of this admission control approach. Even under the availability of resources the virtual circuit is not allowed to be set up so this may lead to underutilization but definitely it helps in overcoming congestion.

Second approach under the close loop control technique is choke packets.
(Refer Slide Time: 38:22)



Indian Institute of Technology, Kharagpur

Choke Packets

- Can be used for both virtual circuit and datagram type of networks
- Each node monitors the utilization of the output lines.
- If the utilization goes beyond some threshold level, an output line enters a 'warning state'.
- If the output line of a newly arriving packet is 'warning state', a control packet (called **choke packet**) is sent from a congested node to the source station.
- The original packet is **tagged** so that it does not generate any more choke packet.
- After receiving a choke packet, the source station reduces **traffic** by certain percentage.

This approach can be used both in case of virtual circuit as well as datagram type of networks. Here each node monitors the utilization of the output lines. This is based on the utilization of the output line. As we already mentioned the thumb rule, whenever utilization is increased beyond 80% then we may consider that the network is congested. so whenever this kind of utilization increases beyond some limit, beyond some threshold level the output line enters a warning state so the particular line enters a warning state. So if the output line is of a newly arriving packet is in warning state a control packet called choke packet is sent from a congested node to the source station.

That means the node to which a link is connected and which has reached a warning state that sends a choke packet towards the source node. so the original packet is tagged so that it does not generate any more choke packet. So although a choke packet is sent towards the source node the node forwards the packets towards the destination so it may be possible that the other nodes in the path may again send the choke packet to prevent that it is tagged so that no choke packets are generated. Then after receiving a choke packet the source station reduces traffic by a certain percentage.

Suppose after receiving a choke packet the station reduces traffic by 50%. Now, after reducing the traffic for fifty percent again it waits for certain duration and still if it receives a choke packet it further reduces by 25% and again after waiting for some more time even if it receives a choke packet it reduces by another 10% so in this way it goes on and at some point time it may discard a packet. But usually whenever this kind of reduction takes place the network will come out of congestion and no more choke packet will be received.

If no more choke packet is received for certain duration then the traffic is again increased but not at a high rate, but may be increased at the rate of 10%. So it is increased at the rate of 10% and reduced at a higher rate in the beginning then the rate is smaller and smaller. This is how the traffic is controlled by the source node in response to choke

packets and the system comes out of congestion. This choke packet approach has a serious drawback that the action taken by a source is voluntary. That means a source node after receiving a choke packet may decide to reduce the traffic or it may not reduce the traffic.

(Refer Slide Time: 41:56)

Indian Institute of Technology, Kharagpur

Fair Queuing

- Choke packet approach has the drawback that the action taken by a source is voluntary.
- To overcome this problem, **fair queuing** algorithm is used, where queues are scanned in a round-robin manner.
- Packets are **sorted** in order of their finishing time and sent in that order.

1	5	9	12
2	6		
3	7	10	
4	8	11	13
			14

Packet	Finishing Time
B	6
C	10
A	12
D	14

So to get around this problem or to overcome this problem fair queuing approach is done, fair queuing algorithm is used where queues are scanned in a round-robin manner and then packets are sorted in order of their finishing time. so you can see that a byte by byte scanning is done and the finishing time is found out for example 6 is the finishing time for queue packet on the input line B, then 10 is the finishing time on the packet on the input line C and so on.

Now, after finding out the finishing times the packets are ordered in this manner in order of finishing times that means B C A D then the packets are sent in that order. First B is sent, C is sent, A is sent and D is sent this is known as fair queuing. This is based on the queue length. Another possibility is that it can be based on the application. For example, for some applications it may be necessary to discard a recent packet. For example, if it is sending data. In case of data it is necessary to discard a recent packet rather than old packet. The reason is if the recent packet is not discarded and if an old packet is discarded then again you have to perform retransmission of a number of packets by using go-back-N ARQ.

(Refer Slide Time: 43:50)

Indian Institute of Technology, Kharagpur

Weighted Fair Queuing

- Instead of giving same priority to all the the hosts, higher priority can be given to some hosts, such as server, leading to the modified algorithm known as **weighted fair queuing**.

Data Recent
Video Old

On the other hand, if a recent packet is discarded then the number of retransmissions will be reduced. On the other hand, if it is a video or voice in such a case it may necessary to discard an old packet rather than a recent packet. The reason is old packet is no longer important and it may have already cost some kind of damage **or jitter** in the system. But if a recent packet is not allowed to be discarded then some weights can be assigned based on the application so that the packet discarding policy can be **formed** and this may lead to weighted fair queuing. Therefore based on these applications you can do weighted fair queuing where some **weightage** is given to different packets based on different applications. Then as I was mentioning packets have to be discarded and when other methods fail the nodes can resort to heavy artillery known as load shedding.

(Refer Slide Time: 46:30)

Indian Institute of Technology, Kharagpur

Load Shedding

- When other methods fail, the nodes can resort to a heavy artillery: **Load Shedding**.
- When the nodes are not able to handle the packets, packets are **discarded**.
- A node drowning in packets, one approach is to discard packets **at random**.
- In many situations, some packets are more important than others.
- To implement this **intelligent discard policy**, the applications must mark the packets with **priority classes**.
- Simulation results show that it is better to start **discarding packets early**, rather than wait until the network is completely clogged up

That means whenever the nodes are not able to handle the packets the buffer is full or delay is too high so in such cases packets can be discarded. Now one possibility is that a node drowning in packets may use at random discard policy.

That means it may discard packets at random however this at random policy is not good. In many situations some packets are more important than others as I already mentioned so in such a case some intelligent discard policy can be adopted based on the application and the application must mark the packets with priority classes. In such a case instead of discarding packets at random using the intelligent discard policy the packets with lower priority are discarded than packets of higher priority. So this approach is known as load shedding. The terminology or the word has been taken from the electrical distribution system where whenever the load on the electrical network is high load shedding is done so this approach is similar to that and here essentially packet discarding occurs.

The simulation results show that it is better to start discarding packets early rather than wait until the network is completely clogged up. That means question arises when packet discarding should start. Simulation result has confirmed that it is better to start discarding in the beginning other in the onset of congestion rather than when the network is heavily congested. That means whenever discarding is performed in the early phase of the congestion it may come very quickly out of congestion but whenever it is already congested then its effect is lesser.

Then we shall discuss about another important technique known as resource reservation protocol.

(Refer Slide Time: 46:54)


Indian Institute of Technology, Kharagpur
RSVP – Resource reSerVation Protocol

- Multicast flows from multiple sources to multiple destinations
- Uses multicast routing using spanning trees.
- Each group is assigned a group address, which is used to send packets to that group
- The multicast routing algorithm builds a spanning tree covering all group members.
- To eliminate congestion any of the receivers can send reservation message up the tree to the sender.



This is particularly important in the context of multicast applications. So far we have discussed about point-to-point data flow that means there is a source and there is destination. The traffic is going from source to the destination, it is essentially point-to-point between two nodes. But there are many applications where the data has to go to multiple destinations or it has to be broadcasted. So, whenever a packet has to go to multiple destinations we call it multicasting.

One important application for multicasting is, for example there is a station who is giving video on demand service to a number of users so depending on the network a group of people will ask for video services for particular stations so may be the same video has to go to a number of stations depending on the requirement. In such a situation this is useful. First of all it uses multicast routing using spanning trees. So let us see how it is being done.

Here 1 2 3 (Refer Slide Time: 48:28) these are the sources and 4 5 6 are the destinations. Now 1 2 3 are giving video services to the destination stations 4 5 and 6 so each source will form a spanning tree. As we can see here the spanning tree is from one station will go to node A, then it will go to node C, then it will go to node D and from there it is going to three different destinations so it is transmitted on three paths rather than one and this spanning tree is based on the least-cost path.

Thus from 1 to 4 5 6 this is the spanning tree similarly this spanning tree can be from 2 to again 4 5 6. Now let us see how the resource reservation can be done. Suppose 4 wants some service from the source 1 so it will reserve sources along the network the bandwidth and the data rate that is required and after that the same node may decide to have another video from another source so it reserves the bandwidth and the buffers in different nodes along the path.

Now at this point what can happen is another destination may also want to have the sources along the path. Now you can see here (Refer Slide Time: 50:22) that between C

and D 4 has already reserved for two streamed video traffic and at the same time 6 has demanded another one. Now, if the nodes between C and D have to find out whether there exist enough resources between C and D only then it will allow destination station D to set up the virtual circuit. So we find that in this way the resources are reserved before transmission of data takes place. Particularly in multicasting application this is very important.

Another possibility is that it may be necessary to broadcast some information to number of destination stations. So in such case one important candidate for broadcasting is flooding as you know. Although flooding increases the traffic significantly but for broadcasting purpose when broadcasting has to be done the flooding is used for the purpose of broadcasting.

Finally we shall discuss about the difference between congestion and flow control.

(Refer Slide time: 51:56)

The slide is titled "Congestion Versus Flow Control" and is from the Indian Institute of Technology, Kharagpur. It is divided into two columns. The left column is titled "Congestion control:" and lists three points: it is a global issue, it occurs due to combined behavior of stations and switches, and its job is to ensure the subnet can handle the load. The right column is titled "Flow control:" and lists two points: it is a local issue between a sender-receiver pair, and its primary function is to prevent a fast sender from overwhelming a slow receiver.

Congestion control:	Flow control:
<ul style="list-style-type: none">> Congestion control is a global issue. It is a joint responsibility of the users and the network.> It occurs because of the combined behavior of the stations, switches, routing policies, etc> Its job is to ensure that the subnet is able to carry the offered load.	<ul style="list-style-type: none">> Flow control is a local issue between a sender-receiver pair.> Its primary function is to ensure that a fast sender does not overwhelm a slow receiver.

People are confused about these two techniques congestion control and flow control. We have seen that both cases the destination nodes sometimes send a packet towards the source node either for flow control or for congestion control the choke packets are sent as we have seen. That is why people get confused about these two techniques. But they are much different.

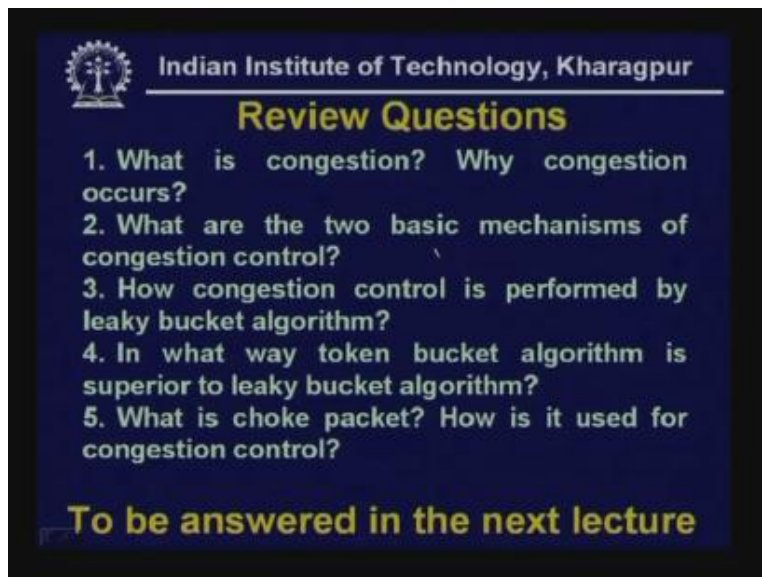
As you can see congestion control is a global issue, it is a joint responsibility of the users and the network. That means so far as the congestion control is concerned not only all the nodes but all the stations are responsible for the congestion control for congestion to take place and it occurs because of combined behavior of the stations, switches, routing policies and so on.

Its job is to ensure that the subnet is able to carry the offered load. Let us take an example where congestion occurs.

Suppose you have got thousand nodes and they are sending at the rate of 1 Mbps so in such a situation when all of them start sending at that rate may be at lower rate that is 1 Mbps congestion will occur. On the other hand, flow control is a local issue between sender-receiver pair and it is not a global issue. The source destination pair or the sender-receiver pair is responsible. Its primary function is to ensure that a fast sender does not overwhelm a slow receiver. That means flow control is necessary in such a situation where if there is a server which can send at the rate of 10 Giga bytes per second on the other hand, the source destination node which is a desktop can receive only at 1 Giga byte per second so in this case it will get overwhelmed. Although there is no heavy traffic in the network a source node with heavy load can overwhelm a receiver thus in such a situation flow control is performed.

Thus we have discussed the differences between the congestion control and flow control. Now it is time to give you the review questions on this lecture.

(Refer Slide Time: 54:47)



Indian Institute of Technology, Kharagpur

Review Questions

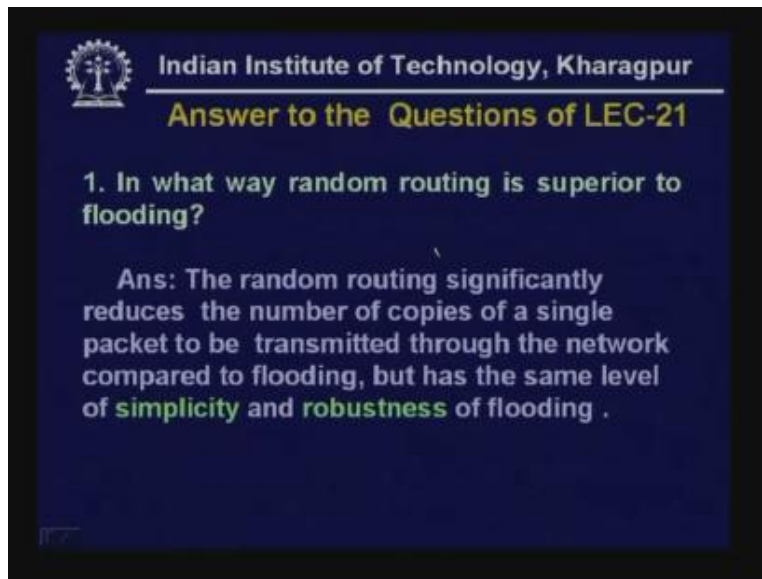
1. What is congestion? Why congestion occurs?
2. What are the two basic mechanisms of congestion control?
3. How congestion control is performed by leaky bucket algorithm?
4. In what way token bucket algorithm is superior to leaky bucket algorithm?
5. What is choke packet? How is it used for congestion control?

To be answered in the next lecture

- 1) What is congestion? Why congestion occurs?
- 2) What are the two basic mechanism of congestion control?
- 3) How congestion control is performed by Leaky Bucket Algorithm?
- 4) In what way Token Bucket Algorithm is superior to Leaky Bucket Algorithm?
- 5) What is choke packet? How it is used for congestion control?

Now let me give you answers of lecture – 21.

(Refer Slide Time: 55:24)



Indian Institute of Technology, Kharagpur

Answer to the Questions of LEC-21

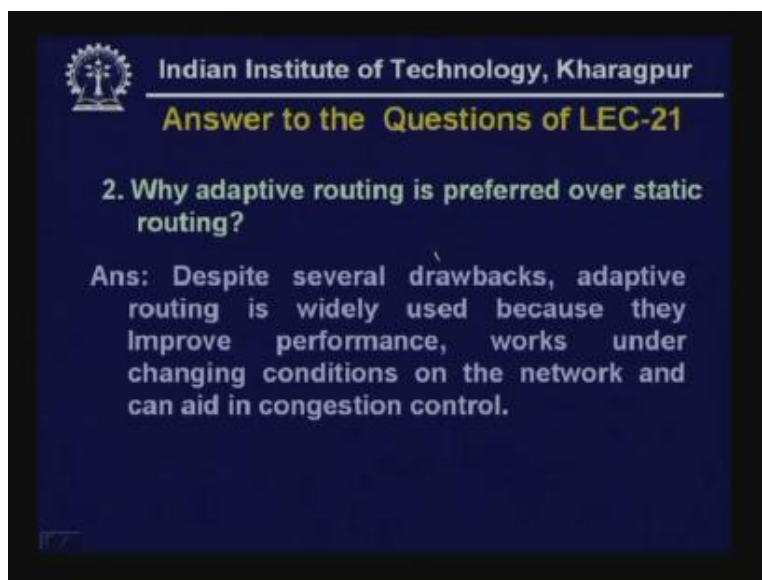
1. In what way random routing is superior to flooding?

Ans: The random routing significantly reduces the number of copies of a single packet to be transmitted through the network compared to flooding, but has the same level of simplicity and robustness of flooding .

1) In what way random routing is superior to flooding?

As we have discussed the random routing significantly reduces the number of copies of a single packet to be transmitted through the network compared to flooding but has the same level of simplicity and robustness of flooding. That means random routing reduces the traffic but has the same characteristic features like simplicity and robustness of flooding that is why random routing has some advantage over flooding.

(Refer Slide Time: 56:24)



Indian Institute of Technology, Kharagpur

Answer to the Questions of LEC-21

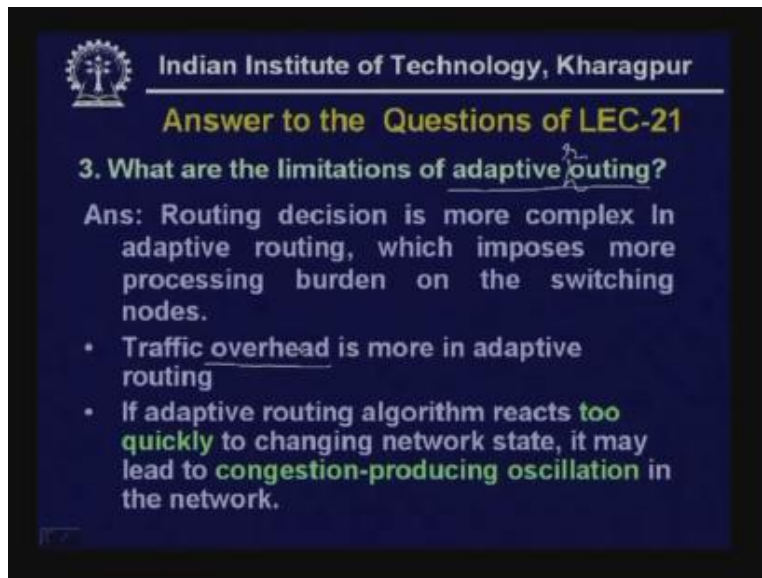
2. Why adaptive routing is preferred over static routing?

Ans: Despite several drawbacks, adaptive routing is widely used because they improve performance, works under changing conditions on the network and can aid in congestion control.

2) Why adaptive routing is preferred over static routing?

We have seen that adaptive routing increases the traffic in the network. However, adaptive routing is preferred because of some advantages. First advantage is that it improves the performance and it works under changing conditions. What are the changing conditions? When there is a node or link failure or there is congestion then this adaptive routing will help in aiding congestion control which the fixed routing cannot do.

(Refer Slide Time: 56:55)



3) What are the limitations of adaptive routing?

Routing decision is more complex in adaptive routing which imposes more processing burden on the switching nodes. As I have already mentioned the routing algorithm used in the adaptive routing is quite complex as a result it imposes burden on the switching nodes. And the traffic overhead is more in adaptive routing. We have seen that in adaptive routing we have to use some additional packets for control purposes that is why the traffic increases.

If adaptive routing algorithm reacts too quickly to changing network state it may lead to congestion producing oscillation in the network. As I have already mentioned whenever adaptive routing is used if it is performed very quickly then the traffic is sent to another part where congestion occurs and again the traffic is sent to another part that means the congestion area keeps on changing that is why it leads to congestion producing oscillation. So these are the limitations of adaptive routing.

(Refer Slide Time: 58:15)

Indian Institute of Technology, Kharagpur
Answer to the Questions of LEC-21

4. Compare and contrast distance vector routing with link state routing.

<ul style="list-style-type: none">➤ Distance vector:➤ Knowledge about the entire network➤ Routing only to neighbors➤ Information sharing at regular interval	<ul style="list-style-type: none">➤ Link state:➤ Knowledge about the neighborhood➤ Routing to all➤ Information sharing at regular interval➤ Converges quickly➤ Requires more CPU power and memory➤ more scalable
--	---

4) Compare and contrast distance vector routing with link state routing.

Distance vector routing uses the knowledge about the entire network, routing only to neighbors, information sharing at regular interval. On the other hand, link state routing has knowledge about the neighborhood, routing to all, information sharing at the regular interval, it converges quickly, requires more CPU power and memory, and it is more scalable.

(Refer Slide Time: 58:40)

Indian Institute of Technology, Kharagpur
Answer to the Questions of LEC-21

5. In what way second generation ARPANET algorithm differs from the first generation ARPANET routing algorithm?

Ans: In the first generation ARPANET, the estimated link delay was simply the queue length for that link and routing was based on distance vector routing.

On the other hand, actual delay was measured and used in the routing algorithm based on link state routing in the second generation ARPANET routing.

5) In what way the second generation ARPANET algorithm differs from first generation ARPANET routing algorithm?

As we have seen in second generation delay was actually measured rather than the queue length. That was the basic difference between the second generation and first generation.