WirelessHART

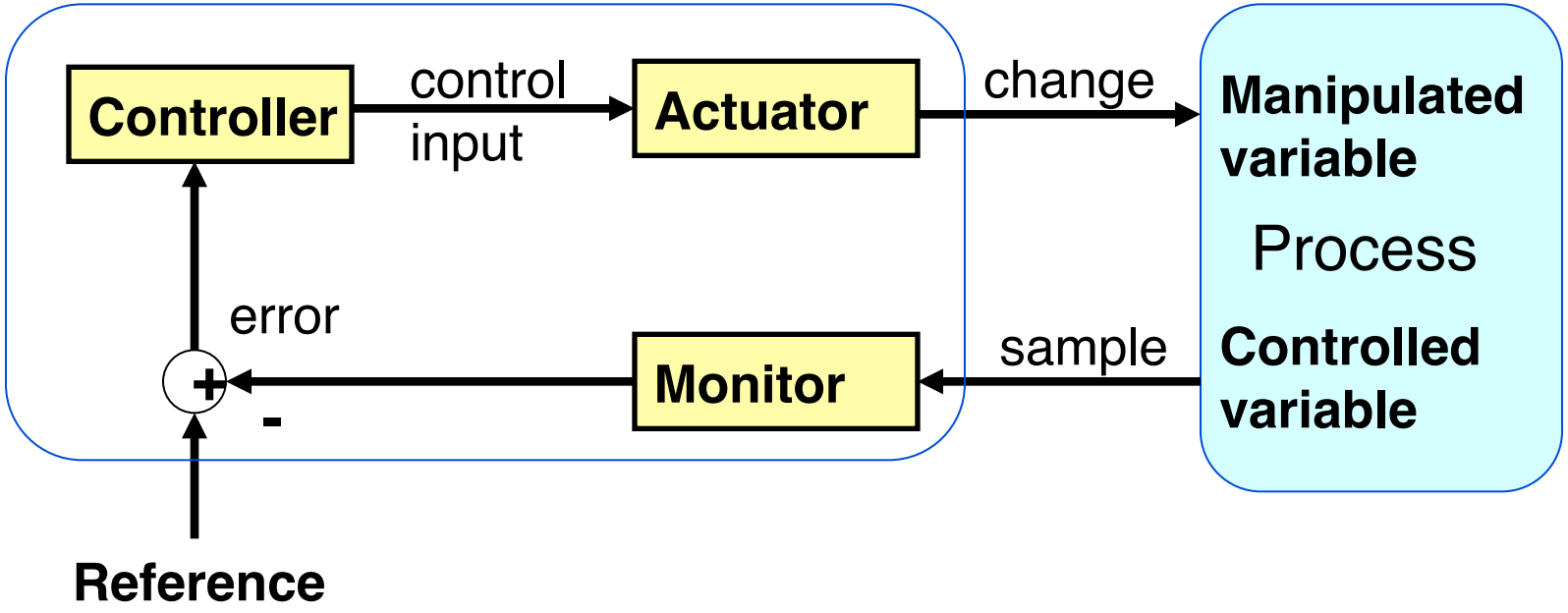
Wireless Technology for Process Industries

Chenyang Lu

Computer Science and Engineering

Process Control

- Feedback control loop controls the output of specific process
  - Ex: maintaining constant temperature by controlling heat supply
- Strategy: Centralized and peer-to-peer control



Why

- Production efficiency through environment maintenance
- Detect leaks and releases before they lead to environmental problems
- Monitor the status of manually operated valves
- Monitor safety relief valves to detect venting to avoid accidents.
- Health, Safety, and the Environment (HSE) regulations

How

- Feedback control via wireless control networks (WCNs).

- Advantages
  - Man power reduction
  - Reduced risk of personal injury
  - Reduced error by human reading
  - Easier and on-time control by field instrumentation through on-time reporting to the control room

Why WCNs

- Cost reduction: there are many remote locations where putting wire or cable is economically infeasible
- Easier installation: many places are inaccessible
- Enhanced control
- Easier maintenance:
  - a wired network is not suitable for plants due to severe heat or exposure of chemicals
  - a wireless infrastructure can remain in place for many years.

Challenges in Wireless Control

- Stricter timing requirement
- Higher security concerns
- Requires reliable communication despite wireless deficiencies
- Plant environments are inherently unreliable
  - Interferences, obstacles, power failures, environmental factors such as lightening, storms.

Wireless Technology

- Existing standards fail in industrial environments
  - ZigBee: static channel
  - Bluetooth: quasi-static star network

- WirelessHART
  - For process measurement & control applications
  - First open and interoperable wireless standard to address the critical needs of real-world industrial applications

Wireless Technology

- WirelessHART released in Sep 2007 (as a part of HART 7 Specification)

- HART (Highway Addressable Remote Transducer Protocol)
  - Most widely used field communication protocol (30 million devices worldwide)

- WirelessHART adds wireless capabilities to the HART protocol while maintaining compatibility with existing devices, commands and tools.

WirelessHART Use Cases

- Improving the control of plant steam supply by detecting "cool spots" in cross plant steam lines
- Reducing risk of overfilling tanks by adding redundant level measurements (in oil and petroleum refineries)
- Monitoring and control of safety valves
- Monitoring and control of pressure and/or temperature process fluids & gases

WirelessHART PHY

- Adopts IEEE 802.15.4
- On top of that, defines its own MAC
- Same 16 mutually orthogonal channels
- Operates in the 2.4GHz ISM band
- Data rate of up to 250 kbps

WirelessHART Radio Tranceivers

- Omni-directional
- Half-duplex
- 100 meters LOS @ 0 dB
- Time to switch between channels: 0.192 ms
- Radio Turn-on time: 4ms

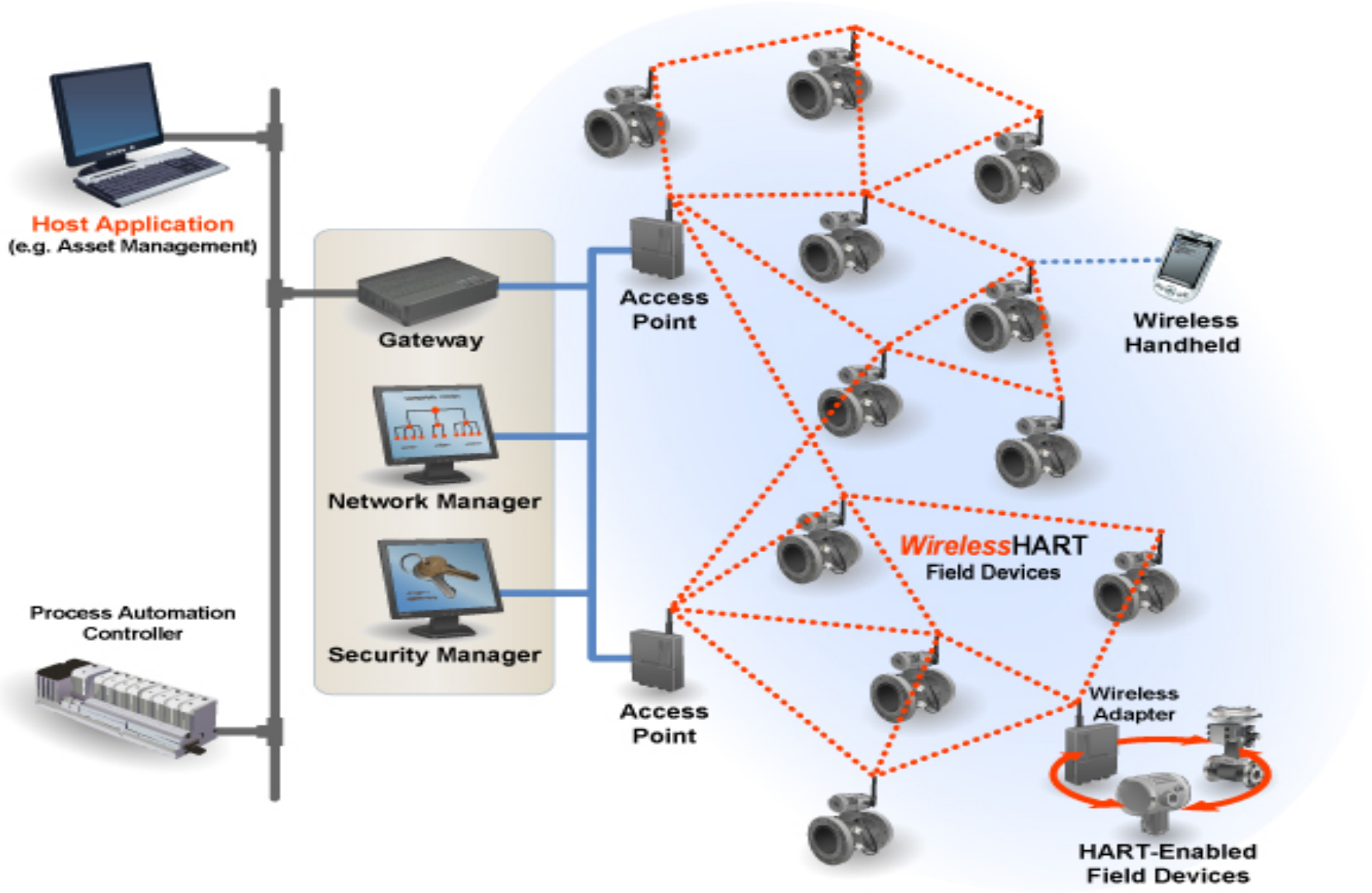
What Is Special

- Reliable: 99.9%
- Secure
- Self-organizing, self-healing
- Interoperable
- Supports both star and mesh topologies
- Built-in time synchronization

Why Reliable

- Diversity Measures
  - Time diversity
  - Channel diversity
  - Route diversity
  - Power Diversity
- Channel hopping
- Channel blacklisting

Components


Host Application
(e.g. Asset Management)
Gateway
Network Manager
Security Manager
Process Automation
Controller
Access
Point
Access
Point
Wireless
Handheld
WirelessHART
Field Devices
Wireless
Adapter
HART-Enabled
Field Devices

Network Manager

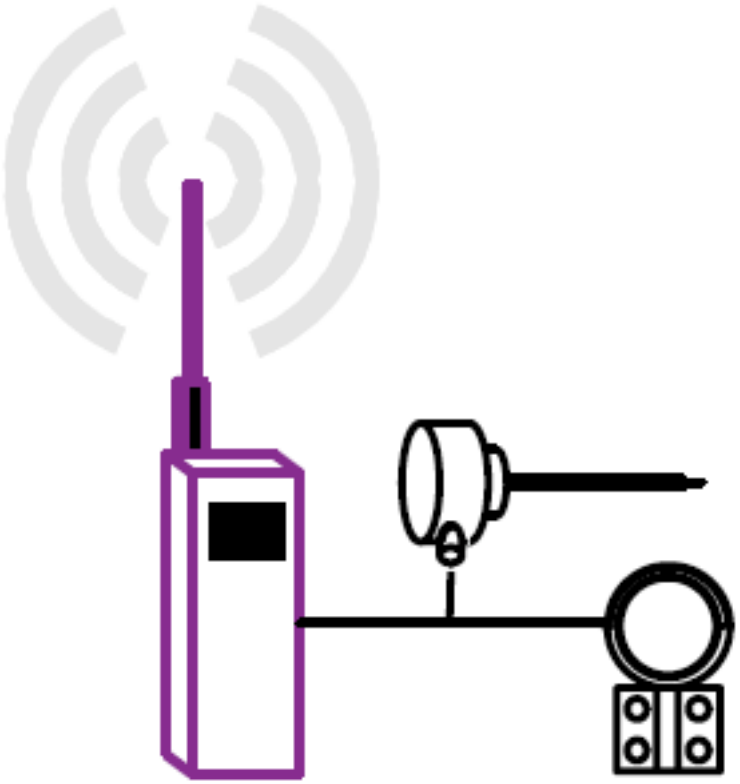
- Centralized brain
- Manages the network and its devices
  - User/administrator interacts with the Network Manager
  - Generates network management control packets to network devices.
- Routing, scheduling
- Redundant Network Managers supported (only one active)

Field Devices

- The most common type of network device
- Sensor/Actuator/Both
- Connected to the Process or Plant Equipment.
- Combines wireless communications with traditional HART communication field device capabilities.
- May be line or battery-powered

WirelessHART Adapter

- Enables communication to be passed to/from a non-native device through a WirelessHART Network. .



Gateway

- One gateway can support up to 80 devices

- Gateway provides
  - One or more Access Points providing the physical connection into the WirelessHART Network
  - A Virtual Gateway providing a sink or source point
  - One or more Host Interfaces connecting the Gateway to backbone networks (e.g., the plant automation network)
  - A connection to the Network Manager
  - Buffering and local storage for Publish Data, event notification, and common commands
  - Time synchronization sourcing

Other Devices

- Handheld devices
  - Portable applications used to configure, maintain or control plant assets.
  - Typically belong to networks of different standards

- Plant Automation Network: connects client applications to the gateway

- Security Manager: Industry standard AES-128 ciphers and keys

TDMA Data Link Layer

- 10ms time slot
  - Transmission starts at a specified time after the beginning of a slot
    - Source & destination set channel
    - Allows receiver to begin listening
  - Enough time for transmission+ACK

- Superframe: a series of time slots defining the communication pattern of a set of devices

Shared VS Dedicated Time Slots

- A time slot might be shared or dedicated
- Dedicated time slots: only one sender sends to a receiver
- Shared time slots: multiple senders attempt to send to a receiver

Shared Time Slots

- Shared time slots
  - Devices contest for access using a contention-based scheme.
  - Behave similar to Slotted Aloha
  - Devices use a collision-avoidance scheme (backoff).

- Using shared links may be desirable when
  - Throughput requirements of devices are low
  - Traffic is irregular or comes in bursts

- Shared slots may decrease latency since the device does not need to wait for dedicated slot
  - True only when chances of collisions are low

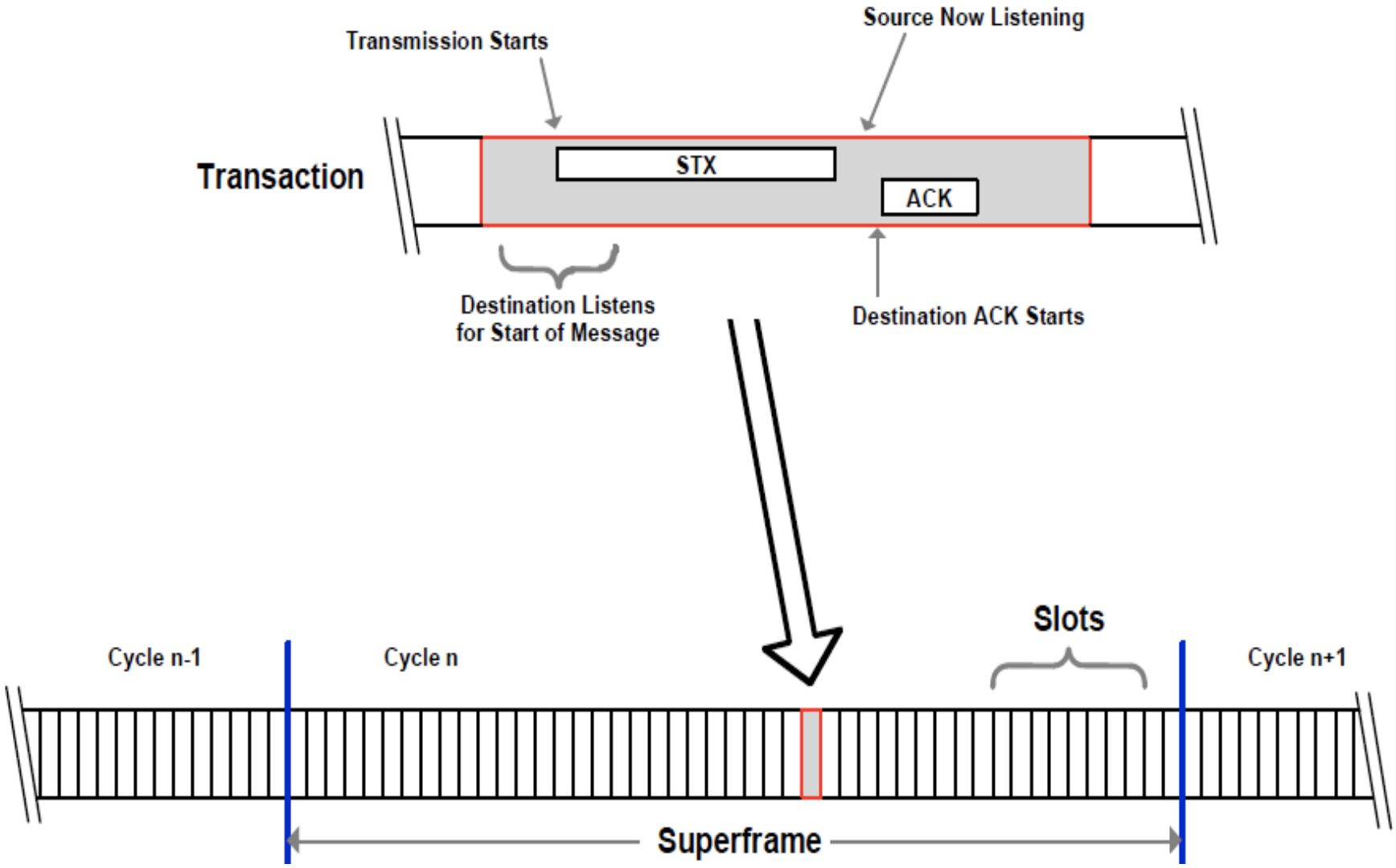
Time Synchronization

- Gateway is the root source of time
- Some neighbors are specified as time synchronization sources
- When the destination device receives a DLPDU, its time of arrival is noted
- Destination calculates the difference (Δt) from the ideal time at which it believes the communication should have occurred.
- This Δt is sent via ACK
- Sender adjusts time

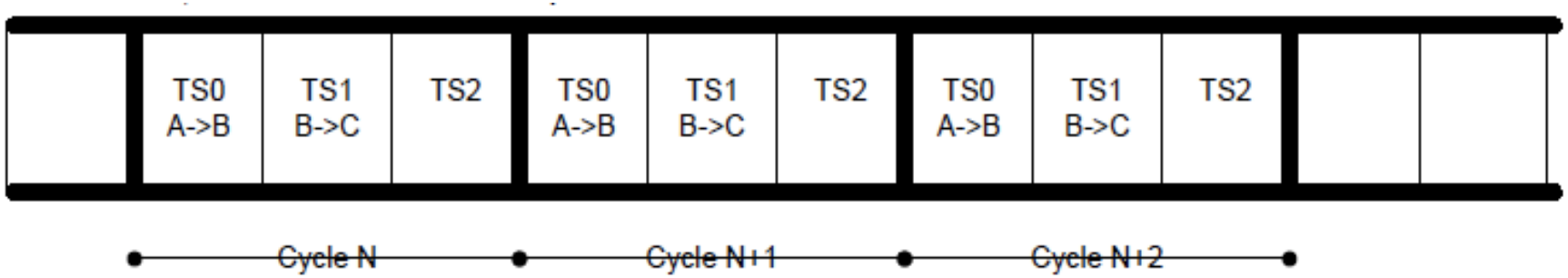
Channel Hopping

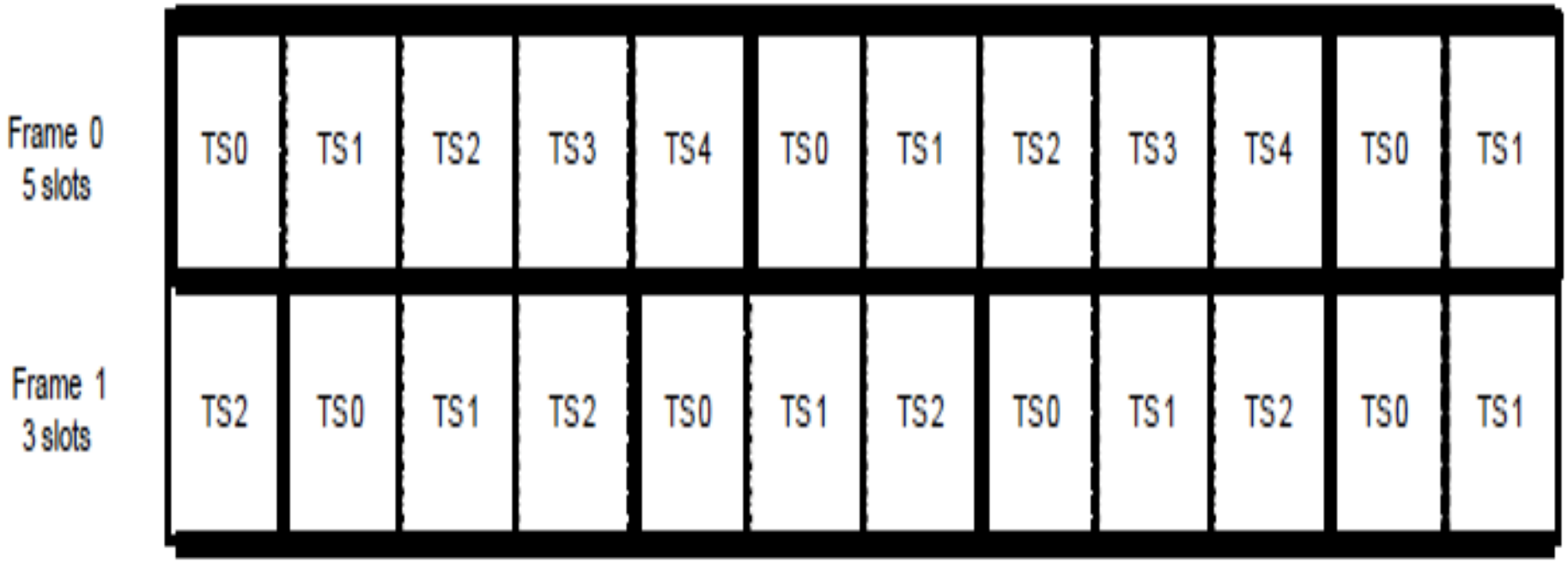
- Enhances reliability
  - Avoid interferers
  - Reduce multi-path fading effects
- Blacklisting restricts hopping to some channels
- Each device has a channel map (logical to physical)
- ActiveChannel = (ChannelOffset + ASN) % TotalChannels

Superframe


Transmission Starts
Source Now Listening
Transaction
STX
ACK
Destination Listens
for Start of Message
Destination ACK Starts
Slots
Cycle n-1
Cycle n
Cycle n+1
Superframe

Superframe


TS0
A->B
TS1
B->C
TS2
TS0
A->B
TS1
B->C
TS2
TS0
A->B
TS1
B->C
TS2
Cycle N
Cycle N+1
Cycle N+2


Frame 0
5 slots
TS0
TS1
TS2
TS3
TS4
TS0
TS1
TS2
TS3
TS4
TS0
TS1
Frame 1
3 slots
TS2
TS0
TS1
TS2
TS0
TS1
TS2
TS0
TS1
TS2
TS0
TS1

Superframe

- All devices must support multiple superframes
- At least one Superframe is always enabled while additional superframes can be enabled or disabled
- Slot sizes and the superframe length are fixed and form a network cycle with a fixed repetition rate
- **SuperframeSlot = (Absolute Slot Number) % Superframe.NumSlots**

DLPDU Types

- Five DLPDU types:
  - Data DLPDUs
  - Keep-Alive (periodic)
  - Advertise DLPDUs (periodic)
  - Disconnect
  - ACK

- Devices receiving a packet with an unknown packet type must not acknowledge the packet and shall immediately discard it.

Network Maintenance

- Advertise and Keep-Alive DLPDUs assist in building and maintaining the device's neighbor list
- A Keep-Alive must be transmitted to the neighbor if Last Time Communicated > keep Alive Interval.
- Keep-Alive transmissions are repeated until a new DLPDU is received from the neighbor
- Keep-Alive no more often than once per 30 seconds (if temperature varies 2º C per minute or less.)

Network Maintenance

- Path failures are reported to the Network Manager when devices lose connectivity to neighbors
- After the Path Fail Interval lapses, a Path-Down Alarm is generated (by both the sender and the receiver)
- As each device's Health Report Timer lapses, the devices generate health reports, which include indications of any problems the device is having with a neighbor.
- Default period of each devices health report is 15 minutes.

Network Maintenance

- Devices continue trying to reestablish communication until the links between them are deleted by the Network Manager
- It is common for broken paths to be restored after a temporary environmental effect passes.
- If the disruption persists, additional Path-Down Alarms will be generated when the Path Fail Interval lapses again.

Network Initialization

- WirelessHART Network automatically starts up and self-organize.
- Before a network can form, a Network Manager and a Gateway must exist.
- The Network Manager activates the first superframe. This establishes the system epoch – ASN 0.
- Once the Network Access Point starts to advertise, devices can begin to join the network.
- As devices join, the network forms.

Routing

- Message routing: WirelessHART supports both Graph and Source routing
- Graph routing: provides redundant paths
- Routing graphs
  - Uplink graph: upstream communication
  - Downlink graph: Downstream communication
  - Broadcast graph

Scheduling

- Scheduling: slots and channel assignment
  - Each receiver uses a separate channel for reception in a slot
  - A transmission is followed by a retransmission on the same link on a dedicated slot, then again on another link on a shared slot

- Each network contains exactly one overall schedule that is created and managed by the Network Manager.

- The schedule is organized into Superframes
  - Superframes can be enabled/disabled

Best Practices

- Each field device should have at least 3 neighbors: the 3rd neighbor will act as a backup if one of the two primary paths is obstructed or unavailable
- Devices (antenna) mounted >0.5m from any vertical surface
- Devices mounted >1.5m off the ground
- 25% of the network devices should have a direct connection to the gateway in large networks