

Message Integrity, Reliable Delivery, Acknowledgements, Non-Repudiation and Encryption

By Verity Carney

Assume that the network links of the Internet offer reliable delivery service. Should TCP be used in this network?

The network layer is responsible for delivering datagram's from source to destination subject to pre-specified quality of service parameters. The transport layer determines how to use the network layer to provide a virtual error-free, point-to-point connection so that a source host can send messages to a destination host that will arrive un-corrupted and in the correct order. If network layer provides reliable delivery services, the upper layer interaction with the transport layer is less onerous.

However TCP should still be used as long as there is no need for broadcast or multicast real time transmission. This is because TCP provides a greater guarantee that the network doesn't get clogged up and made unreliable (discarding packets) by ensuring that the applications running over the network cooperate with other connections by adjusting their transmission rates appropriately. In this way TCP ensures fairness in the use of the network by providing a mechanism for flow control and congestion control that regulates an applications transmission rate via the congestion-window.

Describe, compare and contrast the basic concepts of the stop-and-wait protocol with the sliding window protocol.

In Stop and wait protocols the send-side waits for data to be passed down from the upper layer. When the send data event occurs the sender creates a packet containing the data to be sent, along with a packet checksum and then send the packet. The sender then waits for an acknowledgement or non-acknowledgment to be sent by the receiver. If an acknowledgement is sent it knows the packet has been received correctly and then waits for data from the upper layer. If a non-acknowledgment is received the protocol

1

By Verity Carney

retransmits the last packet and waits for an acknowledgement to be received in response. Effectively it stops and waits between sending to receive an acknowledgment before it sends more data. (Kurose & Rose 2003: 206-207)

In the sliding window protocol the sender is allowed to transmit multiple packets without waiting for an acknowledgment. However, it is constrained to have no more than some maximum allowable number, N of unacknowledged packets in the pipeline. The range of permissible sequence numbers for transmitted but not yet acknowledged packets can be viewed as a “window” of size N over the range of sequence numbers. As the protocol operates this window slides forward over the sequence number space. Flow control imposes some limit on the sender. An acknowledgement for packet with sequence number n will be taken to be a cumulative acknowledgement. (Kurose & Rose 2003: 217-218)

About Transfer Control Protocol (TCP)

Once a TCP connection is established the client process passes a stream of data through the socket. TCP directs this data to the connections’ send buffer. The send buffer is one of the buffers set aside during the initial three-way handshake. TCP “grabs” chunks of data from the send buffer and places this data in a segment. The amount of data that it can grab is limited by the maximum segment size (MSS). Because the send buffer receives data through the socket at 10 times the rate (S) than it can send data to the Internet R and the send buffer is only 1% of the size of the receive buffer, there must be some process to prevent the process in host A from continuously passing data into its socket at rate S bps.

By using congestion control a TCP sender limits the rate at which it sends traffic into its connection. Because the TCP receive window is so larger that the receive-window constraint can be ignored then flow control is not a factor that could limit the sending rate of the process at host A. Rather the sending rate is a function of the congestion window (CongWin) and thus can be adjusted via the congestion control mechanism of TCP. The way that this occurs is as follows.

The CongWin imposes a constraint on the rate at which the TCP sender can send traffic into a network. The amount of unacknowledged data cannot exceed the minimum of the congestion window. Assuming that there is no packet loss and timers never expire then the senders send rate is determined simply by a relationship between the perceived congestion and the Round Trip Time (RTT) from sending to receiving acknowledgments, this can be represented as $\text{CongWin}/\text{RTT}$ bytes/sec. By adjusting the value of CongWin, the sender can adjust the rate at which it sends data it its connection via the socket. In this way the sending host will establish an equilibrium sending rate which will maximise its throughput while ensuring that the transmission from the socket doesn't overflow the buffer. (Kurose & Rose 2003: 262-264)

With the selective repeat protocol, it is possible for the sender to receive an acknowledgment for a packet that falls outside of its current window.

If the packets send by a sender are received but the acknowledgement takes a long time to return to the sender the senders timer will timeout and result in it resending the packets. However after sending the packets a second time the sender receives the first acknowledgement (that was delayed) the senders window will move forward when as the acknowledgment has been received for the packet at the send_base of the window. However the receiver in the meantime receives the second copy of the packets and thus acknowledges their receipt by sending a second acknowledgement for those packets even though they have already been acknowledged. The sender will then receive a second acknowledgement for those packets even though the sliding window has moved passed the packets and they are outside of the current window. This is possible because “the receiver reacknowledges (rather than ignores) already received packets with certain sequence numbers below the current window base. (Kurose & Ross 2003: 222).

Is the alternating-bit protocol the same as the selective repeat protocol with a sender and receiver window size of 1

In the alternating bit protocol there are only 2 possible consecutive sequence numbers in any state. The alternating-bit protocol is the same as the Selective repeat protocol with a sender and receiver window size of 1 because the senders receive window would move forward one sequence number when a single acknowledgement was received. It could still operate (although with a slow transmission rate) if there were only two sequence numbers and with the minimal window size.

Describe the operation of the CSMA/CD medium access control protocol. Identify and discuss the features of this protocol that allow it to use the network bandwidth efficiently.

CSMA/CD is a partitioning protocol in that it partitions the code-space (as opposed to the time frequency) and assigns each node a dedicated piece of the code-space. An adapter using CSMA/CD protocol may begin to transmit at any time however it uses carrier sensing to prevent it from transmitting a frame when it senses that some other adapter is transmitting. It uses collision detection to abort transmission when it detects another adapter is also transmitting. Before attempting a retransmission the adapter using CSMA/CD waits some random yet relatively short amount of time. Ethernet adapters used by this protocol detect another transmission and possible collision by measuring the voltage levels before transmission. (Kurose & Rose 2003: 438 & 460)

The features of this protocol that allow it to use the network bandwidth efficiently include carrier sensing and collision detection as discussed above. There is another feature that is also very important and that is the transmission of a jam signal and exponential backoff, which occurs when aborting a transmission due to the detection of signal energy from other adapter while transmitting. This makes all other transmitters aware of the collision. The efficiency of CSMA/CD can be viewed in terms of the long run fraction of time during which frames are being transmitted on the channel without collision when there is a large number of active nodes, with each node having a large number of frames to send. If propagation delay is zero, colliding nodes will abort without wasting the channels bandwidth. (Kurose & Rose 2003: 461-462)

Describe the 802.11 architecture and identify the protocols used.

802.11 is a wireless LAN protocol that includes a number of standards. All standards of this protocol use the same architecture and the same MAC protocol. The primary component of the 802.11 architecture is the cell, which is also known as the Basic Service Set (BSS). A BSS contains one or more wireless stations and a central base station (STA). Multiple access points (AP) may be connected together to form a distribution system (DS). The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The AP functions as a bridge between the wireless STAs and the existing network backbone for network access. IEEE 802.11 uses the Media

4

By Verity Carney

Access Control (MAC) protocol, which is a carrier sense, multiple access protocol with collision avoidance. (Kurose & Rose 2003: 482 – 483)

Define frequency-division-multiplexing (FDM) and time-division-multiplexing (TDM). Compare and contrast FDM and TDM. What advantages does TDM have over FDM in a circuit-switched network?

Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM) are two techniques that can be used to partition a broadcast channel's bandwidth among all nodes sharing that channel. FDM divides the channel into different frequencies and assigns each frequency to each of the nodes. It thus avoids collisions and divides the bandwidth fairly among the nodes. TDM divides time into frames and further divides each frame into time slots. Each slot is then assigned to one of the nodes. When a node wishes to send a packet it transmits the packet's bits during its assigned time slot in the revolving TDM frame. In a circuit switched network TDM has a number of advantages. It eliminates collisions and is perfectly fair. In addition it can better support high bit-rate real-time traffic and multicasting, and when used as a link layer for IP networks, can provide Quality of Service guarantees. (Kurose & Rose 2003: 434-436)

Specify the differences between message confidentiality and message integrity? Is it possible to have one without the other?

Message confidentiality is a security feature that requires that third parties who are not the intended recipients of a message are unable to view the content of the message. Cryptography techniques allow a sender to disguise data so that an intruder can gain no information from the intercepted data. However the receiver must be able to recover the original data from the disguised data (Kurose & Ross 2003: 608)

Message integrity, whilst also having a security dimension, also requires that there is an assurance that a message is not modified after transmission en-route to its destination. It must be possible to prove that a message sent by a party was in the same form as originally composed and that it hasn't been changed by a third party before it arrives at the recipient's destination. Message integrity goes hand in hand with the need for achieving non-repudiation.

These two security issues require each other. Confidentiality necessitates some form of encryption as provided by means of cryptography techniques to ensure privacy and is inextricably woven into authentication, message integrity, non repudiation etc. Whilst it is possible to have integrity without confidentiality and visa versa these measures are both required for secure and official systems and communication especially in a networked environment that requires message transmission.

Define, compare and contrast symmetric cryptosystems and public key systems. Discuss the application of these two systems.

All cryptographic algorithms involve substituting one thing for another. Symmetric cryptography requires a single private key to both encrypt and decrypt data. Symmetric cryptography techniques are also referred to as block ciphers. Because any party that has the key can use it to encrypt and decrypt data, it is less secure than public key cryptography systems.

Public key encryption requires two algorithms one for encryption and the second for decryption. A public key cryptography requires each user to have two keys: a public key used by the whole world for encrypting messages to be sent to that user and a private key which the user needs for decrypting messages. (Tanenbaum 1996: 598)

Symmetric cryptography algorithms are normally faster than public key cryptography and are suitable for processing large streams of data. The disadvantage of symmetric cryptography is that it presumes two parties have agreed on a key and been able to exchange that key in a secure manner prior to communication. Symmetric algorithms are usually mixed with public key algorithms to obtain a blend of security and speed. One of the most widely used public key algorithms is RSA. Other schemes exist such as the elliptical curve algorithm. Cryptographic techniques are most widely used in high level design and use of secure email systems - ensuring confidentiality, integrity and authentication.

Provide a definition of the mono-alphabetic cipher.

The mono-alphabetic cipher is an advance from the Caesar cipher. It involves the substitution of one letter for another letter of the alphabet. Unlike the Caesar cipher it doesn't use an offset in a regular pattern. Instead any letter can be substituted for any other letter as long as each has a unique substitute letter. There are therefore 10^{26} possible pairings of letters rather than just 25. (Kurose & Ross 2003: 610)

Describe the concept of a digital signature and its role in providing integrity. Present the application of the different authentication techniques in digital signatures.

A digital signature is a cryptographic technique for indicating the owner or creator of a document, or to signify one's agreement with a document's content. Digital signatures provide integrity insofar as they are required to be verifiable, non-forgable and non-repudiable and that protects against later modification of the document (Kurose & Ross 2003: 627).

Different applications of authentication techniques include public key signatures using RSA algorithms which have become a defacto industry standard for digital signatures. An advance from RSA is the Digital Signature Standard (DSS). Message digests such as SHA-1 are also an example of a different digital signature application. These different application protocols use varying degrees of encryption techniques that include the use of either/or public and private keys in symmetrical and asymmetrical cryptography respectively.

Explain the reasons for using message digests in signing messages. Compare and contrast signing long messages with and without message digests.

Digests are an alternative to signature methods that can provide authentication but are not concerned with ensuring secrecy in the form of cryptography, which may not be required. Encryption and decryption are computationally expensive; the high overhead of

these can be unnecessary. A message digest is like a checksum. The message digest algorithms take a message, m , and protect the data such that if the message is changed (maliciously or by accident) then the message digest algorithm computed for the original data (and transmitted with the data) will not match and therefore the message integrity remains un-verified and un-authenticated. One of the major applications of the message digest function is the Secure Hash Algorithm (SHA). (Tanenbaum 1996) Long messages are better suited to digital signatures using message digests. A message that is too long for computationally efficient encryption, that is not of a highly confidential content, need not be fully encrypted. It is preferable then to use a message digest rather than public key digital signature as the latter can result in a greater overhead of computation when sending a long message.

Compare and contrast two digital signatures, one that uses a public-key encrypted message digest and another that uses the public-key encrypted message.

Both are a cryptographic technique used as a countermeasure against integrity attacks. They ensure that a message is verifiable, non-forgable and non-repudiable.

SHA-1 Secure Hash algorithm is an example of a public-key encrypted message digest. It produces a 160-bit message digest – a longer output length, which makes SHA-1 more secure than other message digests. RSA is a public key digital signature algorithm based on principles of number theory and Euclid's algorithm which uses asymmetrical public key encryption. A message digests as used in SHA-1 is computationally less expensive to encrypt long messages than the RSA signature. SHA-1 as a message digest is more efficient when complete encryption and decryption is not needed. Public key encryption used for encryption of the whole message by the sender. In the case of the RSA a Private key is required to decrypt message only known and used by the recipient. The private key cannot be deduced or derived from the public key. The RSA algorithm results in complete encryption and decryption and it thus is computationally more expensive and can be considered too slow for actually encrypting large volumes of data. Unlike the RSA algorithm, SHA-1 produces a fixed sized message digest (fingerprint) and functions like a checksum or a cyclic redundancy check – which is the same for all hash functions (Kurose & Ross 2003: 629-633).

Explain the basic concept of the PGP encryption scheme.

PGP is an acronym for Pretty Good Privacy. It is a high security RSA public-key encryption application for MS-DOS, Unix, VAX/VMS and other computers mainly used as an email encryption scheme. PGP uses a public-key encryption algorithm. PGP allows people to exchange files or messages with privacy and authentication. Privacy and authentication are provided without managing the keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on public-key cryptography. PGP encrypts data using the International Data Encryption Algorithm with a random key, and uses the RSA algorithm to encrypt the key. (Webnox 2003)

Firewalls could be classified as one of the security countermeasures or a network management tool. Present your reasons to support both claims.

A firewall allows a network administrator to control access between the outside world and resources within the administered network by managing the flow to and from these resources. It allows some packets to pass through an organisations internal network while blocking others. A firewall can be classified as a security counter measure in so far as it protects a network against malicious attacks of hackers or the contagion of viruses. At this level a packet-filtering firewall that operates at the network layer can ensure security countermeasures. On the other hand a firewall can be viewed as a network management tool as it can be used to manage and enforce security access policies. In this way the type of firewall that is used is an application-level gateway, which operates at the application layer. In so far as the filtering rules for firewalls are specified and set by the network administrator they can be classified as a dimension of network management. (Kurose & Ross 2003: 640-641)

References

Kurose, J & Ross, W (2nd ed) 2003 Computer Networks: A Top-Down Approach Featuring the Internet, Addison & Wesley New York

Tanenbaum, A, (3rd ed) 1996, Computer Networks, Prentice Hall New Jersey