Lecture 1 Terms: Introduction to Communication Systems

- **Noise** - Unwanted added signals from the environment. It disturbs the signal, and adds uncertainty at the receiver in terms of what the original signal was.
- **Channel** - An abstraction of the medium through which we communicate. In wireless this would be based on a signal that is propagated on a specific frequency with a protocol-defined bandwidth.
- **Data rate**: the number of bits transmitted from one device to another or over a network per second. Data rates are usually expressed in bits per second or bytes per second.
- **Preamble** - Used to tell receivers that a frame is incoming and they should start listening
- **Signaling** - General processes involved in establishing and maintaining a connection between users.
- **Error detection** - General framework to detect if received messages are correct. The result can be used to determine if ACK or NACK should be sent.
- **Parity check** - Using the parity bit, we can look for single bit errors.
- **CRC** (Cyclic Redundancy Check): an error detection technique to detect changes to raw data and is used widely in today's computer networks. In the cyclic redundancy check, a fixed number of check bits, often called a checksum, are appended to the message that needs to be transmitted. The data receivers receive the data, and inspect the check bits for any errors.
- **ACK/NACK** - Special messages used to ensure correct reception of messages, by telling the transmitter if they were or weren't successful.
- **Time Division Duplex (TDD)**- One way of allowing 2 users to communicate by splitting the channel up in timeslots in which the participants can transmit, or otherwise will have to receive.
- **ARQ (Automatic Repeat Request)** - A protocol used to ensure correction of incorrectly received packets. Different variants exists. When wrong packets are received they can be retransmitted
- **Sequence number** - Generally a number used to identify the packet. A protocol like ARQ can leverage it to determine which packet was lost
- **Packet** - Messages are often of a larger size, and are thus broken down into packets. Packets can be sent individually, but must all be received to extract the message.
- **Frame**: a simple container for a single network packet. A frame including 3 parts
    - header: contains instructions about the data carried by the packet
    - payload: the actual data that the packet is delivering to the destination
    - trailer: contains a couple of bits that tell the receiving device that it has reached the end of the packet ,and may have some type of error checking
- **Synchronous and asynchronous protocols** - Related to if the communication between sender and receiver occurs on a periodic level, i.e. the receiver knows when the next message will occur. asynchronous is related to protocols that allow a transmitter to send when they want. These 2 are also based on the periodic and event-trigger based communication.

Lecture 2 Terms: Simple multiuser systems and layered system design

- **Shared communication medium:** a medium or channel of information transfer that serves more than one user at the same time
- **TDMA** (time-division multiple access): is a channel access method for shared-medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots.
- **FDMA** (frequency-division multiple access): It works similar to TDMA, FDMA allows several users to share the same frequency channel by dividing the signal into different frequency slots.
- **Token-based**: control token passed from one node to next sequentially
- **Round-robin**: time slices assigned to each process in equal portions and in circular order, handling all processes without priority. In round-robin, each person gets an equal share of something in turn.
- **Pure ALOHA**: is a multiple access protocol for transmission of data via a shared network channel. Whenever a station has data to send, it sends the data. If, while you are transmitting data, you receive any data from another station, there has been a message collision. All transmitting stations will need to try resending later.
- **Slotted ALOHA**: An improvement to the original ALOHA protocol by discreting timeslots. A station can start a transmission only at the beginning of a timeslot, and thus collisions are reduced.
- **CAN** (controller area network): a method of serial communication, which supports distributed real-time control with a very high level of data integrity
- **OSI model** (Open Systems Interconnection model): describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. An OSI model includes 7 layers: 1) Physical layer, 2) Data link layer, 3) Network layer, 4) Transport layer, 5) Session layer, 6) Presentation layer, 7) Application layer.
- **TCP/IP** (Transmission Control Protocol/Internet Protocol): is a set of standardized rules that allow computers to communicate on a network such as the internet. The modern Internet is not based on OSI, but on the simpler TCP/IP model. A TCP/IP model includes: Network interface, Internet (IP), Transport, and Application.

Lecture 3 Terms: Network Infrastructure, Topologies, and Architectures

- **Throughput** - Total number of *correctly* transmitted bits over time. Bad channels leading to packet loss reduces the throughput.
- **Goodput** - Total number of *correctly useful* bits transmitted over time. Bad channels and overhead reduces this.
- **Packet loss** - The rate/probability at which a sent packet is lost in transmission.
- **Session** - sequence of messages exchanged between users
- **Switching** - how to deal with the different sessions that are being carried by the same subnet
- **Layering** - An abstraction of how different processes, and rulesets can occur at ones, “stacked” on top of each other. The goal is to make the system modular and flexible, by giving a layer a specific set of goal and purpose. Each layer will have their own metadata used for transmitting and receiving data.
- **Network Protocols** - Defines the methods and mechanisms necessary to achieve reliable communication between partners. Protocol headers are used here to add metadata that supports the functionalities of the layer in question.
- **Network systems** - The implementation of network protocols on multiple nodes, where the protocols enable communication between these.
- **Area networks (PAN, LAN etc.)** - A definition of the range of which the network should extend to.
- **Network Nodes** - A generic computing device that has a role in the process of the network. These could be routers, switches, users, firewalls and more.
- **Network Links** - Used to illustrate that nodes are connected, through some means. Could be physically connected (wires/wireless), or logically connected.
- **Network topology** - Can be seen from multiple perspectives, hence we can have a logical topology, and a physical topology. Therein are nodes that are connected through links to each other. In a physical topology nodes could be connected, but not in a logical topology, and vice versa.
- **Network Topology classifications** - The specifics can be seen in slide set 3 slide 39, but they are generally used to illustrate the logical structure through which nodes can communicate with each other. The physical representation can be very different from this.
- **Cloud computing** - Large processing capabilities with large data storage available. Used frequently on the internet. It is based on a centralization concepts, which is almost always available.
- **Edge computing** - Similar to cloud computing, but on a much smaller scale in terms of capabilities. It is also much more decentralized and thus more servers are closer to the sources of data, and different performance guarantees can be made.

Lecture 4 Terms: Networking and Transport Layers

- **Network layer:** transport segment from sending to receiving host. The network layer interfaces to the transport layer and the data link layer (OSI) / the host-to-network layer (TCP/IP).
- **Connectionless services**: modeled by the postal service with **no prior setup** and **no readiness to receive**.

- **connection-oriented services:** modeled by the phone service. This services need initial handshake to establish communication. Even if the network layer is connectionless, the transport layer can still be connection-oriented (e.g. TCP).
- **Routing:** purpose to ensure that packets are sent the best possible way through a (sub)net. Communication networks are extremely complex and need to consider a lot of metrics, so finding a good routing algorithm means finding a good path is very important, e.g., Dijkstra algorithm, distance vector algorithm, link state routing
- **IS-IS** (Intermediate System to Intermediate System): is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.
- **OSPF** (Open Shortest Path First): a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm.
- **Unicast**: one-to-one transmission from one point in the network to another point.
- **Broadcast**: one send to all
- **Multicast**: one send to a group
- **Anycast**: multiple nodes can have the response, so any response from them is fine
- **Transport layer:** end-to-end addressing based on port numbers. The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- **TCP connection:** TCP is connection-oriented, and a connection between client and server is established before data can be sent. The server must be listening (passive open) for connection requests from clients before a connection is established.
- **Congestion control:** preventing from overloading the network. Congestion appeared when “too many sources sending too much data too fast for network to handle”. TCP congestion could be handle by using
    - end-to-end congestion control
    - network assisted congestion control
    - AIMD (additive increase, multiplicative decrease)
- **TCP fairness:** Fairness measure is a great tool to determine if all the TCP flows are getting the fair share of the available network bandwidth. There are various transport layer protocols available, TCP fairness requires that a new TCP protocol should not affect the performance of other available protocols or variation of TCP itself.

Lecture 5 Terms: Introduction to security in communication systems

Security terms - General goals related to a security system, where these may not always be necessary, but a subset will generally in any multiuser system.

- **Authentication** - the communication parties want to be sure that the other party is indeed the one claimed.
- **Confidentiality** - only sender and receiver shall be able to read the transferred data.
- **Privacy/Anonymity** - personal information (including own identity) should not be revealed
- **Integrity** - assurance that data has not been changed on the way from the sender to the receiver.
- **Availability** - network and services shall be available whenever needed.
- **Non-repudiation** - a user cannot deny having used a certain service.
- **Legal requirements** - country specific legal security requirements (e.g.Legal interception, etc.)
- **Double spending** - ensure that digital money is spent only once (the main invention in Bitcoin).

Passive attacks - Attacks generally related to listening on open channels. These are not really detectable as they do not interact with the system, but simply observe and try to infer, based on the information available in the public open channel. This could be based on eavesdropping, and traffic analysis, or trying to decrypt . Normally the solution here is preventing it from being feasible.

Active Attacks - Attacks that would generally also be detectable. They are based on interacting with the system to achieve their goal. This can be more or less obvious such as Denial of service attacks, or masquerading as a legitimate user. Prevention is optimal, but will typically be difficult, hence detection can be used for human input in terms of understanding if an attack is happening or not.

Intrusion detection - The process/methods of observing the system itself, or incoming messages to detect if any malicious activity is ongoing in either. Normally an alarm would be activated probing a human to interact.

Cryptographic terms - Terminology associated with the practice of cryptography

- **Plaintext** - Original message
- **Ciphertext** - Coded message
- **Cipher** - Algorithm for transforming plaintext to ciphertext
- **key** – Secret information used in cipher known only to sender/receiver
- **encipher (encrypt)** - Converting plaintext to ciphertext
- **decipher (decrypt)** - Recovering ciphertext from plaintext
- **cryptography** - The study of encryption principles/methods
- **cryptanalysis (code breaking)** – The study of principles/methods of deciphering ciphertext without knowing key

Encryption - The process of taking data, typically in a plaintext, and apply a set of mathematical operation (the cipher), taking a unique encryption key as input through which the original message is scrambled. The goal being to make it difficult, ideally impossible, for outsiders to read the content unless they are the recipient.

Decryption - The process of unscrambling data from an encrypted message. Similarly based on a set of mathematical operations, which would also depend on some key, only the recipient should own. Otherwise cryptoanalysis should have been used.
Symmetric encryption - Uses symmetric keys, where both sender and receiver encrypt and decrypt using the same unique key.
Asymmetric encryption (Public key cryptography) - Uses 2 keys for the process of encrypting and decrypting. When sending a message from A to B, A would encrypt the message with B's public key. B would then decrypt the received message with its private key.
Block cipher - processes the input one block of elements at a time, producing an output block for each input block
Stream cipher - processes the input elements continuously, producing output one element at a time, as it goes along
One time pad - One time use symmetric key, which would have to be larger than the message being sent. Is the only provable security scheme that cannot be cracked.
Electronic code book - Essentially a look-up-table for plaintexts and mapping these to a unique ciphertext. They can be encrypted and decrypted individually, and will given the same plaintext always output the same ciphertext.
Cipher-block-chaining - Taking blocks and making the encryption and decryption dependent on the previous block. If blocks are lost then decryption cannot be continued
Digital certificate - A certificate which proves the ownership and authenticates the owner.
Digital signature - A signature which proves the integrity of a received message.
Certificate Authority (CA) - A trusted third party that we believe to be sincere, and trust when they sign a certificate.
Cryptographic hash function - A one way function which takes an input and gives a deterministic output. This makes the function useful to prove the authenticity of a message. A unique message would have a unique hash, but would be completely random in how the input and output are associated. A minimal change in the input may have great impacts on the output. It should be practically infeasible to recreate the original message from its output hash.

Lecture 7 Terms - Data link layer, packets, frames, coding and digital modulation

- **Data link layer:** the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer. Data link layer response to guarantee reliability communications, which is handle 3 problem
    - line discipline: who should send now?
    - flow control: how much data may be sent
    - error control: how can errors be corrected
- **Flow control**: refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment
    - stop and wait: send one frame at a time
    - sliding window: send several frames at a time
- **Error control**: includes error detection and correction.
- **BSC** (binary symmetric channel): a transmitter wishes to send a bit (a zero or a one), and the receiver will receive a bit.
- **FEC** (linear block code): a simple error control coding technique used for error detection and correction, where Information data is partitioned into blocks of length K pieces for example Information word.
- **Digital modulation**: the process of encoding a digital information signal into the amplitude, phase, or frequency of the transmitted signal.
- **ASK** (Amplitude-shift keying): a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal. The binary signal when ASK modulated, gives a zero value for Low input while it gives the carrier output for High input.
- **M-ASK** (M-ary Amplitude-Shift Keying): a symbol that represents $N = \log_2 M$ bits of information
- **PSK** (Phase-Shift Keying): bit streams are encoded in the phase of the transmitted signal
- **BPSK**(Binary Phase-Shift Keying): is the simplest form of PSK. It uses two phases which are separated by 180° and so can also be termed 2-PSK. It does not particularly matter exactly where the constellation points are positioned, and in this figure they are shown on the real axis, at 0° and 180°.
- **QPSK** (Quaternary Phase-Shift Keying): QPSK uses four points on the constellation diagram, equispaced around a circle. With four phases, QPSK can encode two bits per symbol.
- **QAM** (Quadrature amplitude modulation): QAM has two carriers, each having the same frequency but differing in phase by 90 degrees the information symbol modulates both the amplitude and phase of the carrier combination of PSK and ASK.
- **FSK**: the digital message is carried in the discrete frequency changes of the carrier. Similar to PSK, the simplest form of FSK is Binary FSK (BFSK).