International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Congestion Control Techniques for Mobile Network

Hemalatha J. P.

Lecturer, Department of Computer Science, Kle Society's S.Nijalingappa College, Rajajinagar, Bangalore-10, India

Abstract: ***Congestion Control is concerned with efficiently using a network at high load. Congestion control in mobile networks so that network queues remain bounded and the resulting flow rates satisfy an associated network utility maximization problem transmission failure occurs due to several reasons, such as node mobility, channel collision and abnormal channel conditions. The solution must have capability to handle bad channel condition and connectivity failures in unicast transmission. Joint congestion control scheme with scheduling algorithm is improved for dynamic wireless network by changing scheduling scheme with adaptation model.***

1. Introduction

When too many packets are transmitted through a network, congestion occurs at very high traffic, performance collapses completely and almost no packets are delivered.

The assumption that statistical multiplexing can be used to improve the link utilization is that the users do not take their peak rate values simultaneously. But since the traffic demands are stochastic and cannot be predicted, congestion is unavoidable.

Whenever the total input rate is greater than the output link Capacity, congestion happens. Under a congestion situation, the queue length may become very large in a short time, resulting in buffer overflow and cell loss.

1.1 Differences between congestion control and flow control

- **Congestion control:** try to make sure subnet can carry offered traffic, a global issue involving all the hosts and routers. It can be open-loop based or involving feedback
- **Flow control:** is related to point-to-point traffic between given sender and receiver, it always involves direct feedback from receiver to sender

1.2 Causes for congestion control

- Congestion is caused by the shortage of buffer space. The problem will be solved when the cost of memory becomes cheap enough to allow very large memory.
- Packet arrival rate exceeds the outgoing link capacity.
- Insufficient memory to store arriving packets
- Bursty traffic: When part of the network no longer can cope a sudden increase of traffic, congestion builds upon. Other factors, such as lack of bandwidth, ill-configuration and slow routers can also bring up congestion Maximum carrying capacity of subnet Packets delivered Perfect Desirable Congested Packets sent.
- Slow processor
- Congestion is caused by slow links. The problem will be solved when high-speed links become available.
- It is not always the case; sometimes increases in link bandwidth can aggravate the congestion problem because higher speed links may make the network more unbalanced.

Congestion is dynamic problem, any static solutions are not sufficient to solve the problem.

1.3 Security Concerns to be considered

1) **Insertion Attacks** – The intruder attempts to insert traffic into your network, typically through an unsecured mobile access point.
2) **Session Hijacking**—Also known as the man in the middle attack, it is possible to hijack a wireless session based upon the reality that the phone authenticates itself to the base station but not vice versa. It is possible to emulate the base station and thus hijack a phones session.
3) **Jamming** – This is a DoS (Denial of Service) attack where the attacker tries to flood the radio frequency (RF) spectrum of your wireless network by broadcasting packets at the same frequency as your network.
4) **Encryption Attacks** – The IEEE 802.11b wireless network standard uses an WEP (Wired Equivalent Privacy) encryption method. This standard uses weak Encryption and Initialization Vectors (IVs) and has been cracked successfully many times.
5) **Traffic Interception and Monitoring** (War Driving) – Wireless packets using the 802.11b standard has an approximate transmission distance of 300 feet. This means that anyone with the proper standard equipment can receive that signal if they are in transmission range. Equipment to further extend that range is easily available, so the area of interception can be quite large and hard to secure properly.
6) **Mobile Node to Mobile Node** – Most mobile nodes (laptops, PDA's) are able to Communicate directly with each other if file sharing or other TCP/IP services are running. This means that any mobile node can transfer a malicious file or program rapidly throughout your network.
7) **Configuration Issues** – Any wireless device, service, or application that is not correctly configured before installation and use can leave an entire network at risk. Most wireless devices and applications are pre-configured to accept any request for services or access. This means any passing mobile client can request and receive telnet sessions or ftp.
8) **Brute Force Attacks** – Most wireless access points use a shared password or key for all devices on that network. This makes wireless access points vulnerable to brute force dictionary attacks against passwords.

2. Congestion Control in Virtual Circuits

- These are closed-loop based designed for virtual circuits subnets, which are connection oriented. During connection set up, something can be done to help congestion control
- The basic principle is obvious: When setting up a virtual circuit, make sure that congestion can be avoided
- Admission control: Once congestion has been signaled, no more new virtual circuits can be set up until the problem has gone away. This is crude but simple and easy to do

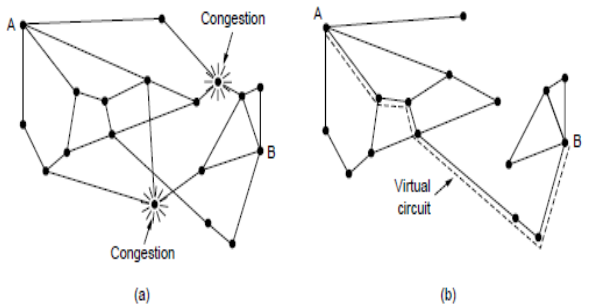

Figure 1: (a) (b)

Avoid part of the network that is overloaded, i.e. temporarily rebuild your view of network

E.g. normally, when router A sets a connection to B, it would pass through one of the two congested routers, as this would result in a Minimum-hop route (4 and 5 hops respectively). To avoid congestion, a temporary subnet is redrawn by eliminating congested routers. A Virtual circuit can then be established to avoid congestion. Negotiate quality of connection in advance, so that network provider can reserve buffers another resources, guaranteed to be there

3. Warning Bit

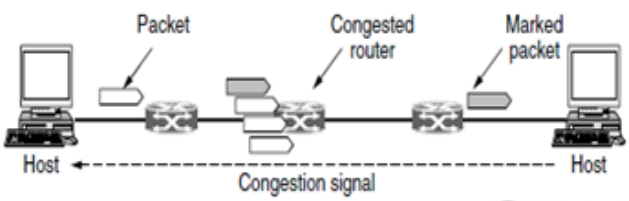

Figure 2: Warning Bit

A special bit in the packet header is set by the router to warn the source when congestion is detected. The bit is copied and piggy---backed on the ACK and sent to the sender. The sender monitors the number of ACK packets it receives with the warning Bit set and adjusts its transmission rate accordingly.

- Most effective way to control conges-on is to reduce the load that the transport layer is placing on the network.
- This requires the network and transport layers to work together.
- In this lecture, we will look at the network aspects of congestion.
- We will complete the topic by covering the transport aspects of congestion later

4. Congestion Control for Multicasting

a) Congestion control algorithms discussed so far deal with single-source to single-destination case
b) In the advent of all kinds of services on the Internet that deal with broadcasting streams of data (voice and video) with a limited bandwidth, managing multicast flows from multiple sources to multiple destinations becomes critical
c) Multicast routing uses spanning trees

– Hosts 1 and 2 are multicast senders,
and hosts 3, 4 and 5 are multicast receivers
– (a) shows network topology, multicast Trees from hosts 1 and 2 are shown in (B) and (c)

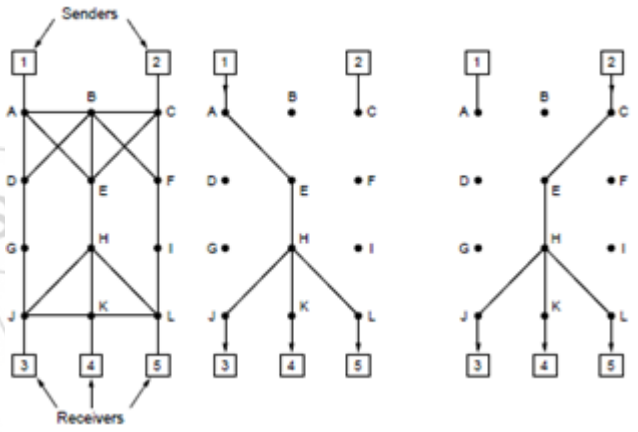

Figure 3: (a) (b) (c)

5. Resource Reservation Protocol (RSVP)

The basic idea is that, to avoid congestion, Extra information can be broadcasted to the group periodically to tell the routers along the tree to maintain certain data structures in their memories

Any receiver can send a reservation message up the tree to the sender, using the reverse path forwarding routing algorithm

At each hop, router notes reservation and reserve necessary bandwidth if insufficient bandwidth is available, it reports back failure. By the time the message gets back to Source, bandwidth has been reserved all the way from sender to receiver along the spanning tree

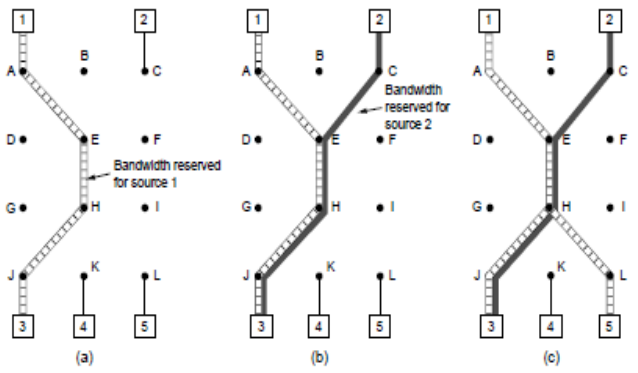

Figure 4: (a) (b) (c)

- Host 3 has requested a channel to host 1. Once it has been established, packets can flow from 1to 3 without congestion. Next host 3 decides to reserve a channel to the other sender, host 2, and 2nd path is reserved
- Now, host 5 makes a reservation to host 1. First, dedicated bandwidth has to be reserved as far as Router H. Router H can see that it already has a feed from host 1
- Assume bandwidth requested for host 1 to host 5 is no more than that reserved for host 1 to host 3. As the necessary bandwidth has already been reserved, it does not have to reserve any more

6. Agent Based Congestion Control Routing

The agent based congestion routing Architecture can be explained from the following

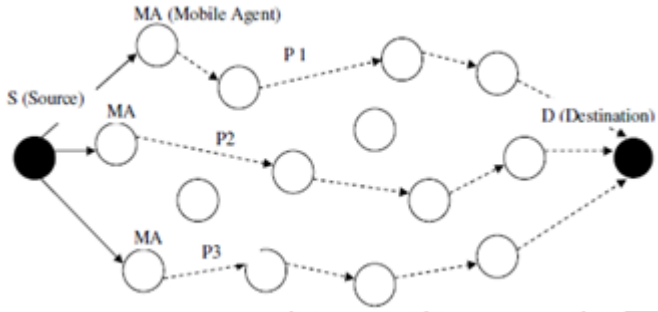

Figure 5: Agent Based Congestion routing

Step 1: The source S checks the number of available one hop neighbors and clones the Mobile Agent (MA) to those neighbors.

Step 2: The Mobile Agent selects the shortest path of the route to move towards the destination D as given in the figure 1 such as P1, P2 and P3.

Step 3: The MA1 moves towards the destination D in a hop-by-hop manner in the path P1 and MA2 in P2 and MA3 in P3 respectively.

Step 4: Then the MA1 calculates the TCM1 of that path P1 and similarly MA2 calculates the TCM2 of P2 and MA3 calculates the TCM3 of P3

Step 5: Now the destination D sends the total congestion metrics TCM1, TCM2 and TCM3 of the paths P1, P2 and P3 respectively to the source.

Step 6: Now the source selects path using min (TCM1, TCM2, and TCM3) and sends the data through the corresponding path which has the minimum congestion.

7. DTN Model

In the simulator, DTN nodes advertise their buffer content to each other every 100 ms by sending Hello messages. In our simulations, this message has enough room for the identifiers of buffered bundles and return receipts. A bundle can be generated only if the node has sufficient buffer space available.

When the bundle lifetime expires, all copies of that bundle are deleted. If the sender does not receive a return receipt within retransmission timeout, it will retransmit the bundle. Return receipts may also serve as anti packets; their lifetime is the minimum of retransmission timeout (1000 seconds) less bundle forwarding time and bundle lifetime (750 seconds). Anti packets and Hello messages are small in size. The selected routing protocol is either epidemic routing or binary spray and waits; the latter if uses 16 message copies. Return receipts are forwarded first. When the head-of-line receipt has been forwarded to all current neighbors, one by one, we put that receipt to the tail of the receipt queue and dequeue the next receipt. Then, we forward regular bundles to their destinations, in a similar manner as return receipts. After this, the bundles are re-ordered so that the least forwarded bundles are put to the head of the queue. Finally, regular bundles are forwarded to neighboring, non-destination nodes.

8. WIN: Next Generation Threat Intelligence

The Web root Mobile Security SDK accesses the Web root Intelligence Network (WIN) to provide next generation threat intelligence that is highly accurate and always up to date. This architecture incorporates the patented fourth generation Web root threat processing and malicious code identification system which has intimate knowledge of more than 300 million executables, including their runtime behavioral characteristics.

Optionally, WIN services categorize files and their interactions with other files, and use the Web root Bright cloud IP Reputation Service to track malicious IP addresses and provide accurate content classification, threat reputation, and threat vector data. These systems, along with another 150+ terabytes of threat data, ensure that Web root security solutions are ready to detect new threats. As this collective intelligence delivers comprehensive real-time protection, endpoints collect over 200 gigabytes of behavioral execution data each day. Unique URL and IP data feeds from strategic partners further enrich Web root malware intelligence.

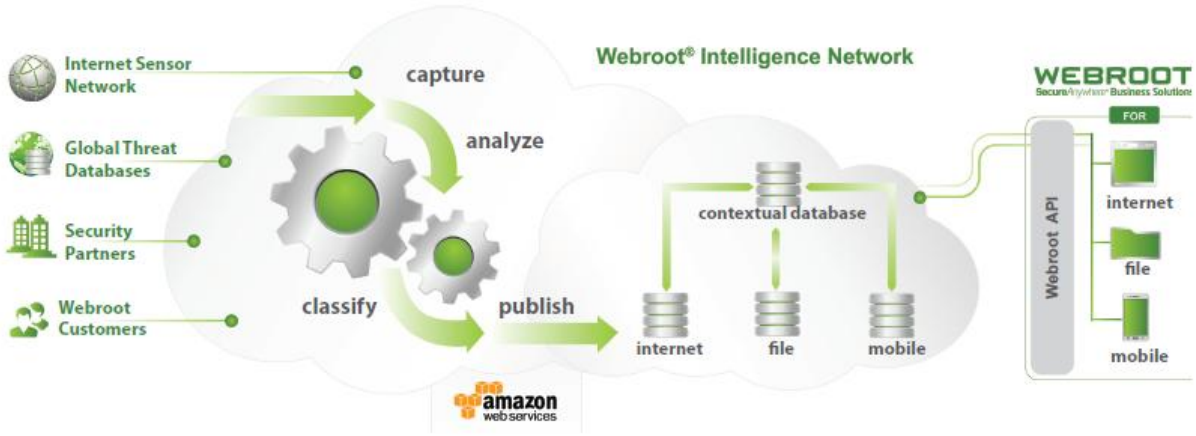

Figure 6: WIN

9. Conclusion

Wireless communications technologies are opening up opportunities to bring unserved segments of society into the digital age, particularly in emerging markets and remote, hard-to-reach areas of the world

Application of different methods to control the congestion in mobile network is a source for development of new methods and technology. “Golden information technology” becomes a source for new computer projects.

It is difficult to precise boundaries but possible to know the concepts well. Hence it is important to control congestion in network.

References

[1] epubl.ltu.se/1402-1757/2005/12/LTU-LIC-0512-SE.pdf
[2] www.jatit.org/volumes/researchpapers/Vol4No10/10Vol4No10.pdf
[3] www.cs.cmu.edu/~dga/15-441/S08/lectures/22-qos.**pdf**
[4] dl.acm.org/citation.cfm?id=1098726
[5] https://www.euro**control**.int/.../**Network**_Cong_2030_1_Strat_recom_Re...
[6] ftp://ftp.cs.umass.edu/pub/net/pub/vfiroiu/red-dynamics-conf.ps
[7] https://en.wikipedia.org/wiki/**Network_congestion**
[8] https://www.ietf.org/proceedings/77/slides/iccrg-7.pdf
[9] https://inst.eecs.berkeley.edu/~ee290t/sp02/**Network_Congestion**.ppt