PA197 Secure Network Design
1. Introduction

Eva Hladká, Luděk Matyska

Fakulty of Informatics

February 18, 2019

Content

Course Organization

- attending the lectures
- the knowledge acquired course materials will be published on the course webpage
- assessment methodology:
- course literature:
  - slides, RFCs, ...
  - literature being announced in relevant course parts

Course Overview

- the course goal:
  - to provide basic network architectures and functions
    - data transmission
    - end to end argument
    - routing
    - switching
    - ...
  - general requirements on the security and reliability
    - implication towards the architecture design
  - Network architectures from the point of secure
    - reliable design also in
    - ad-hoc/sensor networks
    - vehicular and/or mobile networks

Data Transmissions - Introduction

- **the main goal:** to ensure a transmission of bits (= the content of passed frames) between sender and receiver
- several standards (RS-232-C, CCITT V.24, CCITT X.21, *IEEE 802.x*) defining electrical, mechanical, functional, and procedural characteristics of interfaces used for connecting various transmission media and devices, e.g.:
  - parameters of the transmitted signals, their meaning and timing
  - mutual relationships of control and state signals
  - connectors' wiring
  - and many many others

Services - Data Transmissions

- *Bit-to-Signal Transformation*
  - representing the bits by a signal – electromagnetic energy that can propagate through medium
- *Bit-Rate Control*
  - the number of bits sent per second
- *Bit Synchronization*
  - the timing of the bit transfer (synchronization of the bits by providing clocking mechanisms that control both sender and receiver)
- *Multiplexing*
  - the process of dividing a link (physical medium) into logical channels for better efficiency
- *Circuit Switching*
  - circuit switching is usually a function of the physical layer
  - (packet switching is an issue of the data link layer)

Signals

- data is transferred (via transmission media) in the form of (electromagnetic) *signals*
  - the data have to be converted into the signals
- *signal* = a function of time representing changes of physical (electromagnetic) characteristics of the transmission media
- data that have to be transferred (0s and 1s) – *digital* (binary)
- signals spread through the transmission media – *analog* or *digital*
  - some media suitable for both analog and digital transmission – wired media (coaxial cable, twisted pair), optical fibre
  - some media suitable just for analog transmission – ether (air)

Transmission Media

- provide an environment for the functionality of physical layer
- basic distinction:
  - *guided (wired) media*
    - provide a conduit from one device to another
    - twisted pair (LANs, up to 10 Gbps), coaxial cable, optical fibre (backbones, hundreds of Gbps), etc.
  - *unguided (wire-less) media*
    - transfer an electromagnetic wave without the use of physical conductor
    - the signals are broadcasted (spread) via ether (air, vacuum, water, etc.)
    - radio signals, microwave signals, infrared signals, etc.

Multiplexing

- *multiplexing* – a technique of sharing an available bandwidth by concurrent communication channels
  - the goal is to maximize the utilization of the media
  - applied especially for optical fibres and non-wired media
- for analog signals:
  - *Frequency-Division Multiplexing (FDM)*
  - *Wave-Division Multiplexing (WDM)*
- for digital signals:
  - *Time-Division Multiplexing (TDM)*

End to End (E2E) argument

How to provide demanded functionality in computer networks?

- **End-to-End (E2E)** argument
  - application demanded functionality is possible to provide wit knowledge and by application
    - $\Rightarrow$ if it is possible, communication protocol operations have to be defined by realization only in communication system end nodes or in the closest distance
    - in lower system levels protocol function should be implemented only if performance increases.
  - suitable for applications demanding higher degree fidelity transported data and some latency is tolerated.
- **Hop-by-Hop (HbH)**
  - repeating specific functionality on the each two–point connection is possible to obtain increasing performance
  - it requires storing state informations on inside network nodes $\Rightarrow$ limited scalability
  - useful for applications,where minimize latency is more important then transported data fidelity, (e.g. real-time applications)

Routing

- the main goal of routing is:
  - to find optimal paths
    - the optimality criterion is a *metric* – a cost assigned for passing through a network
  - to deliver a data packet to its receiver
- the routing *usually* does not deal with the whole packet path
  - the router deals with just a single step – to whom should be the particular packet forwarded
    - somebody "closer" to the recipient
    - so-called *hop-by-hop* principle
  - the next router then decides, what to further do with the received packet

Routing – basic approaches

The basic approaches divide based on the routing table creation/maintenance:

- *static (non-adaptive)*
  - manually (by hand) edited records
  - suitable for a static topology and smaller networks
- *dynamic (adaptive)* – these respond to network changes
  - complex (usually distributed) algorithms
  - e.g.:
    - *centralized* – a centre controls the whole routing
    - *isolated* – every node on its own
    - *distributed* – nodes' cooperation

Routing – mathematical view

- the routing can be seen as a problem of graph theory
- a network can be represented by a graph, where:
  - nodes represent routers (identified by their IP addresses)
  - edges represent routers' interconnection (a data link)
  - edges' value = the communication cost
  - *the goal:* to find paths having minimal costs between any two nodes in the network

Routing – routing algorithms' required features

Required features of any routing algorithm:

- accuracy
- simplicity
- effectivness and scalability
  - to minimize an amount of control information ($\approx 5\%$ of the whole traffic!)
  - to minimize routing tables' sizes
- robustness and stability
  - a distributed algorithm is necessary
- fairness
- optimality
  - *"What should be treated as the best path?"*

Routing – basic approaches to distributed routing

Basic approaches to distributed routing:

- *Distance Vector (DV)* – Bellman-Ford algorithm
  - the neighboring routers periodically (or when the topology changes) exchange complete copies of their routing tables
  - based on the content of received updates, a router updates its information and increments its *distance vector number*
    - a metric indicating the number of hops in the network
  - i.e., *"all pieces of information about the network just to my neighbors"*
- *Link State (LS)*
  - the routers periodically exchange information about states of the links, to which they are directly connected
  - they maintain complete information about the network topology – every router is aware of all the other routers in the network
  - once acquired, the Dijkstra algorithm is used for shortest paths computation

Packet Switching

- Packet switching refers to protocols in which messages are divided into packets before sending and each packet is transmitted individually. Once all packets forming a message arrive at the destination, they are recompiled into the original message.
- Packet switching operation
  - Data are transmitted in short packets, typically an upper bound on packet size is 1000 bytes.
  - Each packet contains part of the user's data and some control information.
  - The control information should at least contain
    - destination address
    - source address
  - Store and forward - Packets are received, stored briefly and past on the next node.
- Advantages
  - Line efficiency - single node to node link can be shared by

Switching Technique

- Virtual Circuits
  - Pre–planned route is established before any packets sent
  - Call setup before the exchange (handshake)
  - all packets follow the same route and arrive in sequence
  - each packet contains a virtual circuit identifier instead of destination address
  - no routing decision required for each packet
  - clear request to drop circuit
- Datagrams
  - Each packet is treated independently with no reference to packets that have gone before.
  - Packets may arrive out of order
  - Packets may go missing
  - Up to receiver to re-order packets and recover from missing packets
  - More processing time per packet node
  - Robust in the face of link or node failures.

Circuit vs. Packet Switching

- Performance
  - propagation delay
  - transmission time
  - node delay
- Packet switching evolution
  - X.25 packet–switched network
  - router–based networking
  - switching vs. routing
  - frame relay network
  - ATM network

Switching vs Routing

- Switching
  - path set up at connection time
  - simple table look up
  - table maintenance via signaling
  - no out of sequence delivery
  - lost path may lost connection
  - much faster than pure routing
  - link decision made ahead of time, and resources allocate then
- Routing
  - can work as connectionless
  - complex routing algorithm
  - table maintenance via protocol
  - out of sequence delivery likely
  - robust: no connections lost
  - significant processing delay
  - output link decision based on packet header contents – at every node