Wireless Ad Hoc Networks

Lecturer: Riku Jäntti

Email: riku.jantti@uwasa.fi

Contents

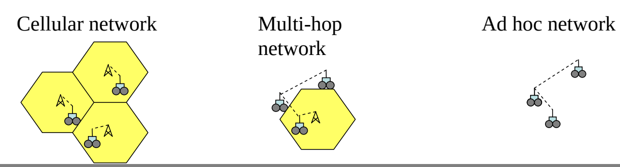
- Introduction
- Performance limits
  - Radio technology
  - Connectivity
  - Capacity
- Medium access control
  - Random access schemes
  - Spatial TDMA
  - Energy efficiency - Power control and sleep modes

Contents

- Network layer
  - Routing principles
  - Interaction between network layer and MAC layer
  - Interaction between network layer and physical layer
  - Energy efficiency and power control
- Transport layer
  - TCP performance
- Security
  - Packet level authentication

Wireless Ad Hoc Networks

- Some of the transceivers (nodes) act as routers
- The network is formed by means of self-configuration without any pre-existing infrastructure
- Network control is distributed among the nodes, no central control unit is needed



Historical Overview

- Multihop networks
  - Early 2000's
  - Multihop extensions to cellular radio access networks
  - Integrated heterogeneous networks
- Multihop packet radio networks
  - Late 1980's
  - DARPA funded research projects
  - Military applications

Historical Overview

- Wireless Ad Hoc networks
  - Late 1990's
  - Ad hoc mode in WLAN standard
  - Peer-to-peer networking, Personal Area Networks
- Wireless sensor (and actuator) networks
  - Late 1990's
  - Berkeley Smart dust project
  - Military sensor networks, environmental monitoring, home/industrial automation, ambient intelligence

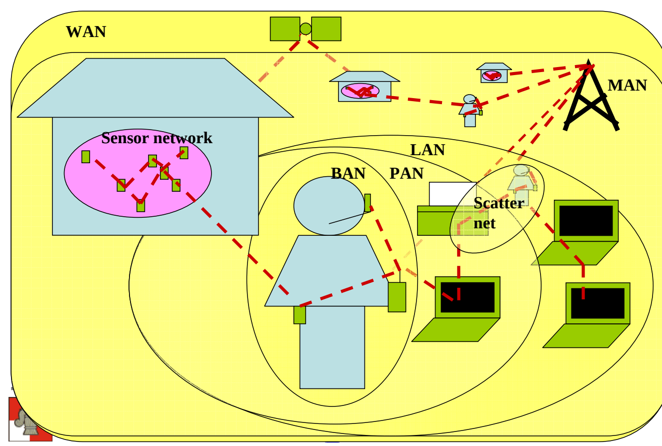
University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Ad Hoc Networks

- Packet radio network
- Wireless / Mobile Ad hoc network
- Scatter network
- Mesh network
- Multihop network

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

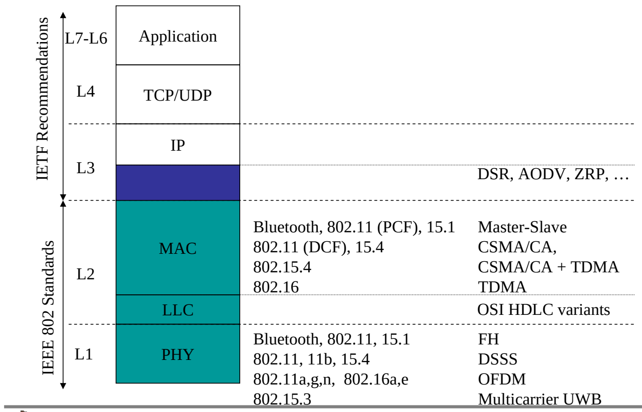
Network Hierarchy



Network Hierarchy

- BAN, Body Area Network
  - IEEE 802.15.3 (UWB)
- PAN, Personal Area Network
  - Bluetooth, IEEE 802.15.1
- LAN, Local Area Network
  - ”Ethernet”, IEEE 802.3
  - WLAN, IEEE 802.11a,b,g,h
- MAN, Metropolitan Area Network
  - IEEE 802.16,
  - Cellular radio (GSM, UMTS, IS-95, CDMA2000, TD-SCDMA,...)
- Sensor networks
  - IEEE 802.15.4 ZigBee
  - IEEE 1451.5 Intelligent actuators

Architecture



University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Ad Hoc Networks

- Benefits
  - No need for separate base stations or the number of them could at least be decreased
  - Easy to deploy, no wiring required
  - Reconfigurable: Network can quickly adapt to topology changes
  - Can be utilized in an areas where infrastructure doesn’t exists
  - Robust: Break down of single network node doesn’t prevent networking
- Drawbacks
  - Distributed operation => difficult to control
  - Lower capacity, higher packet delay and more severe jitter than in cellular/infrastructure networks
  - Nodes are either battery operated or use energy scavenging => Utilized protocols should be energy efficient
  - Network maintenance can be expensive (e.g. change of batteries etc.) => Redundancy is required

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Sensor Networks

- Sensor network is an ad hoc network, in which the nodes are sensor devices
  - Low computation power, small memory space
  - Energy consumption is critical: If nodes are running on batteries their operation time depends heavily on the energy efficiency of the data transmission.
  - Node size and cost are critical: Nodes should be cheap enough, so that they could be deployed in large quantities to obtain both coverage and redundancy
  - Data rates are small: Size of single measurement data unit is only few bytes; data rates 1 … 100 kbytes per second
  - Number of nodes is large: Ad hoc data network ~10 nodes, sensor network ~1000 nodes.

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Performance Limits

- Radio technology
  - Power consumption
  - Single frequency networks
- Connectivity
- Capacity

Radio Technology

- Energy cost of communication
  - Standard radio
    E.g. Bluetooth (2.4 GHz band, 10m distance)
    - 1 nJ/bit transmission energy (thermal limit 30 pJ/bit)
    - Overall energy:
      - 170 nJ/bit reception
      - 150 nJ/bit transmission
      - Standby power 300 mW
  - Picoradio for small sensors
    - <5 nJ/ bit for energy-limited source
    - < 100 μW for power-limited source (enabling energy scavenging)
  - Passive radio
    E.g. RFID Tags
    - Operation power is taken from the received RF power

Radio Technology

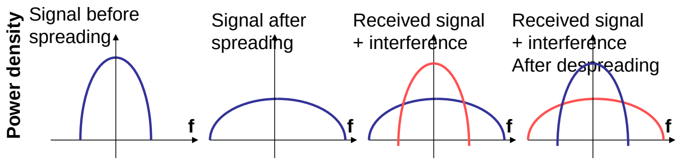
- Ad hoc networks typically run on unlicensed (ISM, Industry, Science, Medical) bands
  - High frequency, radio signal attenuates fast
  - Effective radiated power is limited
    - 100 mW (2400 – 2483,5 MHz)
    - 200 mW (5150 – 5350 MHz)
    - 1 W (5470 – 5725 MHz)
  - There can be interference from other coexisting networks

Radio Technology

- Utilized transmission schemes
  - DSSS, Direct Sequence Spread Spectrum (IEEE802.11b, IEEE802.15.4 ZigBee)
  - FHSS, Frequency Hopping Spread Spectrum (Bluetooth)
  - OFDM, Orthogonal Frequency Division Multiplexing (IEEE802.11g, 11a)
  - UWB, Ultrawideband (IEEE802.15.3a high speed PAN)
- Utilized modulation methods (IEEE802.11a,g)
  - BPSK (1 bit/symbol)
  - QPSK (2 bit/symbol)
  - 16QAM (4 bit/symbol)
  - 64QAM (8 bit/symbol)

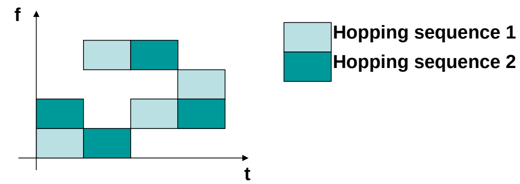
Radio Technology

- DSSS, Direct Sequence Spread Spectrum
  - A bit is modulated with a spreading code consisted of several chips. Spreading factor SF= chip rate / bit rate.
  - As a consequence the bandwidth of the spread signal is SF times larger than without spreading
  - At the receiver the received signal is multiplied with the same spreading code. This despreads the desired signal and spreads the interference resulting in increased signal-to-noise-plus-interference ratio SINR.



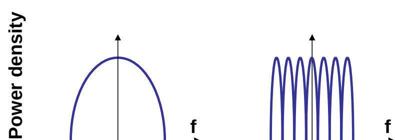
Radio Technology

- FHSS, Frequency Hopping Spread Spectrum
  - Frequency is changed several times during the transmission of the packet based on a frequency hopping sequence
  - Two transmitters end up interfering each other only a small fraction of time



Radio Technology

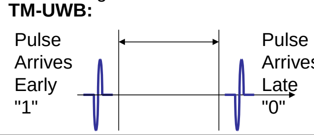
- OFDM, Orthogonal Frequency Division Multiplexing
  - Wideband transmission is divided among many narrowband subchannels that are orthogonal to each other
  - Narrowband channels are more robust against multi-path fading
  - Channelization can be done efficiently using IFFT at the transmitter and FFT at the receiver.



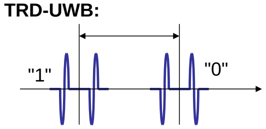
Radio Technology

- Ultrawideband (UWB) communication.
  - UWB: A signal having -10dB bandwidth greater than 25% of the center frequency
- Instead of modulating continuous sinusoidal signal, very narrow time pulses are used. (Resembles the spark gap impulse communication used by Marconi)
  - TM-UWB: Information is coded into the timing of the pulse.
  - DS-UWB: Pseudorandom code based time shifts
  - TRD-UWB: Employs impulse pairs with different polarity with constant timing

TM-UWB:



TRD-UWB:



Radio Technology

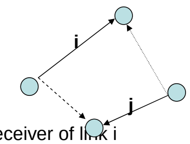
- Benefits of UWB
  - High spatial capacity (0.24 ns pulses, 4 billion pulses per second, range up to tens of meters)
  - High channel capacity and scalability
  - Robust multipath performance
  - Very low transmit power (sub-milliwatt power levels spread over several GHz channel, low interference)
  - Location awareness and tracking (accurate estimation of propagation time)
- Applications
  - Short range BAN and PAN networks with very high data rate
  - Very low power sensor networks with low data rate

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Transmit Power

- Bit and frame error probabilities are functions of received signal-to-interference+noise ratio SINR

$$\frac{g_{ii}p_i}{\sum_{j\in I_i} g_{ij}p_j + \upsilon_i} \geq \Gamma_i$$



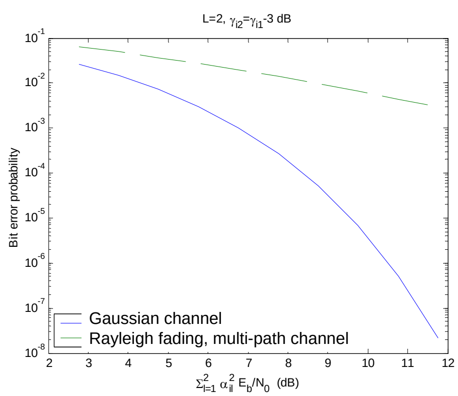
p_i	transmit power in link I
g_{ij}	link gain between transmitter of link j and receiver of link i (distance based attenuation + slow and fast fading)

$$g_{ij} \sim \frac{1}{\left\| X_{receiver,i} - X_{transmitter,j} \right\|^{\alpha}}$$

ν_i	noise power at receiver of link I
α	attenuation factor (α=2 free space, $\alpha \approx$ 4 urban environment)
Γ_i	SINR target value corresponding to tolerable bit error rate (BER)
I_i	set of interferers (simultaneously active links)

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

BER(SINR)

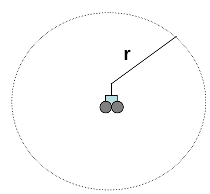


University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Transmit Power

- Assume that interference power is negligible compared to noise (e.g. one-by-one scheduling is used)
- Transmission range of a node is limited by the transmit power

$$p_i \geq \Gamma_i \upsilon_i r^{\alpha}$$



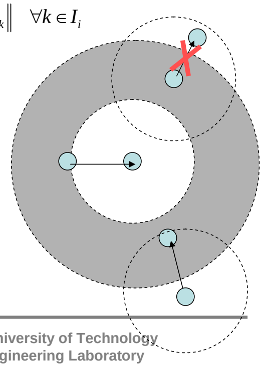
University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Transmit Power

- Simplified interference model. A transmission in link i is successfully received if

$$\left\| X_{receiver,i} - X_{transmitter,j} \right\| \leq (1+\Delta) \left\| X_{receiver,i} - X_{transmitter,k} \right\| \quad \forall k \in I_i$$

- This model is often used due to its simplicity.
- However, it fails to take the aggregate interference power into account.



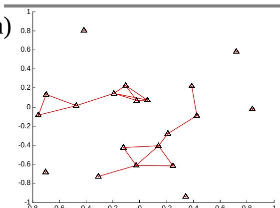
Connectivity

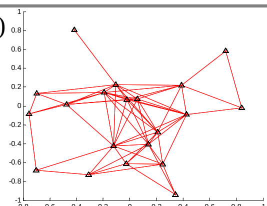
- Consider a random network in which *n* nodes are uniformly distributed in an square area of 1 m^2.
- Two nodes i and j can communicate if their distance is less than the radio range r(n).

$$\left\| X_i - X_j \right\| < r(n)$$

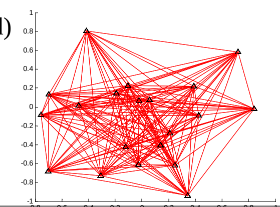
- In order to guarantee connectivity (existence of route between any two nodes in the network), the radio range i.e. transmit power, should be chosen so that the network graph G(n,r(n)) is connected.

Connectivity

a) 

b) 

a) Power is too small and the network is not connected
b) Power level is critical, the network is connected. Communication may require multiple hops.
c) Power level is high, the network is fully connected, all nodes can communicate with each other with direct links

d) 

Connectivity

- Critical power level that guarantees asymptotic connectivity as n→∞ have been analyzed by Gupta and Kumar (1998):

$$\Pr\{G(n,r(n)) \text{ is connected}\} = \Pr\{n\pi r^2(n) - \log n \geq c(n)\} \to 1$$
$$c(n) \to \infty$$
$$n \to \infty$$

- The radio range shrinks to zero as n→∞. However, in order to maintain connectivity it must decrease slower than $\sqrt{\frac{\ln n}{n}}$

Connectivity

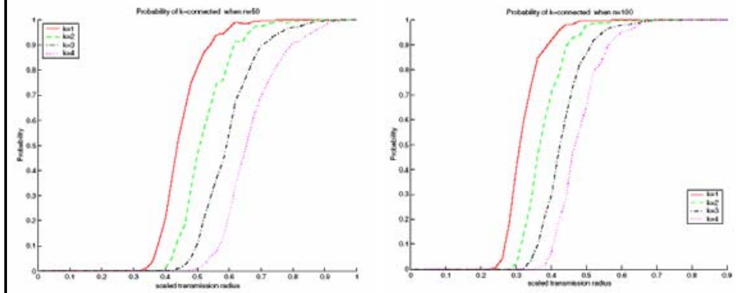
- Penrose (1997) has shown that the longest edge M_n of a minimum spanning tree of n points randomly distributed in unit square satisfies

$$\Pr\left\{n\pi M_n^2 - \ln n \le \beta\right\} = e^{-e^{-\beta}} \qquad \beta \ge 0$$

- Clearly, M_n is related to the critical power, hence the above gives the probability that the network is connected

Connectivity

- k-connectivity (node has links to at least k- neighbors)



(Li *et. al*., 2003)

Capacity

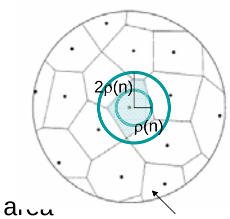
- Nodes are uniformly distributed on a unit disc
- The network graph is connected
- The transmit power in bounded in the inerval $[P_{min}, P_{max}]$.
- Each node can transmit W bit/s over a common wireless channel
- Traffic can be divided into M subchannels with capacity W_m
- Network is synchronizes and slotted

Capacity

- Vornoi tessellation:

  $V(X_i) = \left\{X \in S^2 : \|X - X_i\| = \min_{1\le j\le n} \|X - X_j\|\right\}$

  is a set of points that are closer to point X_i than any other point on a sphere S^2



Vornoi cell

- Every Vornoi cell contains a disk of area

  $\rho(n) = \text{radius of a disc of area } \frac{100\log n}{n} = \sqrt{\frac{100\log n}{\pi n}}$

- And is is contained in disc of radius $2\rho(n)$
- By selecting the radio range as $r(n)=8\rho(n)$, communication between adjacent cells can be guaranteed.

Capacity

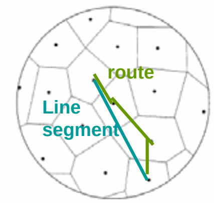
- Two cells are interfering neighbors if there is a point in one cell, which is within distance $(2+\Delta)r(n)$ of some point in the other cell.
- The number of neighbors is upper bounded by c.
- It can be shown that for large enough common transmit power P, there exists a schedule in which every cell gets one time slot every (1+c) slots such that all transmission are successfully received within a distance r(n) from the transmitter. [A graph with bounded degree 1+c can have its vertices colored with no more than 1+c colors]

Capacity

- A node i situated at X_i wishes to communicate with a node X_j closest to a randomly chosen point Y_i. The set of line segments L_i are i.i.d. random variables.
- Asymptotic capacity results

$$\lambda(n) = \Theta\left(\frac{W}{\sqrt{n \log n}}\right)$$

(Gupta and Kumar, 2002)



$$f(n) = \Theta(g(n)) : f(n) = O(g(n)), g(n) = O(f(n))$$

Capacity

- The capacity can be increased by adding m relay nodes that do not generate traffic themselves. In that case the throughput capacity of the network is

$$\lambda(n) = \Theta\left(\frac{(n+m)W}{n\sqrt{(n+m)\log(n+m)}}\right)$$

- Adding kn relay nodes provides less than $\sqrt{k+1}$ increase in the throughput
- If the nodes are optimally placed, then the transmission capacity (bit meters) is $\Theta\left(W\sqrt{n}\right)$

Capacity

- Long range direct communication is usually not possible due to the large interference caused to other users
- As a result, communication can occur between nearest neighbors, at distances of order $\frac{1}{\sqrt{n}}$.
- The number of hops in a typical route is on the order $\sqrt{n}$.
- Because, much of the traffic carried by the nodes are relayed traffic, the actual useful throughput per source-destination par must to be small.

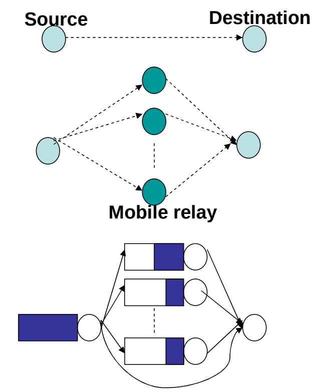
Capacity

- Grossglauser and Tse (2002) have suggested a scheme that exploits the mobility of the nodes to achieve high throughput

$$\lim_{n\to\infty} \Pr\{\lambda(n) = cW \text{ is feasible}\} = 1$$

Capacity

- Transmission scheme exploiting multi-user diversity
  - Nodes split the packet stream to as many different nodes as possible.
  - When a node comes within the radio range of the destination, it will relay the packet.
  - Since the nodes are mobile, the probability that at least one node is close to the destination is large.
  - Packets go through up to two hop path.



Capacity

- Grossglauser and Tse (2002)

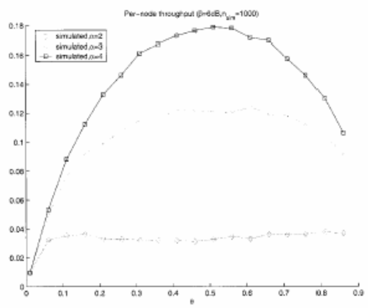


Fig. 7. The normalized per-node throughput for the *receiver-centric* case, as a function of the sender density θ for different values of α.

Medium Access Control

- The purpose of the MAC protocol is to divide the shared medium, radio spectrum, among the different users.
- MAC protocols
  - Collision free (Polling and STDMA)
  - Random access (ALOHA, CSMA/CA)
- Energy efficiency
  - MAC layer power control
  - Sleep modes

Polling

- Star topology network
- One of the nodes acts as a master and polls the others
- Master node can be selected dynamically: if a node does not hear a master it will declare itself as master.
- Slave nodes are only allowed to transmit when master polls them
- Transmission between slaves goes through the master node

Bluetooth MAC

- A new device entering the network starts in an inquiry state in which it continuously sends an inquiry message.
- 32 frequency access code consisted of two 16 frequency trains. (Transmission rate is 1600 hops/s)
- A train is repeated at lest 256 times before switching to another train.
- Up to three repetitions of access code are needed to guarantee sufficient number of responses.
- The inquiry state can take up to 10.24 seconds
- A device willing to communicate with the inquiring devices answers with FHS packet containing its clock information and address.
- When the devices has achieved the clock and address information of another node, communication is started using a polling mechanism.
- The device first to start polling becomes a master.

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Bluetooth MAC

- Transmission is divided into slots
- When a slave receives a packet from a master it is allowed to transmit data in the next slot.
- If a slave does not have date it will transmit an empty NULL packet.
- Synchronous Connection-Oriented (SCO)
  - Point-to-point link between master and slave for transmitting delay sensitive data (64 kbit/s)
  - Master polls the slave periodically
- Asynchronous Connection-less Link (ACL)
  - Master polls the slaves asynchronously

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Bluetooth MAC

- Scheduling:
  - Round robin:
    - All slaves are polled periodically.
    - This can be very inefficient if slaves have little traffic, since most of the time bandwidth is wasted by transmitting NULL packets.
  - Efficient double-cycle EDC scheduling
    - Uplink (slave-to-master) and downlink (master-to-slave) scheduling are separated.
    - In downlink, time slots are allocated to active links having data to transmit.
    - In uplink, time slots are allocated based on estimation of traffic volume.

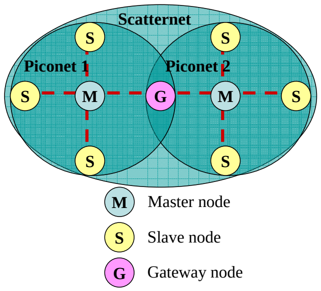
University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Bluetooth MAC

- Exponential binary backoff is applied to slaves issuing NULL packets.
  - Number of NULL packets $c_i = c_i + 1$
  - Backoff window length in terms of polling cycles
    $w_i = \min\{w_{\max}, 2^{c_i}\}$
  - After each polling cycle the window length is reduced
    $w_i = \max\{0, w_i - 1\}$
  - Slave is only egligible for polling if
    $w_i = 0$
- In order to save power, a slave that is not active can be parked untill the backoff window have expired. A parked slave is only maintaining synchronization, but otherwise it is not listening for the radio channel.

Bluetooth

- The network controlled by one master is called piconet.
- In principle it is possible to form a multi-hop network (scatternet) by using a node which is a slave of two masters. The gateway node has to resign one piconet and join another to relay packets. This can be slow process.
- Benefits of Bluetooth
  - Can be used replace wired serial connections.
  - Supports circuit switched connections for voice transport.
- Draw backs
  - Large protocol stack
  - Not energy efficient
  - Service discovery is slow

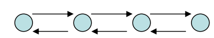


STDMA

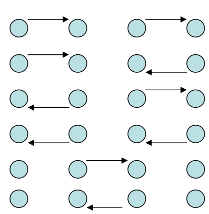
- Spatial Time Division Multiple Access
  - All links are synchronized and time is divided into time slots.
  - Time slots can be spatially reused by links that do not interfere (too much) with each other
    - Link based: Links are grouped into transmission sets that can transmit simultaneously. (Unicast channels)
    - Transmitter based: Transmitters are grouped into transmission sets so that all nodes within a transmission range of a node can receive the data. (Broadcast channels)

STDMA

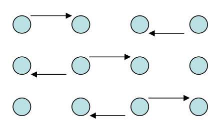
- Network



- Link based STDMA: Feasible transmission groups



- Transmitter based STDMA: Feasible transmission groups



STDMA

- Problem formulation
  - SINR of link i in transmission group k

$$\gamma_{ik} = \frac{g_{ii} p_{ik}}{\sum_{\substack{j \in I_k \\ j \neq i}} g_{ij} p_{jk} + \upsilon_i}$$

I_k set of transmitters active in group k

  - Data rate of link i in transmission group k

$r_{ik} = f(\gamma_{ik})$ **E.g.** $f(\gamma_{ik}) = W \log_2 (1 + \gamma_{ik})$

  - Scheduling constraint

$$\sum_k \phi_k r_{ik} \geq r_i$$

ϕ_k Fraction of the scheduling interval allocated to group k

r_i Minimum rate requirement for link i

STDMA

- Optimal scheduling

$$\max \sum_i U(r_i(\phi))$$

$$\sum_k \phi_k r_{ik} \geq r_i$$

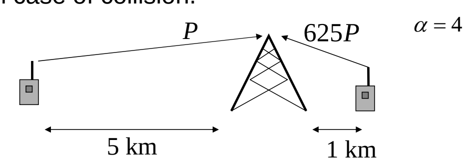
- Curse of dimensionality, the number of different transmission groups grows quickly as the number of links grow.
- Column generation methods can be utilized to determine required transmission groups (Björklund *et. al.*, 2003)

ALOHA

- ALOHA protocol was developed by the University of Hawaii for packet radio communication between terminals and mainframe computer. It is (one of) the first MAC protocol for packet radio (ad hoc) networks.
- A node having traffic to transmit will transmit
- In case of collision, a node will backoff for random time instant to try again.
- If the operation of the network is synchronized, probability of collision can be decreased and the throughput increased.
- In wireless ad hoc network, capture effect can be utilized. A transmission is received correctly if the received SINR is large enough.

ALOHA

- Power received from a transmitter close to the receiver can be significantly larger than from far away. Hence, SINR can be above the treshold for one of the links even in case of collision.

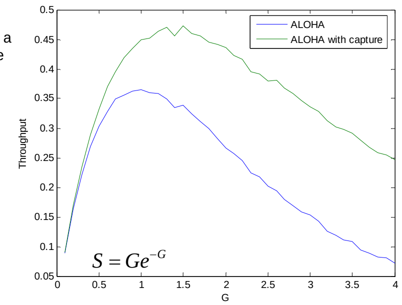


P_{tx} Transmit power

$P_i = \frac{1}{r_i^{\alpha}} P_{tx}, \quad i = 1, 2, \quad 2 \leq \alpha < 5$ Received power

ALOHA

- Slotted ALOHA
  - The nodes are randomly placed in a range from 100 to 1000 m from the base station.
  - The transmit power is 21 dBm and noise power is -140 dBm.
  - Attenuation factor α=4
  - SINR-target Γ=10 dB



Traffic volume

Simulation result is averaged over 10000 time slots.

CSMA/CA

Carrier sensing medium access.

- A node listens for the channel. If there is ongoing traffic, it will backoff; otherwise it will transmit.

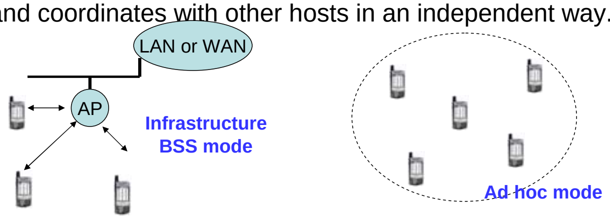
Collision avoidance

- RTS (Request-to-send) – CTS (clear to send) handshake is utilized before transmission to avoid hidden and exposed node problems.

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Type of IEEE802.11 WLAN

- WLAN can be categorized into two types: infrastructure and ad hoc.
- In an infractucture WLAN, every mobile host is under the control of a Wireless Access Point (WAP).
- In an ad hoc WLAN, every mobile host is autonomous and coordinates with other hosts in an independent way.



University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

IEEE 802.11 MAC layer

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Distributed Coordinate Function (DCF).
- A Source node first senses the channel for DIFS (DCF Interframe Space) interval, then the node sends DATA packet.
- The Dest node sends ACK back after a SIFS (Short Interframe Space) interval to garuantee the packet delivery phase.
- All other nodes hold one DIFS and start a random backoff before sending a new data packet.

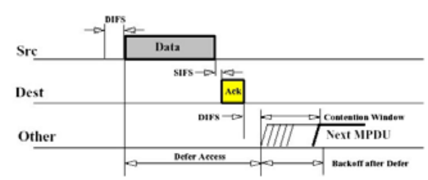
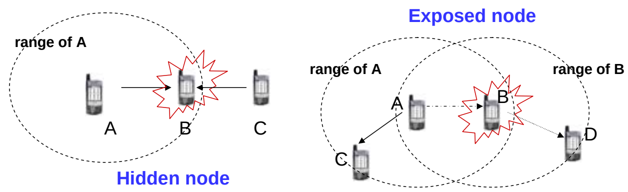


Figure 7 CSMA/CD Back-off Algorithm

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

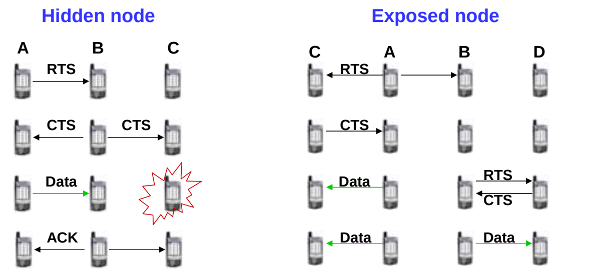
Hidden and Exposed Node Problem

- When not all the nodes can hear each other, hidden node and expose node problems may occur.



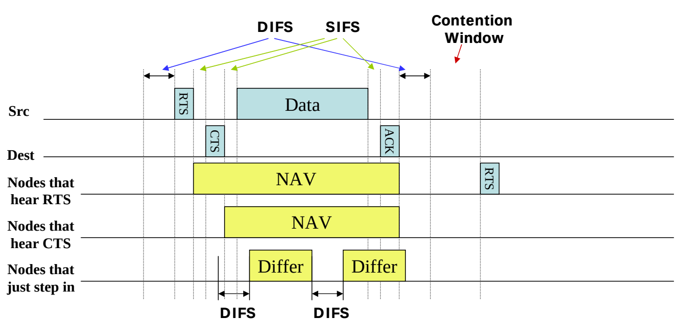
Solution: RTS/CTS

- Before sending the DATA packet, the Src node sends a RTS (Request to Send).
- Upon the reception of RTS, the Dest replys a CTS (Clear to Send).



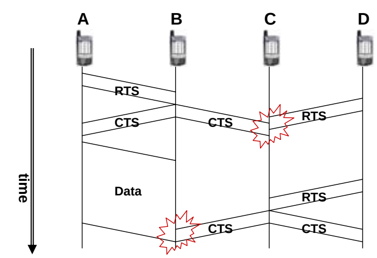
RTS/CTS/DATA/ACK with NAV

- NAV: Network Allocation Vector



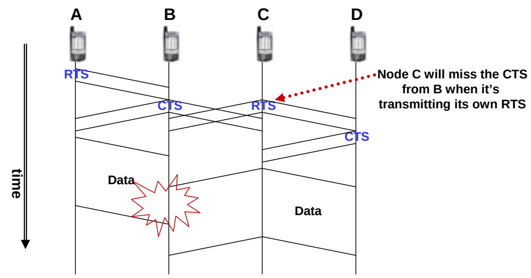
RTS/CTS Flaw (1)

- Because RTS/CTS are broadcast without ACK, nodes are not aware of the collision of this kind of packets.



RTS/CTS Flaw (2)

- Due to the use single antenna, a node cannot hear anything when transmitting.

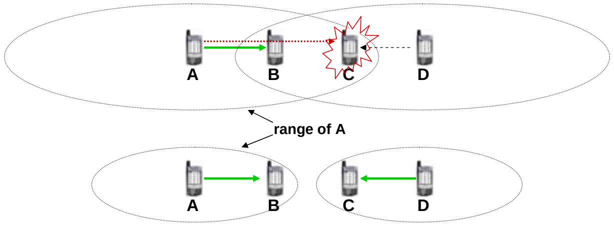


MAC Layer Energy Efficiency

- Power Control
  - basic idea
  - drawbacks
  - realization
- Sleep mode
  - in infrastructure mode
  - in ad hoc mode

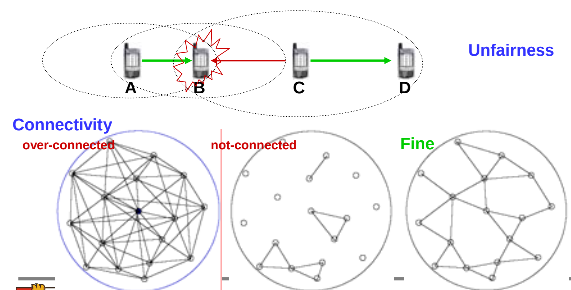
Power Control – Basic Idea

- Power control is to dynamically adjust the transmit power so that the remote node can be reached by minimum power.
- Reduction of Tx power can also improve the network throughput.



Drawback of Power Control

- Unfairness: the communications with higher power have more chance to get the radio channel.
- Connectivity: the whole (ad hoc) network must be fully connected, but should not be over-connected (large interference, spatial reuse not possible).



Power Control

- A node can estimate the received signal quality based on the Beacon signal of WAP.
- RTS and CTS packets can be used to determine the received signal quality.
- Due TDD, uplink and downlink channels have approximately the same attenuation. Hence, based on the received power a node can determine how large its transmit power should be.

Power Control

- Power control algorithm

$$P^*_{tx} = P_{tx} - P_{rx} + P_{min} + M$$

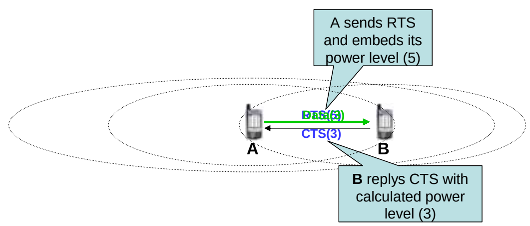
where

P^*_{tx} : the required power to transmit a packet to the remote node,
P_{tx} : the transmit power used by the remote node,
P_{min} : the minimum power required to receive a packet,
M : safty margin for channel fluctuations.

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Power Control

- Example (MACA with power control)



University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Sleep Mode in Infrastructure

- A node consumes much less energy in sleep mode.
- Example: Cisco Aironet 350 802.11b PC card
  - Transmit: 450mA
  - Receive: 270mA, Idle mode is similar to it
  - Sleep: 15mA
- In an infrastructure WLAN, sleep mode is coordinated by the WAP(s).
  - When a node is sleeping, the WAP buffers all the incoming packets for it.
  - The node periodically wakes up and listens to Beacons from the WAP.
- The drawback of sleep mode is the increment of delay.

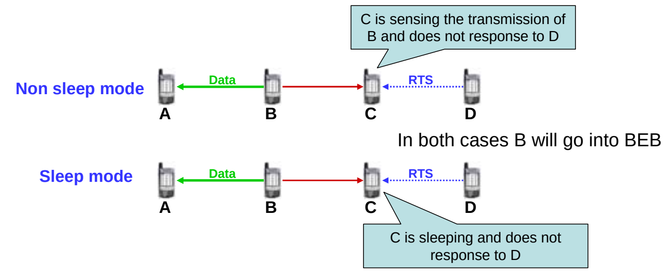
University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

Sleep Mode in Ad-hoc: PAMAS

- In an ad hoc WLAN, sleep mode is a distributed function at MAC or Network Layer.
- PAMAS – Power-Aware Multi-Access protocol with Signalling for ad hoc networks
  - Separate Signalling Channel: RTS/CTS and busy tones use a separate channel.
  - 6 different states: Idle, Transmit, Receive, Await Packet, Await CTS, and BEB (Binary Exponential Backoff).
- PAMAS Sleep Mode:
  - If a node has no packet to send, if should power off itself if a neighbor begins transmitting.
  - If at least one neighbor is transmitting and another is receiving, it powers off itself (even has packets to send).

PAMAS Example

- Sleep mode does not degrade the performance significantly.
- PAMAS achieves 10% to 70% power conservation compared to MACA



Sensor-MAC (SMAC)

- Designed to save energy in a multihop sensor network
- Based on 802.11 CSMA/CA
- Main components:
  - Periodic listen and sleep
  - Collision avoidance
  - Overhearing avoidance
  - Message passing

(W.Ye, J. Heidemann and D. Estrin, 2002)

Virtual Clustering & Synchronization

- Virtual Clustering makes a group of nodes close to each other to be synchronized to wake-up/sleep.
- The first node turned on will act as cluster header to synchronize other nodes.
- Nodes that can hear from two or more cluster headers will use multiple schedules to exchange data between clusters.
- SMAC can reduce the energy consuption up to 50% in heavy traffic (more in light traffic).
- SMAC makes a tradeoff between energy consumption and latency
- Long synchronization period makes the protocol not suitable for high mobility networks.

SMAC

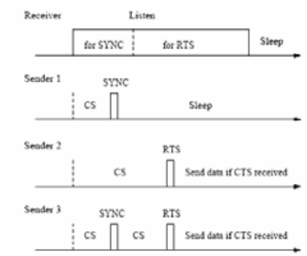


Fig. 3. Timing relationship between a receiver and different senders. CS stands for carrier sense.

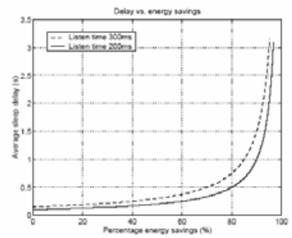


Fig. 5. Energy savings vs. average sleep delay for the listen time of 30ms.

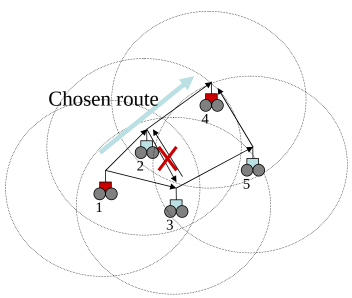
Network layer

- Routing strategies
- Effects of MAC
- Effects of physical layer
- Energy efficiency
  - Combined power control and routing
  - Signaling overhead

Network layer

- Routing strategies
  - Proactive:
    - Nodes maintain routing tables.
    - Tables need to be updated when topology changes.
  - Reactive
    - Route is determined based on demand.
    - If there is no traffic on particular route, no routing table entries are stored.
  - Hybrid/hierarchical protocols

List of routing protocols can be found e.g. http://en.wikipedia.org/wiki/Ad_hoc_protocol_list



IETF AODV Protocol

Ad Hoc On Demand Distance Vector

- Reactive routing:
  - If there is no route between source and destination RREQ packet is flooded in the network
  - Node that knows route to destination answers by sending RREP packet
  - Signaling packets are normal UDP/IP packets

Route Request

RREQ Header:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|  Reserved           |  Hop Count        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Flooding ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Destination Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source IP Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source Sequence Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


Route Request

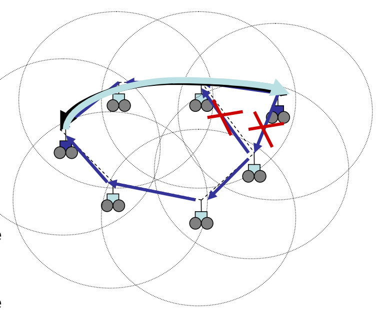
- Type = 1 "standard" AODV
- J,R reserved for multicast
- G: Gratuitous RREP flag, if set RREP will be generated and unicast to source
- Reserved: Reserved for future use
- Flooding ID: Each RREQ packets is given unique ID number to detect multiple copies

Route Request

- Two counters for virtual time
  - Orginator sequence number: When a packet generates RREQ it increases the counter by one
  - Destination sequence number: The last known value of the counter at the destination node
- Hop count: Number of hops in a path from source to destination.
  - When RREQ packet is forwarded, the hop count is increased by one

Determining the Route

- If there is no route, a source will broadcast RREQ packet
- When a node receives an RREQ packet it will store the protocol header information into the routing table.
- If the node already has received RREQ with the same ID, the packet will be discarded.
- If the ID number is greater, routing table will be updated and the RREQ packet forwarded (broadcast).
- If the destination node hears RREQ, it will issue RREP which will be unicasted using the route used by the RREQ.
- When a node hears RREP, it will store the routing table entries it made earlier.
- If a node does not receive RREP in some time window T, it will discard the routing table entries.
- When source receives the RREP it will start data transmission using the route.



Routing Table

- Contents of the routing table:
  - Destination IP address
  - Destination Sequence Number
  - Valid Destination Sequence Number Flag
  - Network interface (wlan, wpan, ethernet, etc.)
  - Next Hop
  - List of precursors (neighbors that are likely to use the node as a relay node)
  - Lifetime

Route Response

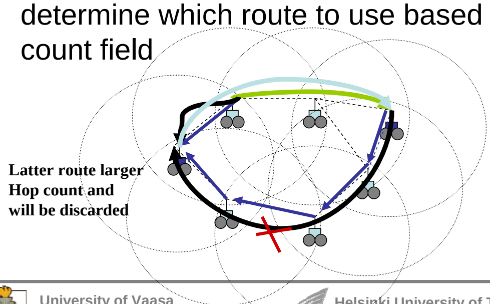
- RREP packet

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

  - R: Repair flag
  - A: Acknowledgement required
  - Lifetime: How long the route will be maintained in the intermediate nodes.

Route Response

- If a node knows the route to the destination, it will issue RREP packet.
- If source gets multiple copies of RREP it will determine which route to use based on the hop count field

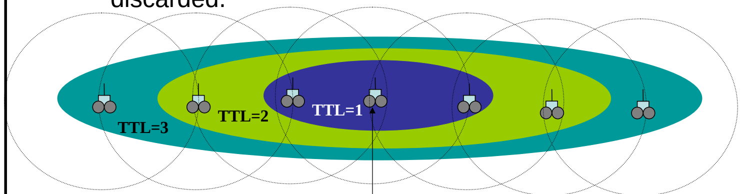


HELLO Exchange

- In order to detect topology changes, nodes periodically broadcast HELLO messages, once in HELLO_INTERVAL.
- If a node does not receive HELLO from a neighbor used in some route, it will issue a RERR packet which will be unicast to the source.
- When a node receives RERR it will remove the corresponding routing table information.
- When a source receives RERR it will issue a new RREQ packet.
- Due to the HELLO exchange, the neighbors of destination already know route to the destination and can issue the RREP packet.
- HELLO packet is simply RREP packet with time-to-live set TTL=1, Hop Count =0 and Sequence Number set to correspond to the node broadcasting the HELLO.

Flooding

- Flooding of RREQ causes lot of overhead.
  - Limit the propagation of the packets to control the time-to-live TTL field of the IP header of the RREQ.
  - When a router relays the packet it will subtract one from the TTL field. Packets with zero TTL are discarded.



Interaction with MAC Layer

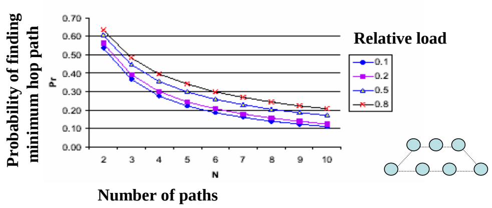
- MACA with
- Congestion on the MAC protocol will cause random delays to the RREQ packets

=>The first packet to arrive destination is not necessarily the one corresponding to the shortest route.

Interaction with MAC Layer

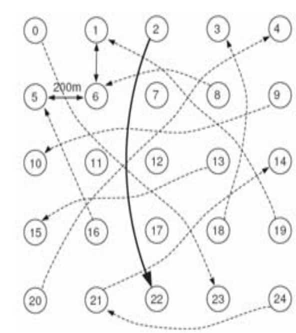
- Analytical study assuming that contention delay is geometrically distributed. Transmission in a link sees occupied channel with probability p (uniform traffic).
- A path with H hops is delayed due to k contentions

$$\Pr(H,k) = \binom{H-1+k}{H-1} p^k (1-p)^H, k = 0, 1, 2...$$



Interaction with MAC Layer

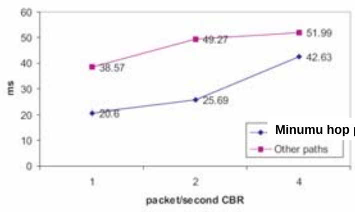
- Simulation study witn NS2
- Grid topology 5x5 nodes
- Random CBR links established before we examine the route establishment between 2 to 22.

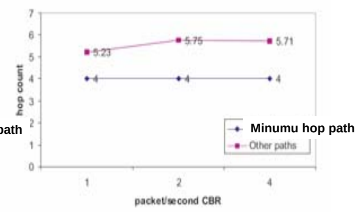


Interaction with MAC Layer

Simulation results

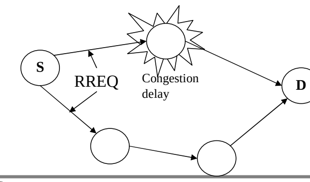
- Average end to end packet delivery delay
- Average hop counts

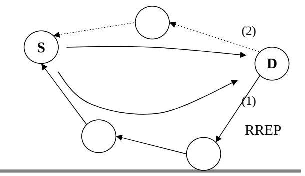




Interaction with MAC Layer

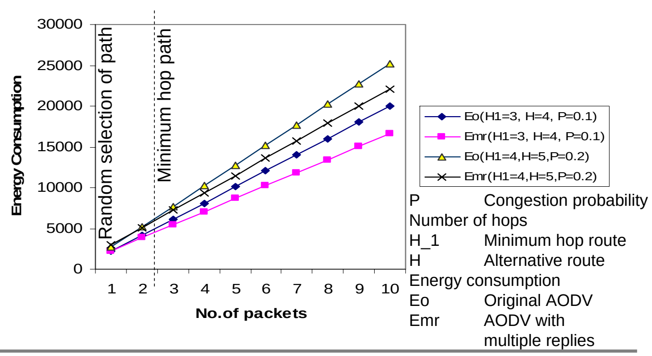
- Minimum hop path can still be found by issuing multiple route replies
  - The destination replies all the incoming RREQ packets.
  - The source will start traffic transmission when the first RREP comes.
  - The source will compare the hop count with that in every later arrived RREP and select the smaller one to continue.





Interaction with MAC Layer

- There is a tradeoff between increases network layer overhead and energy consumption and latency of the data transmission



Interaction with Physical Layer

- Gray zone problem: Data transmission is not possible although HELLO messages indicate neighbor reachability.
  - Packet loss probability depends on the packet length and data rate. Signaling messages tend to be shorter and transmitted with lower data rate than data packets.
  - There are no ACK for HELLO, hence HELLO does not guarantee that bidirectional communication is possible
  - Links are fluctuating. Single successful HELLO does not give information on the average link condition.

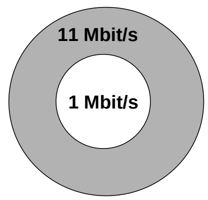
Interaction with Physical Layer

- Cisco 802.11b product Aironet 350 WLAN PC card also shows that the range of gray zone is quite significant.

Rate	Indoor	Outdoor
1Mbps	107m	610m
11Mbps	40m	244m

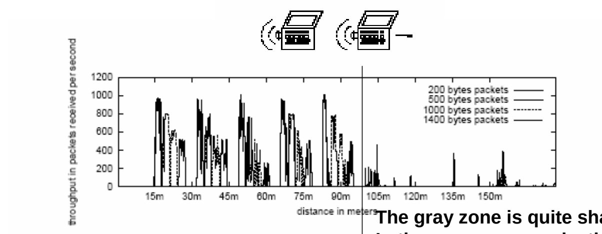
TABLE I

CISCO A350 RADIO RANGE



Interaction with Physical Layer

- Experimental result by Dhoutaut *et. al.*



The gray zone is quite sharp
In the zone, communication
Is hardly possible at all
While outside the zone packet
Losses are small.

Interaction with Physical Layer

- Gray zone can be taken into account by
  - Determining the reachability based on several consecutive HELLO messages
    - If several HELLO messages are received correctly, a link is considered to be active; otherwise it is considered to be broken.
  - Using SINR-margin:
    - If SINR of the received HELLO message is larger than minimum SINR required to receive higher bit rate/ longer packet correctly, then the link is considered to be active; otherwise it is considered to be broken.
  - Using some routing scheme that select only short links (e.g. power aware routing)

Energy Efficiency of Network Layer

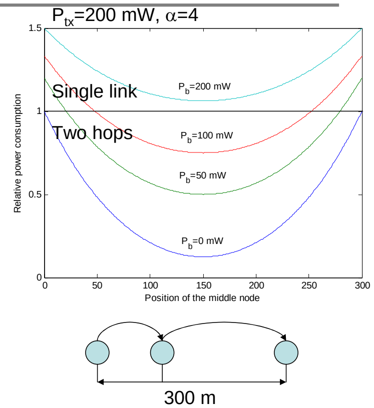
- Multi-hop transmissions
- Power-aware routing

Energy Efficiency of Network Layer

- *Ideal power control*: Transmitter power is a function of the link d length

  $P_{tx} \sim d^{\alpha}$ $\qquad \alpha = 2 \ldots 4.5$

- From transmit power point of view it is beneficial to use short links and multiple hops.
- The baseline power consumption P_b, i.e. power consumed by the transmitter and receiver electronics, is the limiting factor!



Energy Efficiency of Network Layer

- Energy consumption of reactive routing in random network topology as a function of transmit power.
  - In a unit square, the expected distance between two random-selected nodes is

$$E\{\mathcal{D}\} = \underbrace{\int_0^1 \cdots \int_0^1}_{4} \sqrt{(x-u)^2 + (y-v)^2}\,dx\,du\,dy\,dv$$
$$= \frac{1}{15}\left[\sqrt{2} + 2 + 5\ln(1+\sqrt{2})\right]$$
$$= 0.521405433\ldots$$

Energy Efficiency of Network Layer

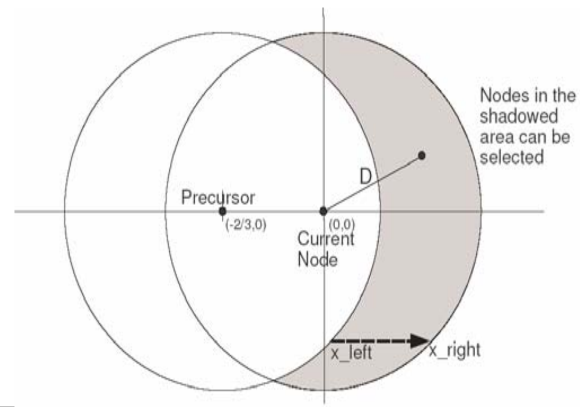
- The expected distance of the hop from the source node to the first routing node is

$$E\{D_1\} = \int_0^R r p(r) dr = \frac{2}{3}R$$

- While $p(r) = 2r/R^2$
- For an intermediate node, only those nodes that have not received a RREQ can be the next hop candidates

$$E\{D_{i,i>1}\} = \frac{1}{A_s}\iint_{A_s} \sqrt{x^2 + y^2}\,dx\,dy$$
$$\approx 0.7670R$$

Energy Efficiency of Network Layer



Energy Efficiency of Network Layer

- Suppose we have a square of A^2, thus the average end-to-end distance $E\{\mathcal{D}\} = 0.5214\sqrt{A}$
- With a proper routing protocol, by which the least-hop route will be selected, we can derive the expected route distance in term of hop counts, denoted as:

$$E\{D(A,R)\} = \frac{E\{\mathcal{D}\} - E\{D_1\}}{E\{D_{i,i>1}\}} + 1 \approx \frac{0.5214\sqrt{A} - 0.6667R}{0.7670R} + 1$$

Energy Efficiency of Network Layer

Simulation study

- **AODV routing protocol**
- **Cisco Aironet 350 802.11 WLAN card with 5 Tx power levels. Two extra levels (0, and -1) are added to inspect the performance of longer route distance.**
- **P_{rx} is 50mW for all the cases.**
- **200 nodes are randomly distributed in a 400 x 400 m² square.**

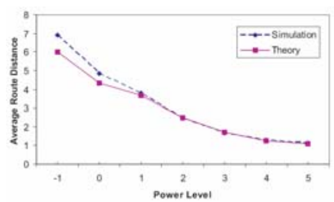
Level	P_{tx_i} (mW)	Radio Range	Number of Hops	Energy consumption
-1	0.2	48.2	5.99	301.01
0	0.5	67.1	4.34	219.38
1	1	79.8	3.67	187.35
2	5	119.3	2.50	137.53
3	25	178.4	1.72	128.66
4	100	252.3	1.25	187.70
5	200	300	1.07	268.30

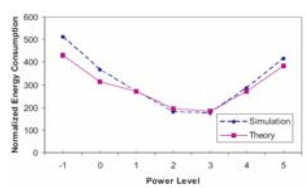
TABLE II

TRANSMIT POWER SETTING IN SIMULATION AND THE EXPECTED RESULTS

Energy Efficiency of Network Layer

- With WLAN type of radio having relative high receiver power consumption on should use moderate transmit powers 5…25 mW and short 1 – 3 hop paths.





Power control

- Power control can be utilized on MAC layer to control spatial reuse and to minimize power consumption.
- Change of transmit power causes topology to change as well requiring rerouting.
- Power control should be taken into account on network layer.

PAR: Power Aware Routing Protocol

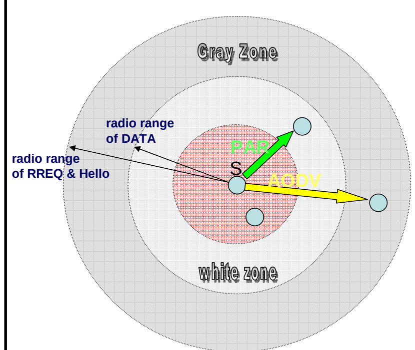
- Hop-by-hop power control. At MAC layer, RTS/CTS handshake uses maximum power to avoid collisions. This handshake will also result to a close loop power control so that the DATA packet can be transmitted by a proper power level.
- RREQ is broadcast with maximum power.
- An intermediate node calculates the *hop weight* of a received RREQ, and puts the *accumulated hop weight* into the RREQ to broadcast it.

$$W_h = |P_r - P_{opt}|.$$

PAR: Power Aware Routing Protocol

- Upon receiving a duplicated RREQ, the node compares the new accumulated hop weight with the previous one. If it is found that the new weight is less, it will update its routing table.
- A gray zone alarm RERR is issued when a node detects several consecutive reception failures.

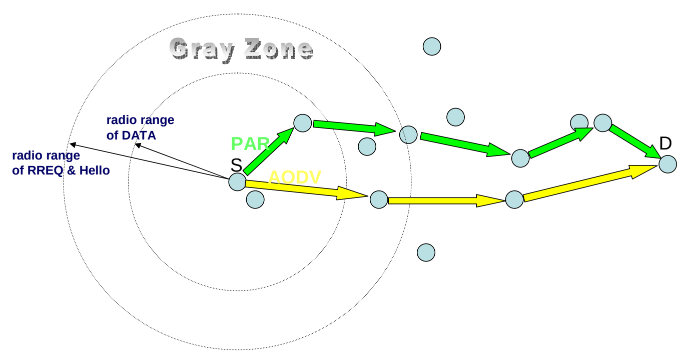
PAR: Power Aware Routing Protocol



- To avoid too short and too long distance, which regarded as energy-inefficient zone and gray zone respectively, a power threshold is given.

$$W_h = |P_r - P_{opt}|.$$

PAR: Power Aware Routing Protocol



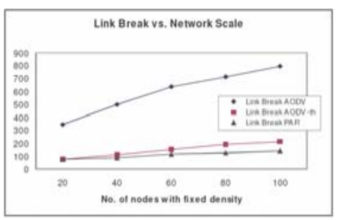
Energy Efficiency of Network Layer

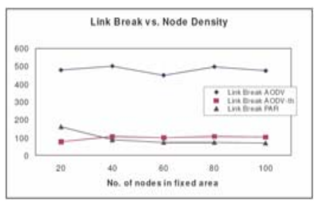
- In the previous example
  - AODV: 3 hops $P_{AODV} = 3P_{tx} + 3P_{rx}$
  - PAR: 5 hops $P_{PAR} = \sum P_{tx}^{*} + 5P_{rx}$ $P_{tx}^{*} \approx 0.1P_{tx}$
  - When the hop distance of PAR is 50% of AODV,
  - Thus $P_{PAR} \approx 0.5P_{tx} + 5P_{rx}$
  - If $P_{rx} \approx 0.5P_{tx}$, then $P_{PAR} = 3.0P_{tx}$ and $P_{AODV} = 4.5P_{tx}$

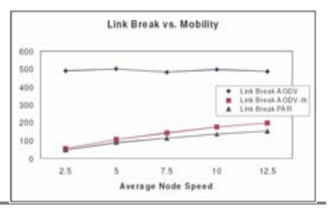
Effect of Network Layer Power Control

- Comparison study
  - AODV
  - AODV with SINR treshold to compensate for the gray zone
  - PAR
- NS2 simulation (Gray zone 40% of max radio range)

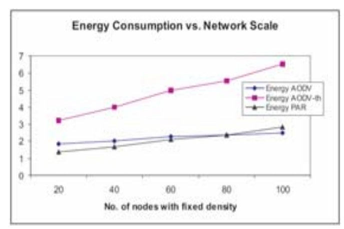
Link Stability

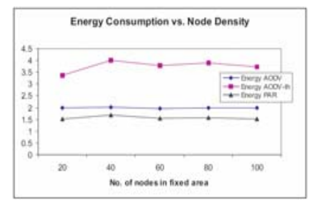


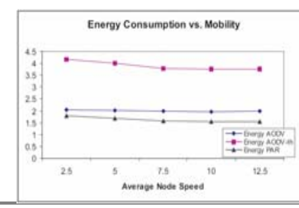




Energy Consumption

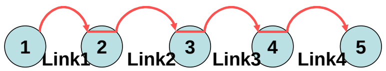


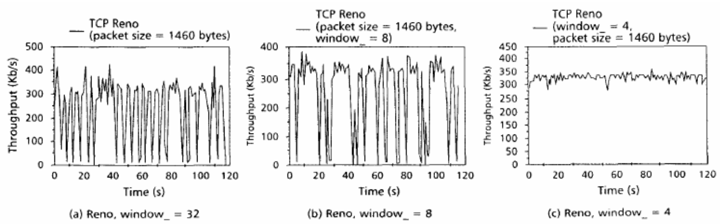




Transport Layer

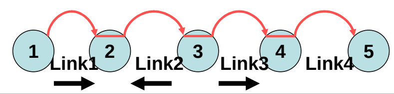
- TCP performance depends on the maximum window size.





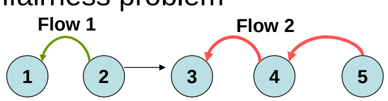
Transport Layer

- If window size is large, a lot of data is generated by the source. This means that node 1 makes frequent transmission attempts.
- Traffic traveling in link 3 can collide with link 1 and traffic in link 4 can collide with link 2.
- If there are seven consecutive collisions, packet is lost. Link is considered to be broken, and rerouting is done.
- Lost packet causes TCP to decrease the window size and packets get transmitted.
- After receiving successful ACK, TCP will increase the window size once again.
- The result is highly oscillatory flow.



Transport Layer

- Unfairness problem



- Assume that Flow 2 is initially in progress
- When node 2 transmits, node 3 sets NAV, and transmission attempt from node 2 sees collision and backs off.
- When it becomes active, there is high probability that it once again collide with the transmission between nodes 2 and 1.
- After failing 7 times, it the packet gets lost, route is considered broken and rerouting is attempted.
- Eventually TCP will time out, since not traffic gets transmitted.

Transport Layer

- C. Tschudin and E. Osipov (2004), concluded that the TCP horizon, i.e. max number of hops that could be used in IEEE 802.11 based Ad hoc network is around 1 – 3.

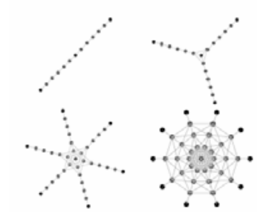


Fig. 1. "Beam star" network topologies for various numbers of beams and beam lengths (2x6, 3x6, 6x6, 10x4) shown with potential connectivity. (The last figure is shown with a different scale: the internode distance along a beam is identical for all topologies.)

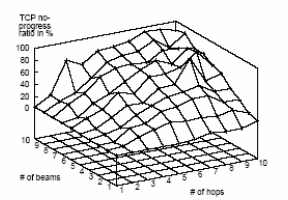


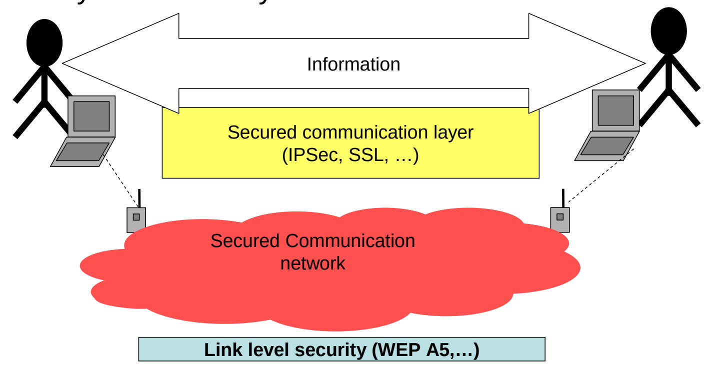
Fig. 2. Worst accumulated TCP no-progress time for AODV, in dependency of the number of beams and their length.

Security in Ad Hoc Networks

- Security problems:
  - Wireless communications:
    - Any outsider can eavesdrop the communication
    - Any outsider can generate traffic to the network
  - Nodes act as mobile relays or routers:
    - Routers can be compromised, there can be malicious routers
    - Rapid changes in topology makes it difficult to detect intrusions
  - Nodes are not physically protected
    - There is considerable risk that nodes are physically harmed, tampered or stolen and their information content is compromised

Security in Ad Hoc Networks

- Layers of security



Security in Ad Hoc Networks

- Security threats
  - Eavesdropping
  - Impersonation
  - Modification
  - Replay
  - Routing disruption
  - Denial of service (DoS) attack
  - Jamming (physical layer DoS)
- Security measures
  - Encryption
  - Authentication
  - Securing integrity with running packet number
  - Authentication of signaling information
  - Filtering traffic, reconfiguring routes
  - Spread spectrum communications

Security in Ad Hoc Networks

- Network layer security requires packet level authentication (PLA):
  - Every packet can be checked for authenticity, integrity, non-repudiation, timeliness, ...
  - Any node in the network can do the PLA checking
- PLA checking should not require previous negotiation or exchange of security parameters between the sender and verifier. (Analogous to holograms and watermarks in bills.)
- Cannot be done using secured communication layer end-to-end protocols like IPSec

(Kari, 2004)

Security in Ad Hoc Networks

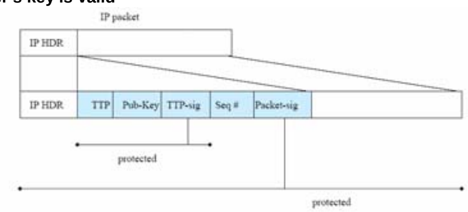
- Benefits of PLA
  - Strong access control
  - Only right packets are routed
  - Easy to implement in hardware
- Disadvantages
  - Increased packet size (~60-100 bytes)
  - Requires strong crypto algorithms
  - More computation per packet

Security in Ad Hoc Networks

- PLA implementation

Extra header per packet:

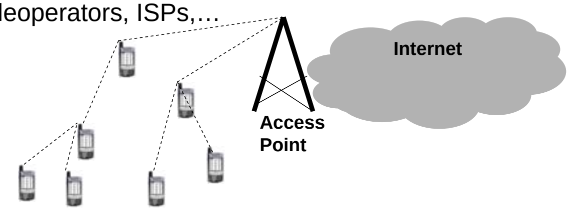
1. **Authority**
2. **Public key of sender**
3. **Authority's signature of sender key and validity time.**
   Authority's assurance that the sender's key is valid
4. **Sending time (+sequnce number)**
   Possibility to remove duplicates and old packets
5. **Signature of the sender of this Packet.**
   Sender's assurance that he has sent this packet



Security in Ad Hoc Networks

Authority

- Networks with access points to fixed core network: Network of trusted third parties that issue certificates.
  - Teleoperators, ISPs,…



Security in Ad Hoc Networks

Pure ad hoc networks

- Central authority:
  - Network has a special purpose server that act as an centralized authority.
  - Not practical, a node could be out of the reach of such server or the server could be damaged.
- Partially distributed authority:
  - Some nodes act as certification authorities CAs for *public keys*.
  - The distribution can be achieved using a secret sharing scheme. Each CA create partial certificate.
  - Only by combining a threshold number of such certificates can the whole certificate be issued.

Security in Ad Hoc Networks

– Fully distributed authority
  - All nodes are equal, all of them act as certification authors
  - Some extra measures are needed to prevent attacker from being able to act as an authority.
  - Proactive secret sharing method is needed, in which the secret is changed after some time. There also needs to be a method to determine whether the secret is valid.
  - Problem: How the nodes initially achieve the certificates when they join the network?

Security in Ad Hoc Networks

– Group identity
  - Nodes that can participate into the network form a group.
  - Each member of the group has physically stored common secret.
  - Individual authentication is not possible. It can only be checked whether the node is a member of a group.
  - Group identity could be useful in wireless sensor and actuator networks.

– Self-issued certificates
  - There exist no form of authority at all; instead every node will decide themselves whom to trust.
  - This approach could be useful in some peer-to-peer applications.

References

Connectivity and capacity

- P. Gupta and P. R. Kumar, "Critical Power for Asymptotic Connectivity in Wireless Networks," A Volume in Honor of W.H. Fleming in Stochastic Analysis, Control Optimization, and Applications, 1998.
- P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, Vol 46., No., 2, March 2000.
- X.-Y. Li, Y. Wang, P.-J. Wan, C.-W. Yi, O. Frieder, "Robust Wireless Ad Hoc Networks," In *Proc. IEEE ICC'03*, 2003.
- P. Gupta, A Correction to the Proof of Lemma in "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, Vol. 49, No. 11, November 2003.
- M. Grossglauser and D. N. C. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Network," IEEE Transactions on Networking, Vol. 10, No. 4, August 2002.

MAC

- P. Björklund, P. Värbrand, and D. Yuan, "Resource optimization of spatial TDMA in ad hoc radio networks: A column generation approach," In Proc. *IEEE Infocom*, San Francisco, CA, April 2003.

References

- W.Ye, J. Heidemann and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," In *Proc. 21st International Annual Joint Conference of the IEEE Computer and Communications Societies,* 2002.
- C.S. Raghavendra and S. Singh, "PAMAS – Power-Aware Multi-Access Protocol with Signaling for Ad Hoc Networks," *ACM Computer Communication Review*, 1998.

Network layer

- C. Perkins, Ad hoc On-Demand Distance Vector (AODV) Routing, Experimental RFC 3561, July 2003. Available in www: **http://www.ietf.org/rfc/rfc3561.txt**
- C. Gao and R. Jäntti, "Least-Hop Routing Analysis of On-Demand Routing Protocols" in Proc. *IEEE ISWCS 2004,* 2004.
- S. Singh, M. Woo and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," *ACM International Conference on Mobile Computing MobiCom,* 1998.
- C. Gao and R. Jäntti, "A Reactive Power-Aware on-Demand Routing Protocols for Wireless Ad Hoc Networks," in *Proc. IEEE VTC 2004 Spring,* 2004.
- D. Dhoutaut and I. Guerin-Lassous, "Experiments with 802.11b in ad hoc configurations," In Proc. *Workshop on Mobile Ad Hoc Networking and Computing Madnet* 2003, France

References

Transport layer

- S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks", IEEE Communications Magazine, June 2001.
- C. Tschudin and E. Osipov, "Estimating the Ad Hoc Horizon for TCP over IEEE 802.11 Networks" in *Proc 3rd Annual Mediterranean Ad Hoc Networking Workshop* (Med-Hoc-Net 2004) June 27-30, 2004, Bodrum, Turkey

Security

- E. Blomqvist, Security in Sensor Networks, Control Engineering Laboratory, Helsinki University of Technology, Report 135, 2003.
- L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," *IEEE Networking Magazine*, November/December, 1999.
- H.H. Kari, "Military grade wireless ad hoc networks ," Presentation at ONRIFO, 2004. Available in www: **http://www.tcs.hut.fi/~hhk/pdf/pdf.htm**

General

- M. Ilyas, ed. The hand book of Ad Hoc Wireless Networks, CRC Press, 2003.

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory

University of Vaasa
Department of Computer Science
Helsinki University of Technology
Control Engineering Laboratory