Module 4

Communication channel that connect adjacent nodes along communication path as links. In order datagram to be transferred from source host to destination host it must be moved over individual links . Transmitting node encapsulates datagram in link-layer frame and transmits the frame into link.

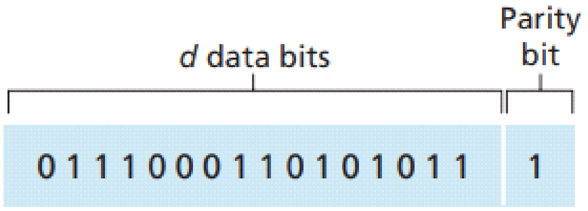
Services provided by link layer:

- Framing: almost all link layer protocols encapsulate each network-layer datagram within link layer frame before transmission over link.   frame consists of data field and number of header fields.
- Link access: MAC protocol coordinates frame transmission of many nodes when multiple nodes share a single broadcast link.
- Reliable delivery: guarantees movement of each network-layer datagram across link without error. A link layer reliable delivery service achieved with acknowledgements and retransmissions.
- Error detection and correction: many link-layer provide mechanism to detect bit error.

The link layer is implemented in network adapter also called network interface card.

Error detection and correction techniques

- parity checks: use of single parity bit.
  sender side:
  - In even parity scheme the information to be sent D has d bits(additional bit ie parity such that total no if 1s is d+1 is even
  - For odd parity bit is chosen such that odd number of 1s.

  Receiver side:
  - Receiver only counts no of 1s in d+1 bits. If odd number of 1valued bits are formed in even parity then atleast 1 bit error .
  - 

  - Sometimes errors are clustered together(bursts)probability of undetected error in this method is 50 percent.

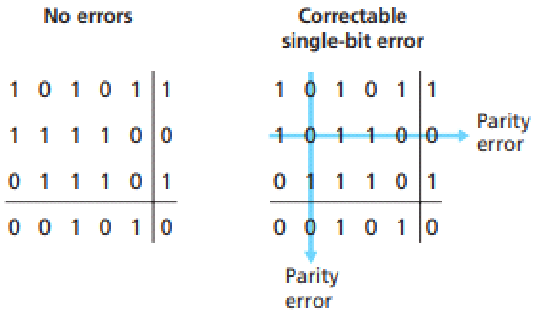
- Two dimensional :
  In a two-dimensional parity scheme, parity is calculated both across rows

and down columns in a data set, which is usually arranged in a rectangular format. This scheme allows not only the detection of a single bit error but also its location, and hence correction.

Here's how it works:

Error Detection: If a single bit error occurs in the original data bits, both the row and the column containing the flipped bit will have incorrect parity. The receiver can detect the error by checking the parity of each row and column.
Error Correction: The receiver can use the indices of the row and column with incorrect parity to identify the exact location of the bit that was corrupted. It can then flip this bit back to its original state, effectively correcting the error.

This method is known as Forward Error Correction (FEC). FEC techniques are valuable because they can decrease the number of sender retransmissions required and allow for immediate correction of errors at the receiver. This is particularly advantageous for real-time network applications or links with long propagation delays.

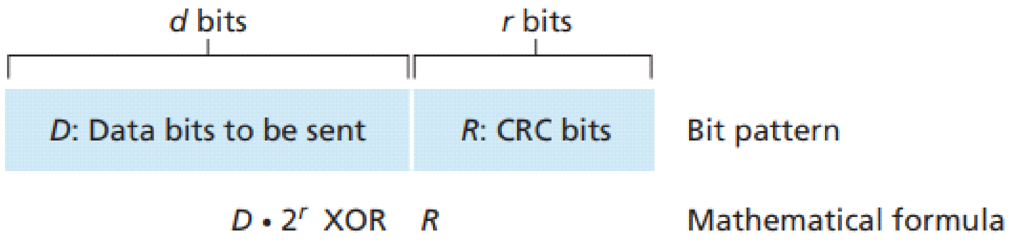


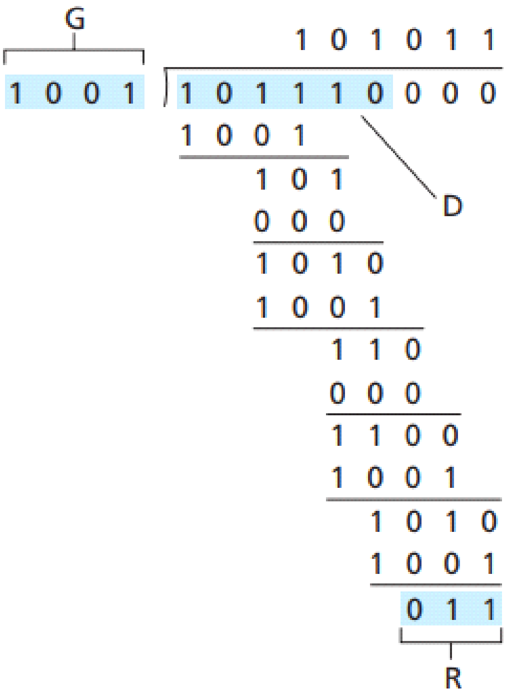
- Check summing methods: data is treated as sequence of k bit integers. In this simple method is sum of k bit integers and sum as error detection.
  - Internet checksum is based on this approach.
  - **Data as Integers**: Data is treated as a sequence of k-bit integers.
  - **Summing**: These integers are summed together.
  - **Internet Checksum**: The 1s complement of the sum is the Internet checksum, included in the segment header.
  - **Verification**: The receiver sums the received data (including the checksum) and takes the 1s complement. If the result is all 1 bits, no error is detected.
  - **Efficiency**: Checksumming requires little overhead, using only 16 bits in TCP and UDP.
  - **Implementation**: It's typically implemented in software within the host's operating system for speed and simplicity, whereas link-layer error detection often uses hardware for more complex operations like CRC.

- Cyclic Redundancy check(polynomial codes):
  - Widely used now
  - Working:
    - sender side- want to send data D with d bit ,first sender and receiver agree on r+1 pattern(generator,G) . Sender will send r with D such resulting in

sending d+r bit pattern and is exactly divided by G(no remainder)

- Receiver side: divides the d+r by G if remainder is non zero error is occurred.





- Multiple access links and protocols: this is to manage the broadcast link problem.
  - When more than 2 nodes transmit frames at same time and all nodes receive multiple frame at same time hence frames collide at receivers.
  - Random access protocols : transmiting node always transmits at full rate of channel . A method of this protocol is slotted aloha
    - Slotted aloha:
      The **Slotted ALOHA** protocol is a simple random access protocol with the following characteristics:

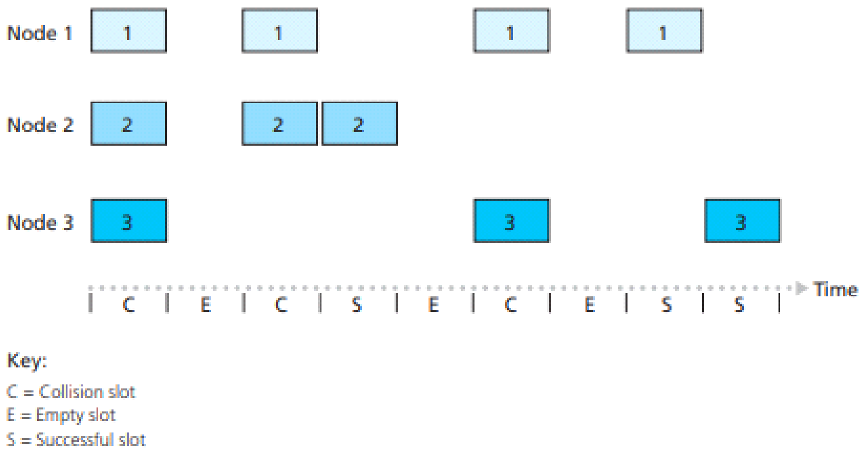
      - All frames consist of exactly **L bits**.
      - Time is divided into slots of size **L/R seconds** (a slot equals the time to transmit one frame).
      - Nodes start to transmit frames only at the beginnings of slots.
      - The nodes are synchronized so that each node knows when the slots begin.

- If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.

The operation of Slotted ALOHA in each node is as follows:

- When the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot.
- If there isn't a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame.
- If there is a collision, the node detects the collision before the end of the slot. The node retransmits its frame in each subsequent slot with probability **p** until the frame is transmitted without a collision.

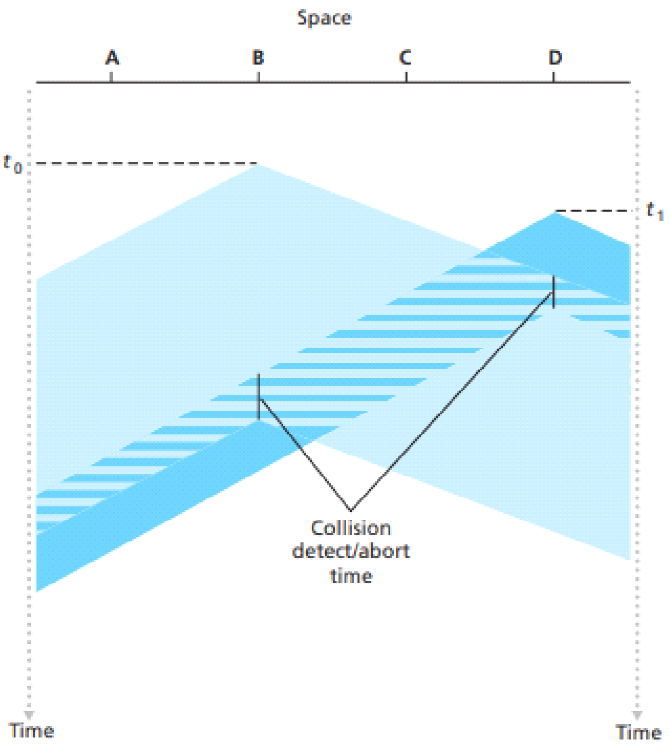
Slotted ALOHA has many advantages. It allows a node to transmit continuously at the full rate, **R**, when that node is the only active node. It is also highly decentralized, because each node detects collisions and independently decides when to retransmit. However, it requires the slots to be synchronized in the nodes.



The efficiency of a slotted multiple access protocol is defined to be the long-run fraction of successful slots (slots in which exactly one node transmits) when there are a large number of active nodes, each always having a large number of frames to send. However, when there are multiple active nodes, a certain fraction of the slots will have collisions and will therefore be "wasted." Another fraction of the slots will be empty because all active nodes refrain from transmitting as a result of the probabilistic transmission policy.

- Carrier sense multiple access(csma):

○



igure 5.13 ▲ CSMA with collision detection

Carrier Sense Multiple Access (CSMA) and CSMA with Collision Detection (CSMA/CD) are protocols where a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. In particular, a node neither pays attention to whether another node happens to be transmitting when it begins to transmit, nor stops transmitting if another node begins to interfere with its transmission.

The first question that might arise about CSMA is why, if all nodes perform carrier sensing, do collisions occur in the first place? After all, a node will refrain from transmitting whenever it senses that another node is transmitting.

This is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It's used to manage data transmission to avoid collision and improve efficiency. Here's a summary of its operation:

1The adapter gets a datagram from the network layer, prepares a link-layer frame, and puts the frame in the adapter buffer.
2If the adapter senses that the channel is idle (no signal energy entering the adapter from the channel), it starts to transmit the frame. If the channel is busy, it waits until it senses no signal energy and then starts to transmit the frame.
3While transmitting, the adapter monitors for the presence of signal energy coming from other adapters using the broadcast channel.
4If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame. If it detects signal energy from other adapters while transmitting, it aborts the transmission (stops transmitting its frame).
5After aborting, the adapter waits a random amount of time and then returns to step 2.

- Token based protocol:
  Token-Passing Protocol:
  In this protocol, there is no master node. Instead, a small, special-purpose frame known as a token is exchanged among the nodes in some fixed order. When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node.
  This protocol is decentralized and highly efficient, but it also has its problems. For example, the failure of one node can crash the entire channel, or if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.
  Examples of token-passing protocols include the fiber distributed data interface (FDDI) protocol and the IEEE 802.5 token ring protocol.
  These protocols are designed to manage the transmission of data in a network, ensuring that all nodes get a fair chance to transmit their data while avoiding collisions. However, they each have their own advantages and disadvantages, and the choice of protocol would depend on the specific requirements of the network.

- IEEE 802.3:
  IEEE 802.3, also known as Ethernet, is a set of standards and protocols that define Ethernet-based networks12. Ethernet technologies are primarily used in local area networks (LANs), though they can also be used in metropolitan area networks (MANs) and even wide area networks (WANs)12.

  IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks12. The standards are produced by the working group of the Institute of Electrical and Electronics Engineers (IEEE)1.

  Ethernet is generally a local area network (LAN) technology with some wide area network (WAN) applications1. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable1.

  IEEE 802.3 also defines a LAN access method using CSMA/CD (Carrier Sense Multiple Access with Collision Detection)1. This is a method for controlling a local area network on a bus structure2.

  There are several standards of IEEE 802.3 Ethernet. The prominent among them are 10BASE-T, 100BASE-TX, 100BASE-T4, 100BASE-FX, 1000BASE-T, and 1000BASE-X1. Each of these standards has different capabilities and operates on different frequency bands1.

- wireless (802.11):
  The IEEE 802.11 standard, commonly known as Wi-Fi, outlines the architecture and defines the MAC and physical layer specifications for wireless LANs (WLANs)12. Wi-Fi uses high-frequency radio waves instead of cables for connecting the devices in LAN12. Given the mobility of WLAN nodes, they can

move unrestricted within the network coverage zone2.

The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards1. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires1.

IEEE 802.11 uses various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands1. The protocols are typically used in conjunction with IEEE 802.2, and are designed to interwork seamlessly with Ethernet, and are very often used to carry Internet Protocol traffic1.

There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax13. Each of these standards has different capabilities and operates on different frequency bands1. For example, 802.11n operates on both 2.4 GHz and 5 GHz bands, while 802.11ac operates only on the 5 GHz band1.

- Cellular networks:
  co.+ellular Internet Access. This is a method of accessing the internet via cellular networks, which are ubiquitous in many parts of the world. The idea is to extend these networks to support not only voice telephony but also wireless internet access.

  The text you've shared discusses the evolution of cellular technology across different "generations". Here's a brief summary:

  First Generation (1G): These were analog Frequency Division Multiple Access (FDMA) systems designed exclusively for voice-only communication. These systems are almost extinct now.
  Second Generation (2G): These were digital systems initially designed for voice, but later extended (2.5G) to support data (i.e., Internet) as well as voice service.
  Third Generation (3G): These systems support both voice and data, with an increasing emphasis on data capabilities and higher-speed radio access links.
  The text also mentions the Global System for Mobile Communications (GSM), which is a standard developed to overcome the incompatibility of numerous analog cellular telephony systems. It has grown to be the dominant standard in the cellular telephone world.

  The goal of these technologies is to provide high-speed internet access that allows for seamless mobility. This means users can maintain their TCP sessions while traveling, and with sufficiently high upstream and downstream bit rates, they could even maintain video-conferencing sessions while roamin