MAIN IOT

1. Radio propagation

The mechanism of radio propagation can generally be described as reflection, diffraction and scattering. Propagation models are traditionally focused on prediction of the average received signal strength used to define the coverage area in a mobile cellular environment. In addition, some statistical properties of the radio channel, such as fading parameters, multipath and associated intersymbol interference heavily impact the system design and various system parameters.

1.1. **Free-space propagation.** The simplest possible scenario is that both transmit and receive antenna are placed in a free space. The power received at a destination in case of no obstacles and in LOS[1] can be described as the **Friis transmission equation**:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right) \frac{1}{L}$$

where the power received depends on the power transmitted, multiplied for both the gain in transmission and reception; $\frac{1}{L}$ represents hardware loss, λ is the wavelength, and d is the distance between the transmitter and the receiver.

1.1.1. *Path loss.* Path loss, which is the rate between the transmitted power and the received power, can be described as:

$$PL = \frac{P_t}{P_r} = \left(\frac{\lambda}{4\pi d}\right)^{-2}$$

Intuitively, path loss increases with higher frequencies and greater distance, assuming that the gains and hardware loss are equal to 1.

1.1.2. *Multi-path fading.* Multiple copy of a signal can arrive at destination because the signal may be scattered, reflected, and diffracted. The receiver may get multiple copies of the signal, each travelling different paths and resulting in different attenuation and delay (**delay spread**).

1.2. **Radio cell size.** Many small cells concentrated in highly populated areas are able to maintain a stable connection. Small cells are also faster to deploy and easier to maintain, however they have a shorter range and can handle fewer simultaneous sessions. One the other hand, larger cells must be used to cover wide, low-dense areas.

[1]Line of Sight, i.e. the signal has not been modied by scattering, reflections, etc.

2. Types of mobile network by multiple-access scheme

Mobile radio networks can be distinguished by operation modes, services and applications and multiple-access schemes. Radio communication systems focus on assigning the maximum number of users to an available radio frequency segment. This objective is achieved by using various multiple-access schemes:

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)
- Orthogonal Frequency Division Multiple Access (ODMA)

In **FDMA**, each mobile user (or user group) is allocated a frequency channel for the duration of the call, while in the **TDMA** scheme a group of callers use the same frequency channel but during different time intervals. Most of the systems using TDMA do, in fact, combine both schemes. In this approach, the system allocates a set of frequency channels to several groups of users, one frequency channel per group. One user in each group accesses an allocated frequency channel during a system assigned time slot.

In **CDMA**, all users occupy the same frequency channel and can transmit/receive at the same time. The information stream of each user is coded by a specific code ensuring orthogonality between users. It can be achieved by allocating additional frequency bandwidth to each user in excess of the bandwidth required for transmitting user source data.

In **OFDMA**, a large spectrum segment is allocated as a channel pool available to one or many simultaneous users. Allocated channel bandwidth and duration can be varied according to user service requirements and instant availability of common resource/channel pool. User channels are mapped on the set of orthogonal narrowband carriers, thus excluding mutual interference.

3. 2G: Global System Mobile

GSM is a standard to describe the protocols of the 2nd generation cellular system. In this system the signal is digital and both TDMA and FDMA schemas are employed. Frequency bands are split between downlink and uplink. The GSM network can be split into three subsystems: the radio access network, the core network and the management network. These respective three subsystems can also be called the Base-Station Subsystem (BSS), the Network Switching Subsystem (NSS) and the Operation Support Subsystem (OSS).

3.1. Base Station Subsystem.

The **BSS** interfaces the mobile users with the cellular system operator network. It manages radio communication and radio resources, configuration of cells, and must handle handovers[2]. It is formed by the Base Transmission Station (**BTS**), whose task is to provide radio coverage on the cell, and the Base Station Controller (**BSC**), which monitors and manages groups of BTS. The BSC tells the BTS when initiate a call or perform a handover, and reserves/relases radio channels.

[2]When a mobile station moves from one cell to another, while on call.

3.2. **Network Switching Subsystem.** The Mobile Switching Center (**MSC**) performs routing on the network to the Gateway MSC (**GMSC**). The Home Location Register (**HLR**) mantains information about all the users that had contact with the cellular system, while the Visited Location Register (**VLR**) store the current location of a mobile user.

Two other databases perform **security** functions: the Authentication Centre (**AuC**) stores security-related data such as keys used for authentication and encryption; the Equipment Identity Register (**EIR**) stores information about the hardware of mobile stations. The GSM security is based on information stored in the SIM. When ciphering is active, all information exchanged between the mobile and the network on the dedicated radio channels is encrypted. Encryption is performed at the transmitting side after channel coding and interleaving and immediately preceding modulation. On the receiving side, decryption directly follows the demodulation of the data stream. Authentication parameters are generated by the AuC, stored in the HLR, and must be sent to the VLRs that requests them.

3.3. **Communication channels.** There are physical and logical channels in GSM radio systems. A physical channel stands for one timeslot at one frequency carrier, while a logical channel refers to the specific type of information carried by the physical channel. Different kinds of information are carried by different logical channels, which are then mapped or multiplexed on physical channels.

Logical channels can be classified either as Common Channels - point-to-multipoint, all mobiles can overhear them - or Dedicated Channels - point-to-point, for dedicated and bi-directional communication between the base station and the mobile. Furthermore, logical channels can also be divided in two groups: Traffic Channels (TCH) and Control (Signalling) Channels.

3.3.1. *Traffic Channels.* Payload data are transmitted via the traffic channels. The payload might consist of encoded voice or raw data. A **logical traffic channel** can be either full rate (TCH/FR) or half rate (TCH/HR).

3.3.2. *Broadcast channels.* The Broadcast Channel (**BCH**), transmitted at downlink, are point-to-multipoint channels. They contain general information about the network and the broadcasting cell. There are three types of broadcast channels:

- Frequency Correction Channel (FCCH). Allows the mobile station in a cell to synchronize to the carrier frequency
- Synchronization Channel (SCH). Allows the identication of the BTS and stores the TDMA frame number
- Broadcast Control Channel (BCCH). Carries information for each cell to all the users served by that BTS, such as: frequencies used in the particular cell and neighbour cells, frequency hopping sequence, channel combination - which informs the mobile station about the mapping method used in the particular cell, paging groups and information on neighbour cells. The BCCH should be cleared of interference

3.3.3. *Common Control Channels.* The Paging Channel (**PCH**) is used by the BTS to notify incoming calls to a MS, in downlink. The Random Access Channel (**RACH**) is used uplink by a MS to request access to the network, and the Access Grant Channel (**AGCH**) carries replies to RACH requests downlink.

3.3.4. *Dedicated Control Channels.* There are three dedicated control channels used for signalling between mobile and base station, namely, the Slow Associated Control Channel (SACCH), Fast Associated Control Channel (FACCH) and Standalone Dedicated Control Channel (SDCCH). The SDCCH is used during the call setup for a traffic channel allocation. Both the SACCH and FACCH are used for signalling during the call, always associated with the allocated traffic channel.

3.4. **Synchronization.** Two kinds of synchronization are distinguished: frequency synchronization and time synchronization of the bits and frames. This is done in three steps:

(1) the MS tunes its carrier frequency to that of the BS
(2) next, the MS synchronizes its timing to the BS by using synchronization sequences
(3) finally, the timing of the MS is additionally shifted with respect to the timing of the BS to compensate for the runtime of the signal between the BS and MS (timing advance)

The **timing advance** values can be used as one of the parameters determining when handover between cells should take place. It can also be used to calculate the distance between the terminals and the base, which will be an important added value service.

3.5. **GPRS.** The GSM Packet Radio Service (**GPRS**) introduces the concept of sharing the pool of available channels in the cell between different users. The concept of sharing is as follows:

- several timeslots in the **PTCH** on one carrier frequency may be allocated to one user - this is known as "bundling" of timeslots. Timeslots can be bundled on the uplink (UL) and the downlink (DL). The allocation of timeslots may also be asymmetric between UL and DL
- opposite to circuit switch traffic, such as voice, a timeslot is not reserved exclusively for one user; that is, a timeslot may be shared by several users according to their priority or on round-robin basis

In order to support the new concept of packet service, the GPRS system was deployed as an overlay of GSM with two new network nodes, SGSN and GGSN, new interfaces and new functionalities in BSC. **EDGE** stands for Enhanced Data rate for GSM Evolution. It is a further evolution of GPRS, giving the option for an increased system data rate without changing the cellular mobile system architecture. The combination of GRS and EDGE is usually referred to as **EGPRS**.

4. 3G: Universal Mobile Telecommunication System

The third generation (3G) of mobile network system, referred as **UMTS**, is backwards compatible with GSM. In addition, GSM and UMTS networks are able to inter-operate between them. The UMTS system has an overall network structure similar to GSM.

The physical layer consists of the UMTS Terrestrial Radio Access Network (**UTRAN**), while at MAC layer it deployes the Wideband Code Division Multiple-Access (**W-CDMA**), where several transmitters can send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (bandwidth). Furthermore, The **HSPA** technology supports

much higher data rates, higher capacity in both uplink and downlink directions and significantly reduces latency compared with the initial WCDMA system.

4.1. **Energy consumption.** In 3G, a large fraction of the energy, referred to as the **tail energy**, is wasted in high-power states after the completion of a typical transfer. The ramp energy on the other end, is described as the energy spent to switch to a high power state, and does not consume much. The tail-ender is a protocol designed to reduce the waste from tail energy, and does so in three ways: combine the usage of 3G and wifi, predict when a wifi network might be available, wait to transfer large batch of data for delay tolerant applications, and prefetch for application that may benefit from it.

5. 4G: Long-Term Evolution

When high capacity and high performance at flat pricing are offered to the end customer, then cost per bit becomes a critical issue for the service provider. These three key drivers, capacity, user experience and lower cost per bit, have led to the specification of a Long Term Evolution (**LTE**) of mobile network. The access scheme in LTE is OFDMA in downlink and a SC-FDMA in uplink. **OFDM** allows for improved interference control, advanced scheduling techniques and ease of implementation of MIMO to improve spectrum efficiency. Further, OFDM enables scaling of user bandwidth very dynamically from very low bit rates required. OFDM technology can be used in both FDD and TDD multiple-access schemes, so that both LTE FDD and TDD system are standardized, thus allowing flexibility in implementation.

6. Ad-hoc wireless networks

An ad-hoc wireless network is a wireless multi-hop infrastructure-less network whose devices act as source and/or destination of messages and act as relay for packets; it self organizes, self congure and self maintain. Main features include: highly dynamic topology, simple protocols with low energy consumption and low overhead (ideally), number of hosts depends on the requirements, traffic can be low to high.

6.1. **Wireless Sensor Network. WSN** networks have a mostly static topology, e.g. networks to monitor the environment, but it is also possible that hosts move. Ideally, the number of hosts must not degrade the performance. Hosts are typically sensors with limited battery capacity and low processing power, so protocols must be simple, low energy consuming, and light, since the memory is also limited; traffic can flows from sensors to one ore more sink(s), where data is gathered and processed.

6.2. **IEEE 802.11 Wi-Fi.** The IEEE 802.11 standard specifies the set of MAC and physical layer protocols for implementing WLAN communication. **CSMA** is a MAC protocol in which a node tries to detect the presence of a signal from another node, before attempting to transmit. Using CSMA, multiple nodes may, in turn, send and receive on the same medium. Carrier-sensing can be of two types, (i) physical by detecting activity on radio, or (ii) **virtual**, by sending RTS/CTS control packets. Furthermore, two common variants of CSMA exists, based on (i) Collision Detection (**CSMA/CD**) or (ii) Collision Avoidance (**CSMA/CA**). Since CSMA/CD is not possible in wireless networks, due to wireless transmitters

desensing their receivers during packet transmission, CSMA/CA has to be used, however it is unreliable due to the hidden node problem.

In CSMA/CA, if the transmission medium is sensed busy before transmission, then the transmission is deferred for a random interval. This random interval reduces the likelihood that two or more nodes waiting to transmit will simultaneously begin transmission upon termination of the detected transmission, thus reducing the incidence of collision. Performances can be improved by combining the Network Allocation Vector (**NAV**) virtual carrier-sensing mechanism, in which nodes include a NAV field into RTS packets. By checking the NAV value, nodes can estimate how much they have to wait before accessing the medium.

6.2.1. *Cross-factor.* A substantial fraction of energy is consumed by the processing of packets throughout the protocol stack. Such **cross-factor** energy toll exhibits two notable features: (i) in some (common) radio settings, it may become the dominant source of energy consumption, and (ii) it is primarily associated to the frame processing itself, rather than to the amount of bytes handled.

The power consumed by an 802.11 device consists of the following components: (i) the idle consumption, ρ_{id}, (ii) the cross-factor for the packets generated by the application, P_{xg}, (iii) the power required to transmit them, P_{tx}, (vi) the power consumed in retransmissions, P_{retx}, (v) the power spent in receiving frames, P_{rx}, (vi) the cross-factor for the received frames, P_{xr}, and (vii) the power spent on sending and receiving ACK frames, $P_{rx,ack}$ and $P_{tx,ack}$:

$$P = \rho_{id} + P_{xg} + P_{tx} + P_{retx} + P_{rx} + P_{xr} + P_{rx,ack} + P_{tx,ack}$$

7. Routing protocols for ad-hoc networks

There are two standard approaches for intra-AS routing: **link state**, where each switching node keeps information on the topology and then applies shortest path algorithms, e.g. Dijkstra, to construct its own routing table; **distance vector**, where switching nodes exchange information (such as the routing table and hop count) and determinate the best route through the Bellman-Ford algorithm. However, ad-hoc wireless networks have different needs from standard networks, and routing protocol should have: minimal control overhead, low processing overhead, no loops, multi-hop path capability, dynamic topology maintenance, and it must be self-starting.

7.1. **Proactive routing protocol.** This type of protocols maintains routes to each other node by periodically distributing routing tables throughout the network. This means that routes are alway available. The main disadvantages of such algorithms are (i) high overheads in high mobility networks, (ii) low scalability, and (iii) slow route convergence time.

7.1.1. *Destination Sequence Distance Vector.* Based on the Distributed Bellman-Ford (**DBF**) algorithm, incorporating sequence numbers to avoid routing loops. Each route table is tagged with a sequence number which is originated by the destination. To maintain the consistency of routing tables in a dynamic topology, each node periodically transmits updates, and transmits updates immediately when significant new informations are available. Broken links can be detected by layer-2 protocols, or it may instead be inferred if no broadcasts have been received for a

while from a former neighbor. Any route with a more recent sequence number is preferred, while routes with older sequence numbers are discarded.

7.1.2. *Optimized Link State Routing Protocol.* Nodes periodically transmit **HELLO** messages, containing the sender address and its own neighbor, including each link status. Upon receiving a HELLO message, a node can thus gather informations about its neighborhood and two-hop neighborhood, as well as the quality of their link. Such informations are considered valid for a short period of time.

In **OLSR**, the problem of duplicate messages (within a region) is addressed through the notion of Multi-Point Relays (**MPR**). Each node selects its MPRs independently, which must be able to reach all the node's two-hop neighbors. All nodes with a non-empty MPR set periodically generate a topology control message, effectively announcing reachability to all its MPRs. The result is that all nodes will receive a partial topology graph of the network, and it is possible to run a shortest path algorithm for computing optimal routes from a nodes to any reacheable destination.

7.2. **Reactive routing protocol.** This type of protocol finds a route on-demand by flooding the network with Route Request packets, resulting in less control overhead and better scalability. Nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. The main disadvantages of such algorithms are (i) high delays in route finding, and (ii) excessive flooding leading to bottlenecks.

7.2.1. *Dynamic Source Routing.* The sender builds a **source route** in the packet header, giving the address of each host in the network through which the packet should be forwarded in order to reach the destination host. When a host receives a packet, if this host is not the final destination of the packet, it simply forwards it to the next hop in the source route.

Each node maintains a **route cache** in which it caches source routes it has learned. When one host sends a packet to another host, the sender first checks its route cache for a source route to destination. If no route is found, the sender starts the **route discovery** protocol: it broadcasts a **route request** packet to its neighbor identifying the destination, and (if successful) it receives a **route reply** listing a sequence of hops through which it may reach the destination.

While a source route is in use, the node does **route maintenance**, monitoring its working state. If it detects a problem, route discovery may be used again to discover a new, correct route to the destination.

7.2.2. *Ad hoc On-demand Distance Vector.* **AODV** relies on dynamically enstablishing route table entries at intermediate nodes. This difference pays off in highly dense networks, where a large overhead is incurred by carrying source routes as in DSR. To maintain fresh routing information between nodes, sequence numbers are used as in DSDV, but each node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes.

The path discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing informations in its table. The source node broadcasts a Route Request (**RREQ**) packet to its neighbor, which may respond with a Route Reply (**RREP**) back to the source or rebroadcast the

RREQ to their own neighbor, after increasing the hop counter. When an intermediate node receives a RREQ, if it has already received a RREQ with the same ID and source address, it simply drops the redundant packet.

The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that contained in the RREQ. If it does have an current route to the destination, and if the RREQ has not been processed previously, the node then unicasts a RREP back to its neighbor from which it received the RREQ. A node receiving a RREP propagates the first RREP for a given source node towards that source, which can begin data transmission ad can update its routing informations (if it learns a better route).

7.3. **Geographical routing protocol.** Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location. With knowledge of the neighbors' location, each node can select the next-hop that is closer to the destination, and thus advance towards the destination in each step.

The fact that neither routing tables nor route discovery activities are necessary makes geographic routing a good fit for dynamic networks such as wireless adhoc and sensor networks. In such networks, acquiring and maintaining routing information is costly as it involves additional message transmissions that require energy and bandwidth and frequent updates. In contrast, georouting algorithms work nearly stateless and can provide high message delivery rates under mobility, assuming that (i) nodes can determine their own position, (ii) nodes are aware of their neighbors' positions, and (iii) the destination position is known.

The main prerequisite to meet the three assumptions is a positioning system. If this is available, geographic routing provides an efficient and scalable solution for routing in wireless and mobile networks. However, a simple **greedy forwarding** by minimizing the distance to the destination location in each step cannot guarantee message delivery. Greedy algorithms cannot resolve such dead-end or local minimum situation. Therefore, recovery methods have been developed to improve greedy forwarding.

7.3.1. *Location-Aided Routing.* When a source nodes needs to find a route to a destination node, it broadcasts a RREQ message to all its neighbor. A node receiving a message first compares the destination with its identifier. If it does not match, the node broadcasts the request to its neighbor. Duplicate requests are identified through sequence numbers, and discarded. As the RREQ travels the network, the path followed is included in the packet. On receiving the RREQ, the destination sends a RREP to the sender. If the next hop on the route is broken, nodes send a RERR message, and initiates a route discovery for that destination.

Furthermore, **LAR** makes use of location information to reduce routing overhead. The expected zone of a destination node D, from the viewpoint of a source node S at time t_1, is the region that node S expects to contain node D at time t_1. Node S can calculate the expected zone based on the knowledge that node D was at a certain location a time t_0. If node S does not know a previous location of node D, the expected zone may cover the entire network, reducing the algorithm to a basic flooding algorithm. Node S defines a request zone for the RREQ. A node forwards a RREQ only if it belongs to the expected zone.

7.3.2. *Geographic Random Forwarding.* Nodes follow a duty cycle, with asynchronous awake/asleep schedules. The forwarding area of each node is divided into N regions, 1 through N, such that any node in region i is closer to the sink than any node in region j. Whenever a node wants to send a packet it first senses the channel, then transmits a Request-to-Send (RTS) message that silences nodes offering negative advancement and serves as a polling message for region 1. The awake nodes in this region report back using a Clear-to-Send (CTS) message. If more than one respond, the sender issues a COLLISION message to solicit the choice of a single node. After the identification of the next hop, the node sends a data packet, waits for an ACK, and then the sender goes back to sleep, so that the relay finds the channel free and can forward the packet. If no relay is found in any region or the channel is sensed busy, the transmitter backs off and reschedules a later attempt.

Note that, in **GeRaF**, nodes are not required to know the position of any other sensor but their own and the sink's, since any other information is exchanged through RTSs and CTSs. Also nodes do not need to know their neighbors and their wake-up schedule: a relay is selected among the awake neighbors.

7.3.3. *Adaptive Load-Balanced Algorithm.* **ALBA** is designed to take congestion and traffic load balancing into consideration, other than just advancement. All the eligible relays of a node compute two values, the Geographic Priority Index (**GPI**), i.e. the index of the region the node would belong to in the GeRaF framework, and the Queue Priority Index (**QPI**), which is a measure of forwarding effectiveness as perceived by the relay.

To solicit the election of a forwarder, the source first senses the channel and then issues RTS messages to scan the QPI values in increasing order. If more than one nodes answer the RTS message, the sender tries to select the one with the best GPI, starting a second contention with progressively higher GPIs. This process eventually ends with the selection of a single relay. If no relay is found, the sender backs off. Like GeRaF, ALBA exchanges relevant data such as the geographic coordinates through RTSs and CTSs, requiring little information to be stored inside sensors.

In order to solve the dead-end problem, **ALBA-R** introduces the **Rainbow** node-coloring algorithm, with no need for additional signaling packets. Nodes that recognize themselves as dead-ends progressively stop advertising as relays, and to route traffic out of the dead-end, they begin to transmit packets backward, in the negative advancement zone. Hopefully, a relay that has a greedy forwarding path to the sink will be found.

8. Routing protcols for Wireless Sensor Networks

8.1. **Collection Tree Protocol.** The base idea is to send beacon messages to construct a tree structure, and nodes can relay their information to their best parent. Desired properties are reliability (at least 90%), robustness, energy efficient, and hardware independent.

The number of expected transmissions needed to send data between two nodes, **ETX**, is used as the routing metric. This assumes packets are re-transmitted at the link layer. Routes with a lower metric are preferred. In a route that includes multiple hops, the metric is the sum of the ETX of the individual hops. Each node that wishes to collect data advertises itself as a tree root. Each node sends its

data to the tree root to which it is nearest, that is, the tree root from which it is separated by the smallest ETX. A tree root always has an ETX of zero.

Each node only keeps the smallest ETX (to the nearest tree root). Rapidly changing link qualities, for example in sensor networks with moving nodes, cause routing information to become outdated which can lead to routing loops. CTP attempts to address these issues through datapath validation and adaptive beaconing.

Beacon messages are transmitted regularly when the sink starts the beaconing process, to exchange informations about ETXs. Data packets embed the estimated ETX, and sequence numbers that allow to know the percentage of packets that has been received, allowing to estimate the link quality. To compute the best route, the algorithm is Bellman-Ford with ETX as metric.

When a node receives a packet, if its current ETX is smaller than the one embedded into the packet, the node updates the packet's ETX and forwards it. Otherwise, the "pull" bit is set to 1, and the route must be recomputed starting a beaconing process.

8.2. **Wake-up enabled protocols.** Many recent activities of IEEE 802.11 Working Group have been focused on improving power efficiency of Wi-Fi to make it viable for massive IoT scenarios, in which swarms of battery supplied sensors rarely communicate with remote servers. The 802.11ba standard introduces Wake-Up Radios (**WuR**), low-power hardware in charge of monitoring the channel. The use of wake-up radios enables on-demand communications, allowing nodes to keep their main radio off when not needed, and virtually eliminating idle listening.

8.2.1. *FLOOD-WUP.* A new flooding protocol, achieving high reliability and better latency vs. energy consumption performance. In **FLOOD-WUP** nodes are assigned shared broadcast addresses. Initially nodes are asleep and the sink sends the first broadcast packet to its neighbors. To each broadcast packet a unique sequence number is associated, lets say w_a. Nodes receiving a wake-up signal with sequence w_a awake and set their radio to receive the broadcast packet B. Upon reception of B, each node changes its broadcast wake-up address from w_a to w_b and so on. This means that nodes that have already received the broadcast packet will not wake up when duplicated packets are transmitted.

8.2.2. *GREEN-WUP.* A energy-harvesting and WuR aware protocol. In **GREEN-WUP** packet forwarding is realized by opportunistically selecting the next-hop relay among the whole set of neighbors, rather than just among the awake ones. In particular, nodes activate a given wake-up sequence w_i - i.e. they wake-up if such sequence is transmitted - in case they are in the corresponding state i. Such a state expresses how good a node is to serve as a relay, based on metrics such as residual energy and its own hop-count.

9. Energy-efficient MAC protocols

A low-power MAC protocol aims to minimize energy waste - introduced by collisions, overhearing, control packets overhead, idle listening - and minimize end-to-end latency, while guaranteeing fairness and scalability. For these reasons, an awake/asleep schedule with a given duty cycle is widely adopted.

9.1. **Sensor MAC.** At startup, nodes listen on the medium. If a node hears nothing it sends a SYNC packet with a schedule defining listen and sleep periods, and becomes a **synchronizer**. On the other hand, if a node receives a SYNC packet, it becomes a **follower**, and adopts the corresponding schedule. Border nodes may adopt two or more schedules (if different neighbors have different schedules), resulting in more energy consumption.

Each node keeps a table with the schedules of their neighbors. During a listen period, a node with a packet to send executes a procedure similar to CSMA/CA, transmitting a request-to-send (RTS) frame and the receiver node answering with a clear-to-send (CTS) frame. All nodes not involved in the conversation enter a sleep state while the communicating nodes send data packets and ACKs. The transmission of ACKs are sufficient to deal with the hidden terminal problem.

Sleeping decreases energy consumption but introduces latency, since communication with a sleeping node must wait until it wakes up. Furthermore, clocks may drift and SYNC packets may go lost, so they have to be frequently exchanged (introducing more control overhead).

9.2. **Timeout MAC. T-MAC** improves on **S-MAC** to find a balance between wake time (potentially wasting energy in idle listening) and the repetition of the duty cycle (potentially increasing latency). Active time is changed dynamically adapting on the traffic level of the network: higher the traffic, longer the active time. If a node does not receives transmissions from neighbors for a period of time, the active time is aborted and the node will go to sleep. Nodes do not exchange asleep/awake schedules, since a fixed schedule is not good in practice.

T-MAC still suffers of low throughput, since every channel is active only for a brief period of time. Furthermore, synchronization is very inefficient because of clock drifting.

9.3. **Berkeley MAC. B-MAC** employs an adaptive preamble to reduce idle listening, a major source of energy usage in many protocols. When a node has a packet to send, it waits during a back-off time before checking the channel. If the channel is clear, the node transmits; otherwise it begins a second (congestion) back-off. If the channel is idle and the node has no data to transmit, the node returns to sleep.

B-MAC does not require RTS, CTS, ACK, or any other control frame by default[3], and no synchronization is required. However, the preamble creates large overhead, consumes more energy in transmission, and every node that overhear the preamble will stay awake until the end.

9.4. **X-MAC. X-MAC** improves upon B-MAC by embedding into the preamble the address of the destination, so nodes overhearing can return to sleep. The preamble is a series of short preambles divided by pauses; these latter allow the destination to send an ACK to interrupt the preamble and to start the transmission of data.

9.5. **WiseMAC.** Nodes sense the medium at the same constant period independently. The idea is to learn the sampling schedules of direct neighbours, and use them to minimize preamble size. To recover packet losses, ACK packets are not only used to carry acknowledgement information but also to inform other nodes

[3]but can be added

(including the sender) the remaining time of next sampling. In high traffic, the packet overhead is low, but in low traffic is high; however, the power consumption resulting from this high overhead is low.

10. Low-power wide-area network

10.1. **IEEE 802.15.4.** The IEEE 802.15.4 standard specifies the physical layer and MAC layer (CSMA/CA) for LR-WPANs. These networks are connected through internet via routers or operating in ad-hoc mode. To address several limitations such as (i) no delay guarantees, (ii) no interference resilience, and (iii) not ideal for high traffic environments, the 802.15.4*e* extended standard introduces new features such as BLINK, AMCA, DSME, LLDN, and TSCH.

10.1.1. *Time Slotted Channel Hopping.* Introduces support for slotted access, multi-channel, and frequency hopping. **TSCH** is topology independent and supports high network capacity, high reliability, and predictable latency, allowing low duty-cycles. Nodes synchronize on a cycling frame (of n timeslots) which allows sending data and receiving ACKs. Communications are scheduled on a time-slot $\times$ channel table.

10.2. **6LoWPAN architecture.** The **6LoWPAN** group defines encapsulation and header compression mechanisms to allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks.

A 6LoWPAN network is connected to the IPv6 network using an **edge router**, which handles three actions: (i) the data exchange between 6LoWPAN devices and other networks; (ii) local data exchange between devices inside the 6LoWPAN; and (iii) the generation and maintenance of the radio subnet. Edge routers may also support IPv6 transition mechanisms to connect to IPv4 networks.

6LoWPAN network communicate natively with IP: this means that data going into the network is destined for one device, and edge routers do not need to maintain application-layer states. However, this IP architecture does not preclude the use of proxies and caches to improve network performances.

10.2.1. *System stack.* 6LoWPAN introduces an **adaption layer** between the link and network layer to enable transmission of IPv6 datagrams over 802.15.4 radio links. This adaptation layer uses stateless or shared-context compression to elide header fields. This can compress all headers (adaptation, network and transport layers) down to a few bytes. It is possible to **compress header fields** since they often carry common values. Common values occur due to frequent use of a subset of IPv6 functionality, namely UDP, TCP and ICMP. Assumptions regarding shared context can also be made, such as a common network prefix for the whole 6LoWPAN system. The adaptation layer also removes duplicated information that can be derived from other layers, such as the IPv6 addresses and UDP/IPv6 length fields.

10.3. **LoRa. LoRa** defines a proprietary LP-WAN spectrum modulation technique (physical access), targeted at IoT devices.

10.3.1. *LoRaWAN.* Communication protocol and architecture that uses the LoRa physical layer. **LoRaWAN** supports secure bi-directional communications, mobility and localization, and defines how node should communicate. In a LoRaWAN network there are end-nodes connected to a gateway via LoRa links, and these gateways can be connected to other network via LoRa links or other links such as 3G and ethernet.

LoRaWAN defines three types of devices: Class A, where each uplink communication is followed by two short downlink receive windows; class B is like Class A but there are extra receive windows at scheduled times (called beacons); Class C has continuous receive windows except when it transmits. There are different types of node to balance the battery life and the downlink communication delay: class A is the most energy efficient, followed by B and then C.

Gateways receive on all the channel for all the time, and forward packets to the network server, which identifies duplicates and filter them, validate data and send it to the correct application server. Since there is a central time reference for every gateway, the network server is capable of localization.

Frames start with a preamble of known chirps, followed by a header, CRC, and the payload. There are two layers of security: network and application. The first authenticates users, adds message integrity checks and encrypt the whole packet; the later encrypts its payload.