Paper 1: MANET

What is the goal of the paper?

The goal is to identify issues with how research papers was been written and to raise awareness on how researcher can improve their paper.

This paper shows the current state of MANET research and the lack of consistency. It re-enforce the need for simulation study guidance.

What is the issue with "did not identify the simulator used in the research?"

This may hinder fellow researcher from repeating or reproducing the research work.

What is an Unbiased Simulation Study?

The results must not be specific only to the scenario used in the experiment.
The research should be design to use different scenarios.

What is a terminating and a steady-state simulation?

The steady-state simulation is reached when the output value does not change that much any more. The state is considered stable.

What is the problem with Scenario Development? What is the main statement of Figure 2? How should we fix the problem?

Different researcher used different scenario for their research. In order to have a close output or scenario, we need to agree on a base scenario.

What is the main challenge when Analyzing the Output of a simulation?

- Single set of Data: This pitfall happens when you take the first result of simulation and you accept it out rightly. It is usually not sufficient to run simulation once and take the result due to the random generator. It is good to repeat the simulation and observe how the randomness influence the result.
- Publishing

Question: What did you learn for your paper?

How to write papers, how not to be bias, how to do multiple simulations and not use single set of data.

Paper 2: HTTP over UDP: an Experimental Investigation of QUIC

What is the Goal of QUIC (Transport Layer Protocol)

It was to evaluate the capabilities of QUIC compared to existing protocols like TCP and SPDY.

What is SPDY and what is its main drawback?

SPDY is a transport layer network protocol and its secondary goals include reduced connection and transport latency, and bandwidth estimation in each direction to avoid congestion. Also helps in web loading faster.

How does it achieve this?

- it multiplexes concurrent HTTP requests on a single TCP socket;
- it compresses HTTP headers;
- it enables the server to push data to the client whenever possible;
- it allows prioritization among parallel requests.

Uses one socket but opens several http connections, for example, advertisement loads in concurrent with web browser and not after one another.

Drawback: Since it uses only one TCP socket to multiplex several http headers, if a packet is lost, congestion window and size of TCP socket is dropped and then the throughput for all the parallel HTTP data stream drops as well.

QUIC Implements Retransmission and Congestion at the application layer, why?

It enables QUIC to have control over data stream prioritization and thereby giving more control to the App layer.

Because chrome support it and makes it possible to do fancy things

What is a Connection Identifier (CID) in the context of QUIC.

CID is use to maintain connection while roaming. It takes functionality from the layers below and put it in App layer.

Helps establish connection quickly when for example we are roaming our mobile phone from home Wi-Fi to 4G or 5G without breaking our streaming. This is because CIDs are not IP based and do not need any handover between two networks can be transparently handled by QUIC without needing to re-establish the connection.

Why are packets getting lost at L=0?

This is simply because of the congestion control and queue algorithm in use. The algorithm need to adapt to the sending rate.

This is simply because of the congestion of the queue of packets and hence congestion control comes in.

Explain fig. 5d.

If you have a limited resource for connection, QUIC take more of your bandwidth for connection than TCP. This is why google feeds and search responses are quicker than other browsers if used in parallel. However, it does not lead to total starvation on TCP.

QUIC shows higher goodput.

Paper 3: ALTERNATIVE NETWORKs

What is the goal of this paper?

The goal is to provide alternative network to rural settlements and also provides classification and summary of the main characteristics of different alternative networks.

What is an alternative network according to the authors?

Alternative Networks are considered those that share some of the following characteristics:

- They have a relatively small scale.
- They may follow de-centralized approaches.
- The investment in infrastructure may be low, and may be shared by independent users, commercial and non-commercial entities.
- Users may be involved in the design, deployment, maintenance and daily operation of the network.

What is Digital Divide?

It is the process where the people of the earth are divided from their capabilities to use digital infrastructure. For example, Africa find it difficult to use digital infrastructures like the internet, cell phones, tablets, computers…etc.

The earth in this context is divided Global North and Global South

What is the difference between a primary and a secondary user for TV white spaces?

Primary user = licenced users or licenced broadcasters or main owner of the spectrum.

Secondary users = Allowed to use the spectrum on a non-interfering basis, or when the spectrum is not being use by the primary user.

What is the shared infrastructure model?

This has to do with coming together of a community and private investors to bring connectivity to users.

The investor already has an existing infrastructure and is willing to bind with the local community to get connectivity to a certain point and thereafter the community extends the connection to the users.

PAPER 4: TEGOLA TIERED MESH NETWORK TEST BED IN RURAL

What is the goal of this Paper?

The goal was to deploy a rural WiFi based long distance mesh network testbed in the Scottish Highlands and Islands using solar or wind to power their nodes.

They highlight the unique aspects of their testbed that differentiate it from other existing rural wireless testbeds. They also outline some of the research issues that are currently being investigated in this project.

What is special about the Tegola Testbed compared to other works?

It is the radio propagation over water (sea) and the combination of different renewable power sources like wind and solar which are stored in batteries to power the testbed.

What is the influence of the Tidal level to the signal strength?

The tidal level creates constructive or destructive signal interference with the received signal. This leads to varying signal strength and this could be due to TwoRayPathLoss Model.

What is the possible solution the authors propose for the varying signal strength?

They introduced spatial and antenna diversity by deploying 2 radios to propagate both horizontal and vertical polarization at both end and thereby achieving a linear signal level.

Paper 5: TOKEN BASED MAC for Long Distance IEE802.11 p2p Links

What is the goal of this Paper?

The goal is to minimize the idle time and provide an aggregated link throughput close to the physical datarate.

Independence of distance, lowered delay, jitter and better fairness.

The protocol design focuses solely on the token exchange on a single long distance link

How does propagation delay affects transmission?

The sending station has to wait longer for ack to arrive.

Slot time which defines the carrier sensing interval during the backoff has to be increased

The station holding the token is able to transmit specific amount of data, when done with the transmission, the token is passed to the next station.

In this protocol no backoff is needed since the stations on the link is either in receiving state or token holding state.

- The state machine of Token Based MAC

- Data exchange phase (Tx and Rx states)
- Synchronizing phase (Syn and wait state)

Paper 6: An experimental comparison of routing protocols in multi hop ad-hoc networks

What is the goal of this Paper?

The goal is to compare 3 routing Protocols (OLSR, Babel, and Batman) in respect of their performance and overhead/throughput. Where do these throughputs come from and what make these protocols more efficient.

What can overhead of Protocol mean?/what do we measure if we want to measure overhead?

- The writer focuses more on the extra airtime which is a key in the performance of a routing protocol.
- However, the paper talks about more overhead;
- amount of extra data (bytes)
- route convergence
- memory size / routing table
- number of extra packet.

What is the drawback of this paper?

They compared mesh routing protocols, without mobility and without routing.

Paper 7: IEEE 802.11s: the WLAN mesh standard

What is the goal of this paper?

The goal is to provide insight into the development of 802.11s standard.

What was the motivation for developing the IEEE802.11s Standard?

The motive is to provide routing capabilities at MAC layer (layer 2)

When IEEE802.11 is used in a Distribution System (DS) what is difference between source/destination and transmitter/receiver addresses?

- Source address indicates the station that generated the frame (initial hop), and the destination address indicates the intended receiver (final hop) i.e, it remains unchanged across the network path.
- Transmitting and Receiving station addresses, is the hop address forwarding the frame and it changes from hop to hop.

Why does IEEE802.11s has the need for six addresses?

The 2 additional address bits provides support for proxied stations to send traffic to and from the mesh network i.e. it denoted “To DS” and “From DS” which indicates traffic is entering or leaving the Distribution system (DS) from a Base Service Set (BSS).

Why does the throughput decreases rapidly with the number of hops in the fully connected topology of their experiment?

I think it has to do with the slot time, congestion and the way CSMA/CA is designed.

Paper 8: PROGRAMMING PROTOCOL-INDEPENDENT PACKET PROCESSORS

What is the goal of this paper?

The goal of the paper are to make network devices;

- Reconfigurability in the field: Programmers should be able to change the way switches process packets once they are deployed.
- Protocol independence: Switches should not be tied to any specific network protocols.
- Target independence: Programmers should be able to describe packet-processing functionality independently of the specifics of the underlying hardware.

What is the main motivation behind P4?

Is to use P4 to program network devices (switch ASICs, routers,)

To use P4 for to program the parser, tables, and control flow

P4 provides the developer with a basic set of instruments to implement a network stack in switching hardware.

What is the difference between P4 and OpenFlow?

OpenFlow is designed for SDN networks in which we separate the control plane from the forwarding plane,

P4 is designed to program the behaviour of any network devices (switch or router), whether it's controlled locally from a switch operating system, or remotely by an SDN controller.

What do the authors want to show with the mTag example?

The want to show how to combines the hierarchical routing of PortLand with simple MPLS-like tags

LECTURE 1:- NETWORK ANALYSIS TECHNIQUES

Modelling: Mathematical Analysis
Emulation: HW components that behave like real systems (Hardware & Software)
Simulation: Model the system at abstract level
Experimentation: Experiments using testbed. Real life (Best Solution)

Emulation always work with real time clock, while simulation can be done in milli seconds or hours.

Reasons for Simulation:
Scalability, Repeatability, Education, Predication

Limits of Simulation: Energy consumption, Hardware specific limits are difficult to simulate, Hardware variations

Xteristics of good simulations: Repeatability, Unbiased, Rigorous, Statistically Sound.

LECTURE 2 (Read before exam)

LECTURE 3:- Backhaul Technology

Wireless **backhaul** is the use of wireless communication systems to transport data between the internets and subnetworks. ... One example of wireless **backhaul** is a smartphone that connects to the internet by receiving data from a cell tower or another kind of base station

Barriers for Internet Adoption

- Affordability,
- Ability…cannot set up the system

Network Architecture:

- Backbone: Fibre tech, satellite, p2p wireless 24GHz (Connect cities, national level, high speed)
- Backhaul Close to the customer <100km ||point to point wireless, (Regional level, closer to the customer) || Fibre, Satellite techs
- Last Mile <1km|| Airborne, Fibre, 4g/5G wifi, customer level

CAPEX is the initial cost of setting up a project and OPEX is the operating cost

Difference between Cable Television and digital Subscriber Line (DSL)

DSL Tech uses copper wire while CATV uses coaxial cable
DSL uses Star topology while CATV uses Bus topology.
DSL link capacity is not shared while in CATV link capacity is shared

FIBRE

Transmission rate of up to 100 GBit/seconds even on long distances

Why is it costly to deploy fibre tech?

Answer: It is expensive to deploy the technology because there are already existing techs that are being used by the ISP and the digging is tedious and it expensive to lay the fibre.

Methods of deploying Fibre: Aerial, Digging once, micro-trenching.

Cellular/Mobile Network (2G/3G/4G/5G)

What is the problem of going all wireless?

Sharing the capacity, p2p architecture is being used where each mobile phone is served by one base station.

Base station requirement to be effective: Stable electricity, high speed connection to the backbone, exposed location because the medium is air.

The higher the frequency, the lower the coverage range.

What is a bandwidth?

Bandwidth is the amount of data that can be transferred from one point to another within a network in a specific amount of time. It is measured in bits per second.

TV White Spaces

The term **white spaces** are frequencies allocated to TV broadcasting services which are no longer in use at certain places but may be available for internet purposes.

DIRECTIONLESS WIRELESS

- P2P Links
- Cost effective wire like alternative in the Backhaul to connect Last Mile techs to the backbone
- Different bands 5GHz, 24Ghz

Wi-Fi Mesh/ Hotspot

Wi-Fi at 2.4 and 5GHz are Meshed together. Just like bringing backhaul wireless mile tech to other places. To do this, put routers in close proximity to the already existing GATEWAY network, then the MESH protocol will connect automatically to the next gateway.

Advantages: Can be easily deployed. Decentralized protocol design.

Disadvantages: You always have disconnection due to interferences. Not easy to scale.

GEO Satellites

If satellites can transmit TV channels to our homes, then they should be also to stream internet to our homes. Why is it not happening now?

Satellites are at **35700km** above in the sky, so we have to transmit signals to that distance and then transmit them back which **makes** the latency lag.

Alternative Networks

Google Project Loon, Facebook Aquila, OneWeb, SpaceX

Satellites

Medium Earth Orbit (MEO) & Low Earth Orbit (LEO)

- They are not high enough, so they cannot cover big areas
- Bandwidth will be around 55.4kb per person, so more antennas will be needed
- Causes trash in the space (Space Debris)

Drones and Balloons

Drones need energy to stay up to provide networks, solar energy is not enough

Very large and very expensive

Balloons

They are drifted by the wind, so they cannot stay over a particular country

LECTURE 4:- Alternative Networks and WIFI Based Long Distance Networks (WiLD), Physical Layer and Propagation

Wireless Point to Point Communication

Wireless communication is the transfer of information between two or more points that is not connected by an electrical conductor, using electromagnetic waves.

What are electromagnetic waves? These are radio waves inform of electric and magnetic waves combined together. And what is their speed? 3*10^8m/s

There are vertical and horizontal polarizations. **Magnetic polarization** occurs when an external **magnetic field** is applied to a material with elementary magnets.

Important Effects:

Free-Space Path Loss (FSPL): The path loss depends on the frequency and the distance, just because the wave spreads, so it loses energy.

Reflection: Reflection of electromagnetic waves occurs when propagating electromagnet waves impinges upon an object which has very large dimensions when compared to the wavelength of the propagation wave

When a wave incidents on a surface, some are reflected while some are absorbed into the medium(Refraction). **Property of the incident material and Angle matters,** and Snell's law of refraction comes in, (Sin i/Sin r)

Diffraction: A radio waves that meets an obstacle has a natural tendency to bend around these obstacles. This bending is called diffraction, results in change of direction of part of the wave energy from normal line of sight.

Earth curvature:

Weather Conditions:

LECTURE 5:- HARDWARE AND LINK BUDGET

Hardware for WiLD: WIFI Based Long Distance Networks (Not for over 10km)

a. **Embedded Boards.**
   IP64-IP67 (Durst and water resistance)
   External Antenna Connectors
   Power over Ethernet

b. **IEEE802.11 Transmitter (WIFI Cards)**
   Transmisson power P_{TX} - Output power that come out of the transmitter.
   Sensitivity $RXLevel_{min}$ - Defines the signal to noise ratio at the receiver which is needed to decode a certain modulation. The more complex the modulation, the lesser the P_{TX} and the higher the $RXLevel_{min}$.

c. **High frequency Cables: Important factors are prices, frequency, length and diameter.**
   Cables connecting at high frequency will lead to attenuation for the signals
   The higher the frequency, the more loss in db of receiving and transmitting power
   Ecoflex 15
   Ecoflex 10

d. **Antennas and Masts:** Impedance, Polarization, Antenna Gain

LINK BUDGET

$P_{RX} = P_{TX} – L_{C,TX} + G_{TX} – L_P + G_{RX} – L_{C,RX} >>> RXLevel\ (min)$

Power at the receiver antenna must be greater than the power than the min sensitivity for a certain modulation

EQUIVALENT ISOTROPIC RADIATED POWER

EIRP(dBm) = Ptx – Lc,tx + Gtx (Power minus cable loss plus antenna gain)

LECTURE 6:- Wild MAC and Throughput Enhancement

Medium Access Control with CSMA/CA

Carrier Sensing Multiple Access / Collision Avoidance (CDMA/CA)
Transmitting and Receiving at the same time is difficult for Wi-Fi.
Transmitter has more power and it is mostly half duplex.

The medium which implement CSMA/CA for 802.11 is called **Distributed Coordination Function** (DCF). It coordinates access to the medium among distributed clients without a centralized entity
Contention Window Count if the medium is free. Transmission allowed when counter reaches zero i.e. it uses random number to decide the next transmitter.
Distributed Interference Space (DIFS) It is the time delay for which sender wait after completing it’s backoff.
Airtime/Propagation Time: For long-distance WiFi links, the propagation time of a packet leads to unwanted timing effects in the protocol
802.11a✉5gHz ✉54mb/s
802.11n ✉2.4gHz

WiFi MAC Problem

- The Hidden Node Problem:- When 2 AP that are not in the same transmission range tries to transmit to a 3rd AP, there will be collision domain at the 3rd AP because AP 1 and 2 are not aware of eachother.

- Virtual Carrier Sensing Function:- Virtual Carrier Sensing Function solves the above problem by using Request to send (RTS) and clear to send (CTS) with network allocation vector (NAV)

- The Exposed Terminal Problem:-

WiFi MAC Problem on long-distance links

Unwanted timing effect:- When ACK timeout and the packets are not received, it assumes that the packet is lost

The Slot time and ACK timeout was adapted to solve the unwanted timing effect.

OFDM Enhancement

For 802.11a, 20MHz with 53 sub carriers was allocated and only 16.5625MHz came out because of interference from neighbour channels
For 802.11n, 20MHz with 57 sub carriers was allocated and only 17.1825MHz came out because of interference from neighbour channels

MAC-Layer aggregation - A-MPDU vs. A-MSDU

A-MPDU was used and Selective acknowledgement through a single Block-ACK.

The problem with MAC-Layer aggregation is delay and jitter.

MIMO and How It Works
SISO✉Single Input Single Output (Single antenna transmitting and single antenna receiving)
y= h*x+z
MIMO✉We don't have just one antenna but two antennas transmitting and two antennas receiving
MiMo works polarization (Horizontal and Vertical)
Frequency channel is increased to 40MHz
How to decorrelate signals on long-distance WiFi-Links

- Spatial antenna diversity
- Force Multipath propagation due to a reflection

LECTURE 7:- Wireless Mesh Networks

A mesh network is a topology in which each node relays data for the network
In a full mesh, every node is connected with every other node sender to receiver

Ad-hoc On-demand Distance Vector Routing Protocol (AODV)

- It is a Re-active distance-vector routing protocol i.e. route are created when needed.
- It supports mobile and static route.
- If a source wants to send traffic, it sends a Root Request (AODV-RREQ) and broadcast it all concern nodes. Intermediate route creates a reverse route and the destination sends a Route Reply (AODV-RREP)

Advantages	**Disadvantages**
no overhead	There is waiting time

Optimized Link State Routing Protocol (OLSR)

- It is proactive.
- It uses Multipoint Relays (MPR) to reach all 2-hop-neighbours
- Forwarding path is not shared among all nodes (except among MPRs only)

OLSR MPR Selection
It uses Expected Transmission Count (ETX) for path calculation
Hello are sent to 2-hop-neighbours.
It uses Traffic control Messages (TC) to generate and forwarded by MPRs.
It used announce host-network-associations (HNA)

Advantages	**Disadvantages**
Proactive	Slow to initialize
	Routing loop
	Low throughput

B.A.T.M.A.N

- Node only needs to know the next hop towards a destination.

- Network topology remains unknown.
- Originator: node that generates OGM broadcasts.
- OGM default interval is 1 sec.
- Path selection is based on max throughput and recent OGMs.
- (Internet-)Gateways are connected via tunnels and remain the same in case of changing links

LECTURE 9:- SOFWARE DEFINE NETWORKING

Software-defined networking (**SDN**) is the segregation of data plane, control plane and management plane from physical network devices.

SDN is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring

SDN is divided into 3 different planes.

- **Data Plane:** Processing and delivery of packets with local forwarding states (Moves packets from input to output in 10 ns) eg. Switching, IP forwarding
- **Control Plane:** Determines how packets should be forwarded. Eg software based and uses a CPU (it moves data 10 ms to 10 s)
- **Management Plane:** Methods of configuring the control plane (Using CLI), Simple Network Management Protocol (SNMP) E.g Human-centric, traffic engineering. Conf. of VLANS, MPLS(Multi Protocol Label Switch)

When the switch receive on unknown traffic, it forwards it to the SDN controller and if is a new traffic, the SDN forwards it to the root controller to work on it.

SDN makes it possible to configure network devices without using console cables.

Challenges of Traditional Network Architectures

- Hardware-centric.
- Very complex to manage.
- Control Plane and the Data plane are bundled inside the networking device.
- Each network device is configured manually should changes need to be done.

How does SDN Improves on Traditional Network Architecture?

- Separates the control plane and data plane from networking devices.
- Network switches become forwarding devices
- Control logic is implemented in a logically centralized controller.

Management Plane is configured via the **Northbound interface**
Network devices are configured via the **Southbound interface.** According to the rules in the SDN controller. Its is a down forwarding device.

OPENFLOW

It is a way to define **Southbound interface**.
It is an open API that provides standard interface for programming the data plane switches.
The data path consist of flow-tables and actions associated with the flow entry.

OpenFlow Logical Switch: The switch is connected to the controller using an emulator like mininet and the controller managed the switch using OpenFlow Manager via OpenFlow switch protocol

OpenFlow uses out-of-band connection which means the network connection between the network device and the controller is not controlled by the SDN contoller.

SDN Challenges

- **Controller Placement and connection, reliability and stability**. (If controller is down, all network devices are down because they do not know what to do, hence, the controller has to stay up, it need to have a reliable and redundant connection. Hackers will target this to take it down, which may lead to single point of failure)
- **Scalability: One controller, how many nodes?**
- **Fault Tolerance: What happens if the controller breaks down?**
- **Security: SDN controller and OpenFlow Manager/Protocol are targets.**
- Many new ways to mess up a network

SDN vs. Network Function Virtualization (NFV)
Flexible forwarding and steering of traffic in a physical or virtual network environment while NFV is the Flexible placement of virtualized network functions across the network e.g Firewall, OSPF etc.

LECTURE 10:- LoRa(WAN)

LoRa (Long Range) uses the License-free ISM frequency bands below 1GHz but regulated duty cycle.

- Duty cycle is define as how many percent of signal we are allowed to transmit
- Long range
- Low power
- Low cost
- It is

LoRa	**LoRaWAN**
Is a wireless communication technique i.e Physical layer: No specified encryption, routing, topology. Uses a spread spectrum modulation technique	Is an open specification developed and maintained by the LoRa Alliance for the upper layers Defines protocols to manage and route the

	communication between sensors and applications.
Builds upon the general idea of Chrip Spread Spectrum (CSS)	Typical components in the hierarchy of these networks are sensors, gateways, network server and application server

LoRa - Chirp Spread Spectrum

- A chirp is a signal whose frequency increases or decreases over time.
- A full up-chirp is a signal sweeping from the lowest to the highest frequency of the allocated bandwidth.
- Spread Spectrum is great for low SNR's.

LoRa – Limitations

- Airtime in magnitude of seconds and Bitrate in the magnitude of kbps.
- Duty cycle limitations: Especially for the Gateways.
- Spreading Factor: Trade throughput/latency vs. range.
- Bandwith: Trade throughput vs. range.

LoRaWAN - Network overview

- **A sensor (End Nodes)** gathers data which is transmitted to one or multiple gateways via LoRa.
- **Gateways** simply decode and forward the data to a network server using an arbitrary backhaul technology.
- **Network server:** security checks, handling of redundant packages.
- Afterwards encapsulates the messages and forward it to the final destination called **application sever**.

A topology can be described as several interconnected stars with multiple gateways at the center of these stars connections.

LoRaWAN - Network Classes

Class A:- Connection initiated only by the end devices.

Class B:- It has multiple Rx times, Time sync required (eg GPS), low latency, multicast possible.

Class C:- Continuous RX time, No additional downlink latency, High energy consumption.

LoRaWAN – Security

Two different layers of security.

- Between sensors and the network sever to ensure the authenticity/integrity (MIC)
- End-to-end encryption between the sensor and the user application.

LoRaWAN - Activation Methods

Every End-Device needs to join a network. There are two different possibilities:

Activation by Personalization (ABP)	**Over-The-Air-Activation (OTAA)**
The network session key, application session key and device address are build in when the device is manufactured. Devices can not change the network. Key material can not be updated. No downlink required.	A DevEuI, an APPEuI and an AppKey are build in when the device is manufactured. When the device is turned on it will start a join procedure where it negotiates a new set of keys based on the existing AppKey. More complex and consumes airtime.

LECTURE 11:- Blockchains

A blockchain is a network based on a distributed transaction database for a tamper-proof storage of linear records.

The stored data is protected against unauthorized manipulation by cryptography, decentralization and game theory.

However, the overhead a blockchain is very high compared to a centralized database. The possible application should be questioned critically.

Who manages the credit of the participants?
Each participant manages each credit!

02 P2P-protocol

Transition from a hierarchical bank protocol to a flat P2P-protocol

Rules:

- Each participant manages Each credit of all participants in own credit database
- To transfer credits, participants send signed transactions to all participants.
- Each participant accepts only valid transactions
- Each participant updates all balances according to accepted transactions

Problem:

- Each participant can manipulate their own database as they wish.
- Manipulation of other databases through so-called replay attacks
- Replay attack:

  - Attacker can resend received transactions
  - Recipients verify authenticity only by the signature
  - All participants (except the victim) will accept the transaction

Solution:

- Each participant does not store credit as a mere value.
- Credit is stored as a quantity of digital assets (coins) with unique serial-numbers.

03 Serial-number-protocol

Introduction of coins with serial-numbers to protect against replay attacks.

Rules:

- Each participant manages serial-numbers of coins of all participants in their own credit database
- To transfer credits, participants send signed transactions to all participants
- Each participant accepts only valid transactions
- Each participant updates balances according to accepted transactions

Problem:

- Still (but limited) vulnerable to replay attacks
- Attacker can successfully resend received transactions if the victim has regained possession of the coin

Solution:

- A coin requires not only a serial-number but its entire transaction history

04: Transaction-protocol

Reinterpretation of credit balances as transaction history

Rules:

- The Credit is the transaction that transfers the coin.
- The payee (receiver) of a transaction is the owner of the credit.
- Each participant manages list of all transactions in his own transaction database.
- To transfer credits, participants send signed transactions to all other participants.
- Each participant accepts only valid transactions.
- Each participant updates its transaction database according to accepted transactions

Problem:

- Replay attacks are no longer possible due to the transaction history
- But credit balances can still be issued several times.
- Attackers can send self-signed transaction multiple times, simultaneously or selectively which is the famous **Double-Spending-Problem**.

Solution:

- It must be impossible to send transactions selective to different participants
- Each transactions sent, must reach all participants
- Transactions must be validated in advance
- Randomly selected protocol validators must perform this task

05: validator-protocol

Random selection of network or protocol validators

Rules:

- Each participant is a potential validator
- Participants update their transaction database not immediately
- Participants first collect all valid transactions in a so-called transaction pool (intermediate storage)
- After a temporary validator is randomly selected, its transaction pool is signed and sent to all participants
- Each participant then validates the signature and the received transactions of the validator
- Each participant discards its own transaction pool and updates its transaction database

Problem:

- Restricted to evil validators, but still vulnerable to double-spending.
- If the attacker becomes a validator himself, he can perform a double-spending attack
- Can the random selection of validators be influenced?
  - Yes, by doing a so-called Sybil-Attack
- Sybil-Attack:
  - Influencing a network by creating several false identities.
  - An Attacker can execute the protocol-software on any number of network nodes and clone himself several times.
  - Using this approach, the attacker can become the validator nearly all the time.
  - Attacker possesses centralized power

Solution:

- Periodic selection of validators on the basis of unforgeable characteristics.
- Need for identification features that can not be reproduced with little effort.

06: Proof-of-Work-protocol

Identification using computing time performed: Proof-of-Work (POW)

Rules:

- Each participant is a potential validator and collects valid transactions in its transaction pool
- Each participant works continuously on the so-called Hashcash puzzle
- Each participant uses its transaction pool as input value for the calculation
- As soon as a participant solves the puzzle, he becomes a validator and sends his transaction pool together with the solution to all other participants
- Each participant then validates the solution (Nonce) and the transactions received from the validator
- Each participant discards its transaction pool and updates its transaction database

Problem:

- Sybil-attack/Double-spending has become very costly

- The more participants are involved in the Proof-of-Work calculation, the less likely individual selection becomes.
- A common competition is created - Game Theory.
- The network will split into incompatible sub-networks (Forks)
- Consensus is not assured

Solution:

- Short-term acceptance of inconsistent data by forks.
- Network must be able to reorganize consensus independently.

07: Blocklist-protocol

Chronological sorting of Proof-of-Work and transaction data in units of blocks using a hash-linked list.

Rules:

- Each participant is a potential validator and collects valid transactions in its transaction pool
- Periodic selection by computing a so-called Proof-of-Work
- Each participant uses its transaction pool and the hash value of the previous block as input value for the calculation
- As soon as a participant solves the calculation, he becomes a validator and forms a block consisting of:
    - Transaction pool + hash value of previous block + solution (nonce)
- The validator sends his block to all other participants
- Each participant then validates the block of the validator

Advantages using these hash-linked block list:

- Blocks have a fixed chronological order.
- Previous data inside the blocks cannot be manipulated unnoticed.
- Each new block implicitly confirms all previous blocks and thus also all previous transactions.
- Each block secures all previous transactions through Proof-of-Work.
- Therefore each block is considered a transaction confirmation
- The longest block list is the only valid one

Solution:

- The probability of Forks must be further reduced.
- It must be ensured for a transaction not to be rejected by reorganizations.
- To confirm a transaction safely, a certain time must be waited.
- Each subsequent block increasingly secures previous transactions.
- After a certain number of subsequent blocks, a transaction is considered final or confirmed.

08: Blocktime-protocol

The greater the inter-block time in relation to the block propagation time, the less likely is the repetitive formation of Forks.

If the block chain parameters (block size and inter-block time) are chosen sensibly, network Forks can reorganize itself and finally find a consensus.

Problem:

- The inter-block time is defined by selecting the Proof-of-Work difficulty.
- For a stable network the inter-block time should be longer than the block propagation time
- How can the inter-block time be guaranteed with dynamic network capacity?
- The more participants try to solve the calculation, the faster it will be found, the shorter will be the inter-block time

Solution:

- Introduction of a flexible and relative proof-of-work difficulty

09: Adaptiv-protocol

Adaptive Proof-of-Work difficulty depending on the computing power of the entire network.

Rules:

- The proof-of-work difficulty periodically adjusts to the network capacity
- For each block it is checked whether the protocol requires an adjustment of the difficulty.

Problem:

- Low probability of Forks due to guaranteed inter-block time and maximum block size
- Therefore low probability for indirect double-spending
- But double-spending is not 100% impossible
- An attacker can act selfish and deviate from the given protocol
- Through so-called Selfish-Mining, an attacker with enough computing power can still successfully conduct a double-spending
- The attacker works in secret on its own Fork of the block list. As soon as the attacker received the product payed with the transaction the attacker publishes its own Fork (which needs to be longer).
- Payable double-spending attacks are possible by a rationally acting attacker.

Derivation

The probability of a successful double-spending attack depends on exactly two factors:

- The speed in the competition
- The backlog to be made up

Solution:

- 51%- and double-spending Attacks cannot be prevented
- However, they can be made disproportionately expensive and therefore uneconomic
- The computing power added to the network is compensated by rewards

- Failed attackers will not receive this reward

10: Blockchain-protocol

High cost potential failed attacks due to loss of the so-called Block Rewards

Rules:

- Introduction of a reward for successfully calculated blocks (Block Reward)
  - commercial incentive and game theory
- The more computation power a participant provides to the network, the higher is the probability to find a block and receive the Block Reward.
  - Through a joint competition the overall computing power of the network grows
  - High overall computing power increases the cost of a double-spending attack
  - Double-spending attacks are no longer ”payable”

LECTURE 12:- 5G Mobile Networks in a nutshell

5G Vision (wishes)

Three types of service scenarios:

- Enhanced Mobile Broadband (eMBB)
- Massive Machine Type Communications (mMTC)
- Ultra-reliable low-latency communication (URLLC)

Enhanced Mobile Broadband (eMBB)

- People spend more and more time online with their smartphones
- New applications require more throughput
  - 4K or 8K Video-Streaming
  - Video Calls
- Virtual and Augmented Reality applications
  - Maintenance or remote surgery

Massive Machine Type Communications (mMTC)

- Communication of people using smartphones is not the only application for mobile communications anymore (Internet of things, Industry 4.0, Smart Homes).
  - Numerous Devices
  - Large Area
  - Low Data-Rate

Ultra-reliable low-latency communication (URLLC)

- Factory Automation
- Smart City Automation
  - Latency: < 1ms [8]
  - Reliability: 99,9999%

5G Key Technologies

- **Carrier Aggregation and mmWave**

  Throughput needs Bandwidth

- Mobile Network frequencies are divided in blocks (carrier).
- Aggregate multiple blocks for more bandwidth.
- User higher frequencies (mmWave) due to availability of bandwidth.
  - **Free-Space Path Loss (FSPL) and mmWave**
  - **Rain and mmWave**

But how do we reach an end-to-end latency if the next data-center is hundreds of kilometers away?

- **Mobile Edge Computing (MEC)**