IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

Connectivity Technologies – Part III

Dr. Sudip Misra

Associate Professor

Department of Computer Science and Engineering

IIT KHARAGPUR

Email: smisra@sit.iitkgp.ernet.in

Website: http://cse.iitkgp.ac.in/~smisra/

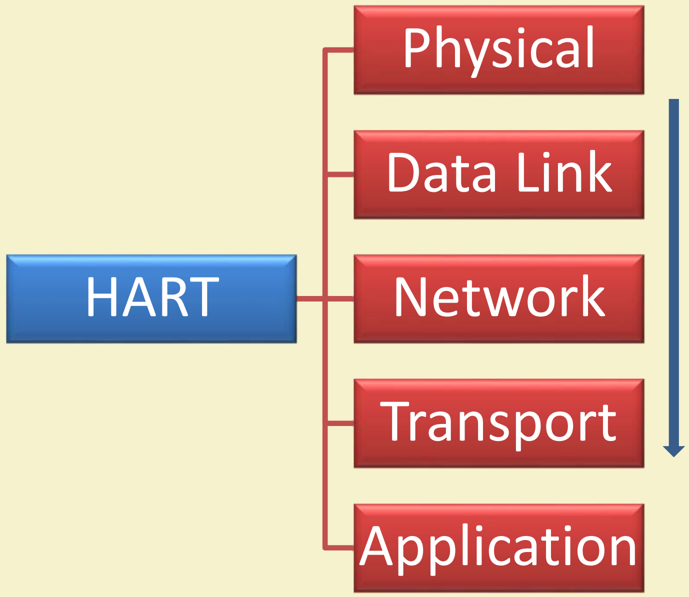
HART & Wireless HART

Introduction

- ✓ WirelessHART is the latest release of **Highway Addressable Remote Transducer** (HART) Protocol.
- ✓ HART standard was developed for **networked smart field devices**.
- ✓ The wireless protocol makes the implementation of HART **cheaper and easier**.
- ✓ HART encompasses the most number of field devices incorporated in any field network.

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

- ✓ Wireless HART enables device placements more accessible and cheaper– such as the top of a reaction tank, inside a pipe, or at widely separated warehouses.
- ✓ Main difference between wired and unwired versions is in the physical, data link and network layers.
- ✓ Wired HART lacks a network layer.



Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

HART Physical Layer

- ✓ Derived from IEEE 802.15.4 protocol.
- ✓ It operates only in the 2.4 GHz ISM band.
- ✓ Employs and exploits 15 channels of the band to increase reliability.

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

HART Data Link Layer

- ✓ Collision free and deterministic communication achieved by means of super-frames and TDMA.
- ✓ Super-frames consist of grouped 10ms wide timeslots.
- ✓ Super-frames control the timing of transmission to ensure collision free and reliable communication.
- ✓ This layer incorporates channel hopping and channel blacklisting to increase reliability and security.
- ✓ Channel blacklisting identifies channels consistently affected by interference and removes them from use.

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

HART Network & Transport Layers

- ✓ Cooperatively handle various types of traffic, routing, session creation, and security.
- ✓ WirelessHART relies on **Mesh networking** for its communication, and each device is primed to forward packets from every other devices.
- ✓ Each device is armed with an updated network graph (i.e., updated topology) to handle routing.
- ✓ **Network layer (HART)=Network + Transport + Session layers (OSI)**

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

HART Application Layer

- ✓ Handles communication between gateways and devices via a series of **command and response messages**.
- ✓ Responsible for **extracting** commands from a message, **executing** it and generating responses.
- ✓ This layer is seamless and does not differentiate between wireless and wired versions of HART.

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

HART Congestion Control

- ✓ Restricted to 2.4Ghz ISM band with channel 26 removed, due to its restricted usage in certain areas.
- ✓ Interference-prone channels avoided by using channel switching post every transmission.
- ✓ Transmissions synchronized using 10ms slots.
- ✓ During each slot, all available channels can be utilized by the various nodes in the network allowing for the propagation of 15 packets through the network at a time, which also minimizes the risk of collisions.

Source: A. Feng, “WirelessHART- Made Easy”, AwiaTech Blog (Online), Nov. 2011

WirelessHART Network Manager

- ✓ The network manager **supervises each node** in the network and guides them on **when and where** to send packets.
- ✓ Allows **for collision-free** and **timely delivery** of packets between a source and destination.
- ✓ The network manager **updates** information about neighbors, **signal strength**, and information needing delivery or **receipt**.
- ✓ Decides who will send, who will listen, and at what frequency is each time-slot.
- ✓ Handles **code-based network security** and prevents unauthorized nodes from joining the network.

WirelessHART vs. ZigBee

- ✓ A WirelessHART node **hops after every message**, changing channels every time it sends a packet. ZigBee does not feature hopping at all, and only **hops when the entire network hops**.
- ✓ At the MAC layer, WirelessHART utilizes time division multiple access (**TDMA**), allotting individual time slots for each transmission. ZigBee applies carrier sense multiple access with collision detection (**CSMA/CD**).

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

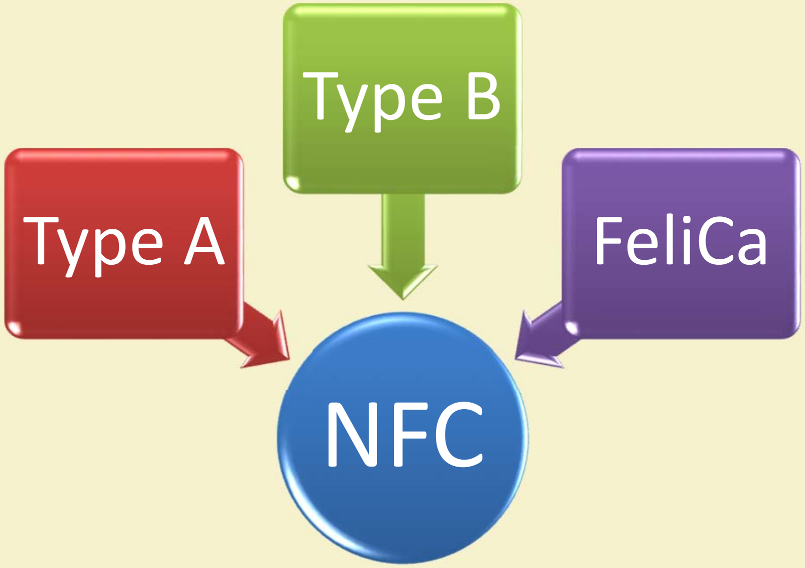
- ✓ WirelessHART represents a true mesh network, where each node is capable of serving as a router so that, if one node goes down, another can replace it, ensuring packet delivery. ZigBee utilizes a tree topology, which makes nodes along the trunk critical.
- ✓ WirelessHART devices are all back compatible, allowing for the integration of legacy devices as well as new ones. ZigBee devices share the same basis for their physical layers, but ZigBee, ZigBee Pro, ZigBee RF4CE, and ZigBee IP are otherwise incompatible with each other

Source: A. Feng, "WirelessHART- Made Easy", AwiaTech Blog (Online), Nov. 2011

NFC

Introduction

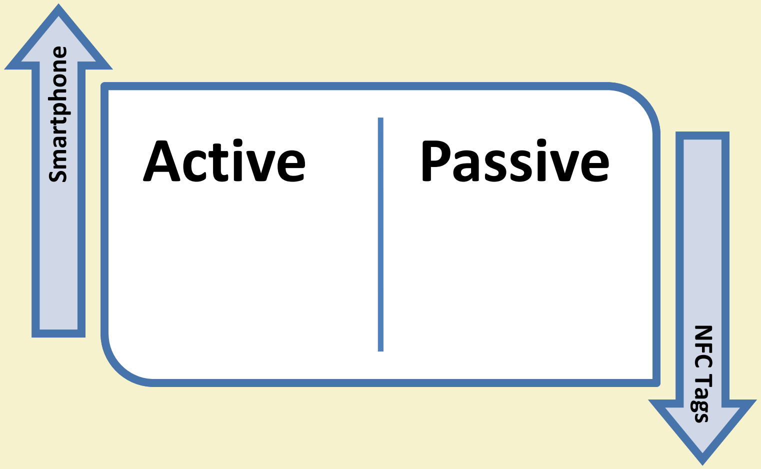
- ✓ **Near field communication**, or NFC for short, is an offshoot of radio-frequency identification (RFID).
- ✓ NFC is designed for use by devices within **close proximity** to each other.
- ✓ All NFC types are similar but communicate in slightly different ways.
- ✓ FeliCa is commonly found in Japan.



Source: "How NFC Works", NFC (Online)

NFC Types

- ✓ **Passive devices** contain information which is readable by other devices, however it cannot read information itself.
- ✓ NFC tags found in supermarket products are examples of passive NFC.
- ✓ **Active devices** are able to collect as well as transmit information.
- ✓ Smartphones are a good example of active devices.

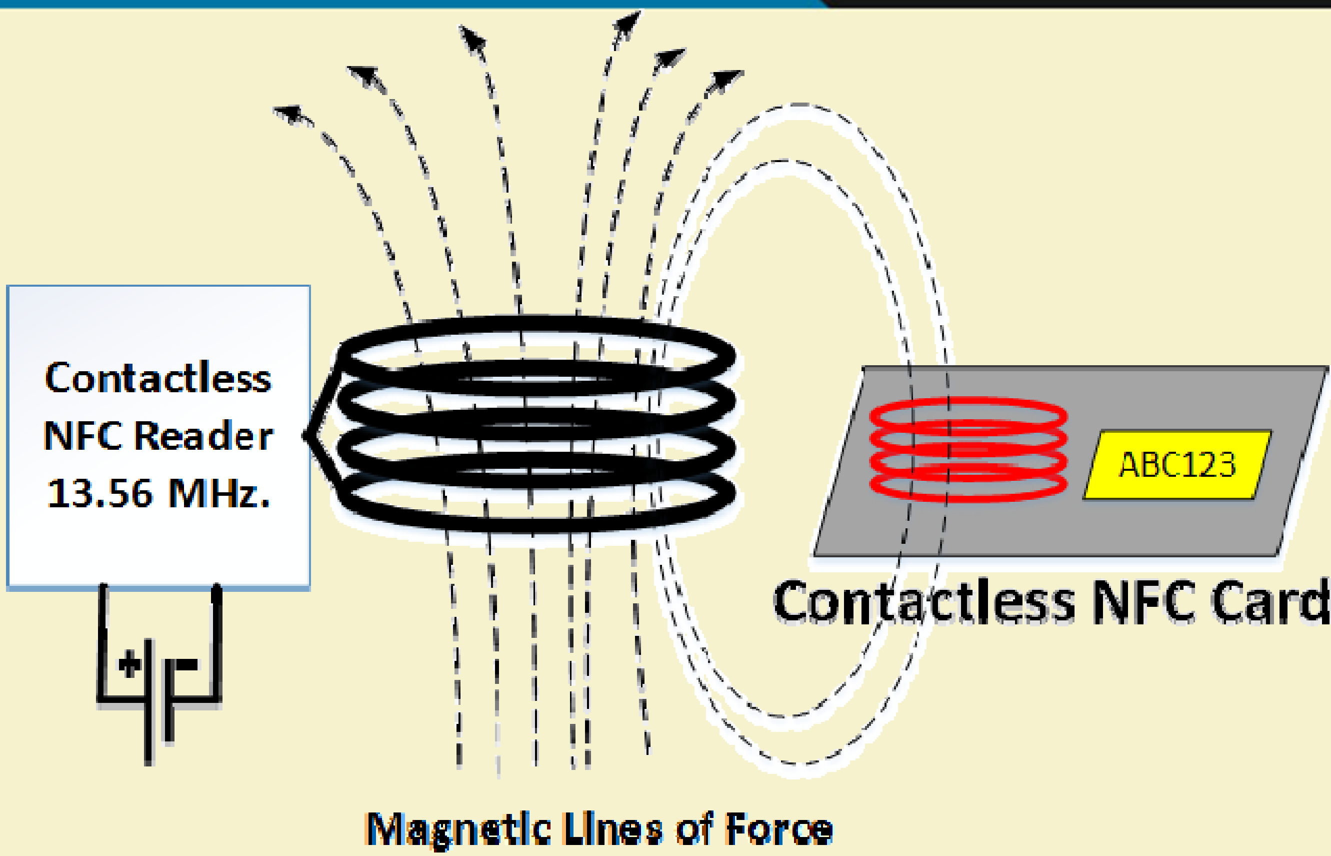


Source: "How NFC Works", NFC (Online)

Working Principle

- ✓ Works on the principle of **magnetic induction**.
- ✓ A reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices.
- ✓ The generated field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information.
- ✓ ‘Passive’ NFC tags use the energy from the reader to encode their response while ‘active’ or ‘peer-to-peer’ tags have their own power source.

Source: “Inside NFC: how near field communication works”, APC (Online), Aug. 2011


Contactless
NFC Reader
13.56 MHz.
ABC123
Contactless NFC Card
Magnetic Lines of Force

NFC Specifications

- ✓ NFC's data-transmission frequency is 13.56MHz.
- ✓ NFC can transmit data at a rate of either 106, 212 or 424 Kbps (kilobits per second).
- ✓ Tags typically store between 96 and 512 bytes of data.
- ✓ Communication range is less than 20cms.

Source: "Inside NFC: how near field communication works", APC (Online), Aug. 2011

Modes of Operation

Peer-to-peer — Lets two smartphones swap data

Read/Write — One active device picks up info from a passive one

Card emulation — NFC device can be used like a contactless credit card

Source: M. Egan, "What is NFC? Uses of NFC | How to use NFC on your smartphone", TechAdvisor (Online), May 2015

NFC Applications

- ✓ Smartphone based payments.
- ✓ Parcel tracking.
- ✓ Information tags in posters and advertisements.
- ✓ Computer game synchronized toys.
- ✓ Low-power home automation systems.

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

Connectivity Technologies – Part IV

Dr. Sudip Misra

Associate Professor

Department of Computer Science and Engineering

IIT KHARAGPUR

Email: smisra@sit.iitkgp.ernet.in

Website: http://cse.iitkgp.ac.in/~smisra/

Bluetooth

Introduction

- ✓ Bluetooth wireless technology is a short range communications technology.
- ✓ Intended for replacing cables connecting portable units
- ✓ Maintains high levels of security.
- ✓ Bluetooth technology is based on **Ad-hoc technology** also known as **Ad-hoc Piconets.**

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

Features

- ✓ Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ.
- ✓ Uses spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec.
- ✓ Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

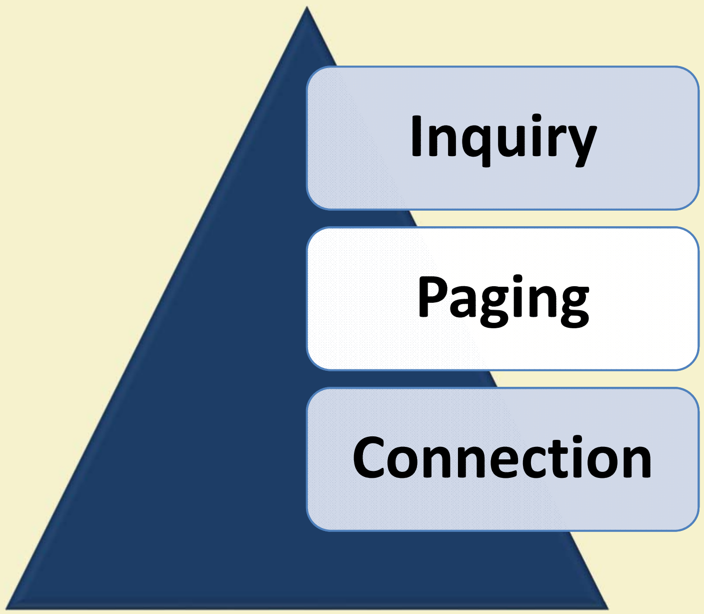
Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

Features

- ✓ Bluetooth operating range depends on the device:
  - **Class 3** radios have a range of up to 1 meter or 3 feet
  - **Class 2** radios are most commonly found in mobile devices have a range of 10 meters or 30 feet
  - **Class 1** radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

Connection Establishment



Inquiry run by one Bluetooth device to try to **discover other devices near it.**

Process of **forming a connection** between two Bluetooth devices.

A device either actively **participates** in the network or enters a low-power sleep mode.

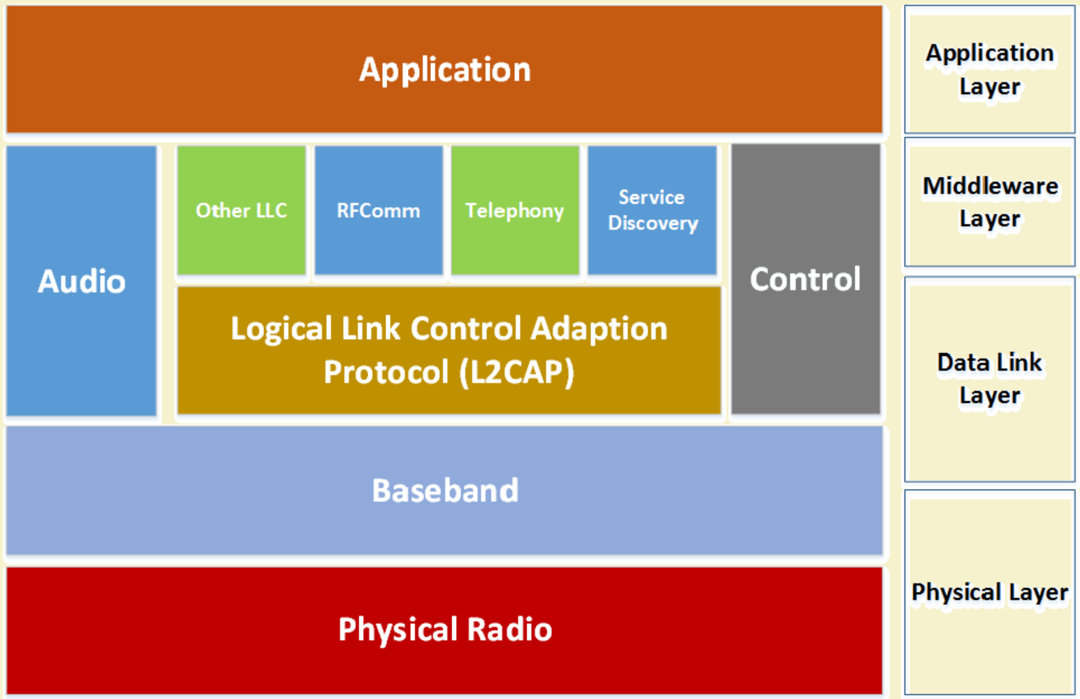
Source: "Bluetooth Basics", Tutorials, Sparkfun.com (Online)

Modes

Active	Sniff	Hold	Park
Actively transmitting or receiving data.	Sleeps and only listens for transmissions at a set interval .	Power-saving mode where a device sleeps for a defined period and then returns back to active mode .	Slave will become inactive until the master tells it to wake back up.

Source: “Bluetooth Basics”, Tutorials, Sparkfun.com (Online)

Protocol Stack



Baseband

- ✓ Physical layer of the Bluetooth.
- ✓ Manages physical channels and links.
- ✓ Other services include:
  - Error correction
  - Data whitening
  - Hop selection
  - Bluetooth security
- ✓ Manages asynchronous and synchronous links.
- ✓ Handles packets, paging and inquiry.

Source: "Bluetooth", Wikipedia (Online)

L2CAP

- ✓ The Logical Link Control and Adaptation Protocol (L2CAP).
- ✓ Layered over the Baseband Protocol and resides in the data link layer.
- ✓ Used to multiplex multiple logical connections between two devices.
- ✓ Provides connection-oriented and connectionless data services to upper layer protocols.
- ✓ Provides:
  - Protocol multiplexing capability
  - Segmentation and reassembly operation
  - Group abstractions

Source: "Bluetooth", Wikipedia (Online)

RFComm

- ✓ Radio Frequency Communications (RFCOMM).
- ✓ It is a cable replacement protocol used for generating a virtual serial data stream.
- ✓ RFCOMM provides for binary data transport .
- ✓ Emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is a serial port emulation.
- ✓ RFCOMM provides a simple reliable data stream to the user, similar to TCP.
- ✓ Supports up to 60 simultaneous connections between two BT devices.

Source: "Bluetooth", Wikipedia (Online)

Service Discovery Protocol (SDP)

- ✓ Enables applications to discover available services and their features.
- ✓ Addresses the unique characteristics of the Bluetooth environment such as, dynamic changes in the quality of services in RF proximity of devices in motion.
- ✓ Can function over a reliable packet transfer protocol.
- ✓ Uses a request/response model.

Source: "Bluetooth", Wikipedia (Online)

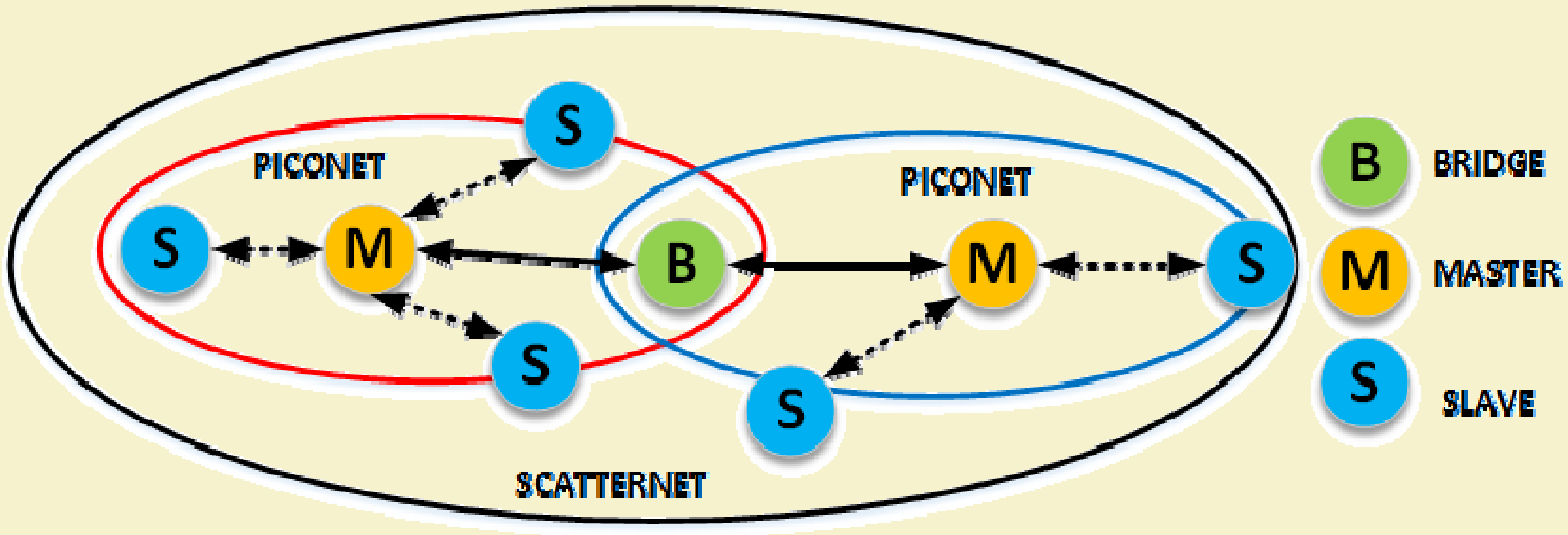
Piconets

- ✓ Bluetooth enabled electronic devices connect and communicate wirelessly through short range networks known as **Piconets**.
- ✓ Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave.
- ✓ Provisions are in place, which allow for a **master** and a **slave** to switch their roles.
- ✓ The simplest configuration is a point to point configuration with one master and one slave.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

- ✓ When more than two Bluetooth devices communicate with one another, it is called a **PICONET**.
- ✓ A Piconet can contain up to seven slaves clustered around a single master.
- ✓ The device that initializes establishment of the Piconet becomes the **master**.
- ✓ The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)



PICONET
PICONET
S
S
M
B
M
S
S
S
SCATTERNET
B
BRIDGE
M
MASTER
S
SLAVE

Features of Piconet

- ✓ Within a Piconet, the clock and unique **48-bit address** of master determines the timing of various devices and the frequency hopping sequence of individual devices.
- ✓ Each Piconet device supports 7 simultaneous connections to other devices.
- ✓ Each device can communicate with several piconets simultaneously.
- ✓ Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

- ✓ There is no direct connection between the slaves.
- ✓ All connections are either master-to-slave or slave-to-master.
- ✓ Slaves are allowed to transmit once these have been polled by the master.
- ✓ Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- ✓ A device can be a member of two or more Piconets.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

- ✓ A device can be a slave in one Piconet and master in another. It however cannot be a master in more than once Piconets.
- ✓ Devices in adjacent Piconets provide a bridge to support inner-Piconet connections, allowing assemblies of linked Piconets to form a physically extensible communication infrastructure known as **Scatternet**.

Source: "Wireless Communication - Bluetooth", Tutorials Point (Online)

Applications

- ✓ Audio players
- ✓ Home automation
- ✓ Smartphones
- ✓ Toys
- ✓ Hands free headphones
- ✓ Sensor networks

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

Connectivity Technologies – Part V

Dr. Sudip Misra

Associate Professor

Department of Computer Science and Engineering

IIT KHARAGPUR

Email: smisra@sit.iitkgp.ernet.in

Website: http://cse.iitkgp.ac.in/~smisra/

Z Wave

Introduction

- ✓ Zwave (or Z wave or Z-wave) is a protocol for communication among devices used for home automation.
- ✓ It uses RF for signaling and control.
- ✓ Operating frequency is 908.42 MHz in the US & 868.42 MHz in Europe.
- ✓ Mesh network topology is the main mode of operation, and can support 232 nodes in a network.

Source: "What is Z-Wave?", Smart Home (Online)

Zwave Global Operating Frequency

Frequency in MHz	Used in
865.2	India
868.1	Malaysia
868.42 ; 869.85	Europe
868.4	China, Korea
869.0	Russia
908.4 ; 916.0	USA
915.0 - 926.0	Israel
919.8	Hong Kong
921.4 ; 919.8	Australia, New Zealand
922.0 - 926.0	Japan

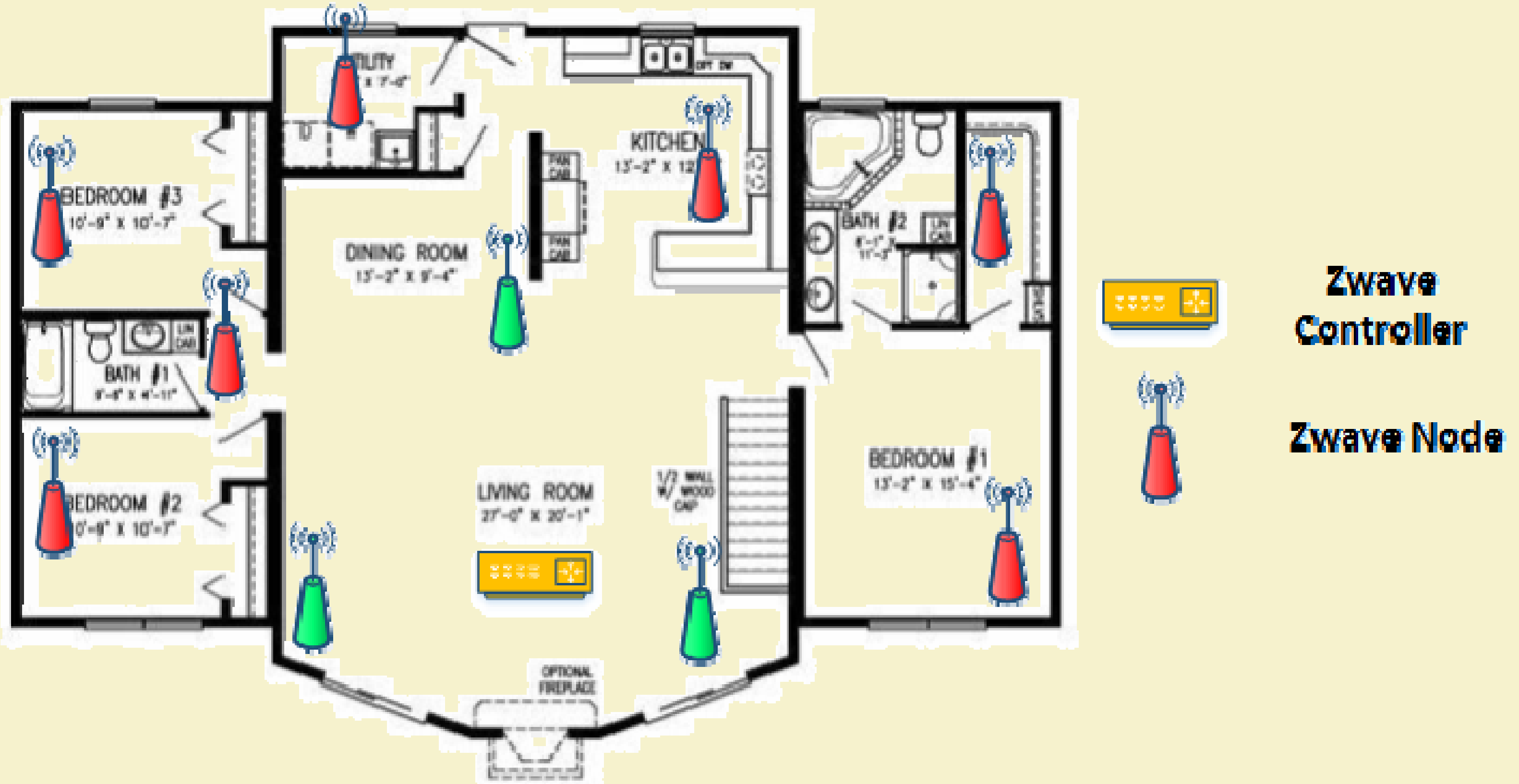
Source: "Z-Wave", Wikipedia (Online**)**

- ✓ Zwave utilizes GFSK modulation and Manchester channel encoding.
- ✓ A central network controller device sets-up and manages a Zwave network.
- ✓ Each logical Zwave network has 1 Home (Network) ID and multiple node IDs for the devices in it.
- ✓ Nodes with different Home IDs cannot communicate with each other.
- ✓ Network ID length=4 Bytes, Node ID length=1 Byte.

Source: "What is Z-Wave?", Smart Home (Online)

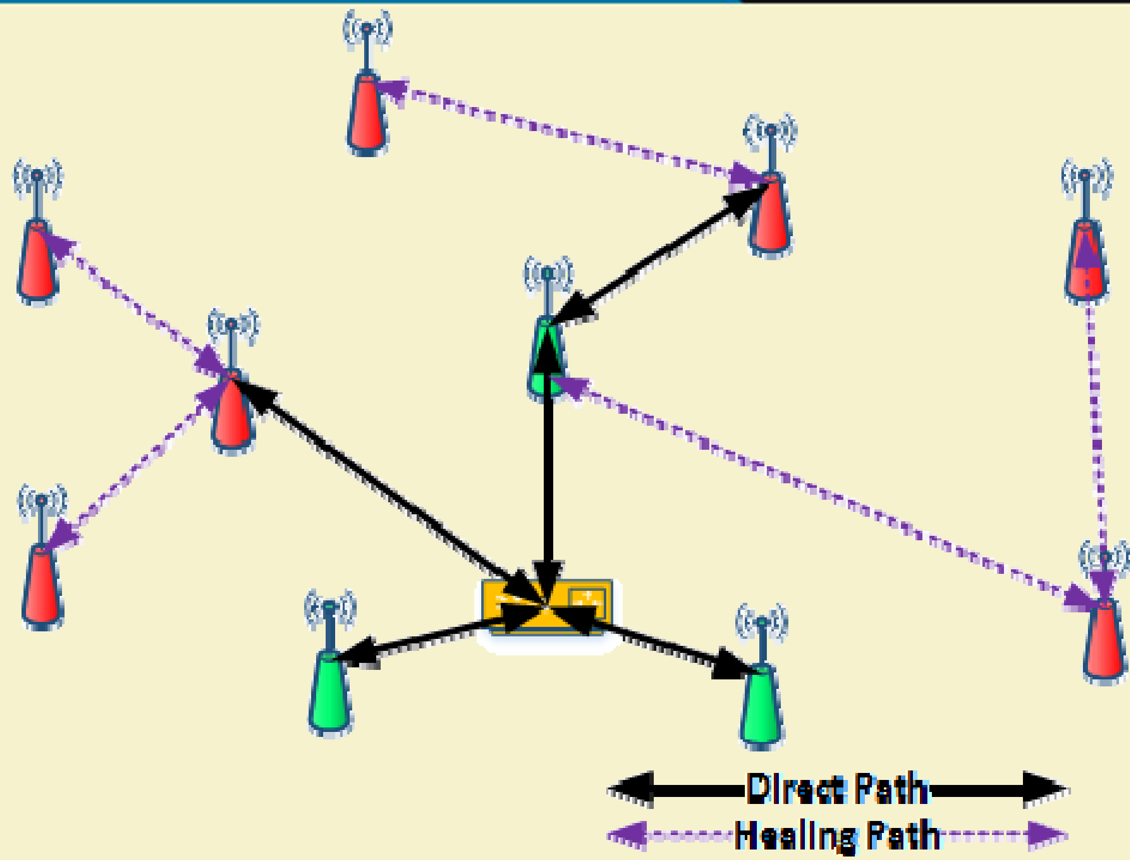
GFSK

- ✓ Gaussian Frequency Shift Keying.
- ✓ Baseband pulses are passed through a Gaussian filter prior to modulation.
- ✓ Filtering operation smoothens the pulses consisting of streams of -1 and 1, and is known as **Pulse shaping**.
- ✓ Pulse shaping limits the modulated spectrum width.


BEDROOM #3
10'-9" X 10'-7"
BATH #1
BEDROOM #2
DINING ROOM
13'-2" X 9'-4"
KITCHEN
LIVING ROOM
27'-0" X 20'-1"
OPTIONAL FIREPLACE
BATH #2
BEDROOM #1
13'-2" X 15'-4"
Zwave Controller
Zwave Node

- ✓ Uses source routed network mesh topology using 1 primary controller.
- ✓ Devices communicate with one another when in range.
- ✓ When devices are not in range, messages are routed though different nodes to bypass obstructions created by household appliances or layout.
- ✓ This process of bypassing radio dead-spots is done using a message called **Healing.**
- ✓ As Zwave uses a source routed static network, <u>mobile devices are excluded</u> from the network and <u>only static devices</u> are considered.

Source: "What is Z-Wave?", Smart Home (Online)



Direct Path
Healing Path

Zwave vs. Zigbee

Zwave

- ✓ User friendly and provides a simple system that users can set up themselves.
- ✓ Ideal for someone with a basic understanding of technology who wants to keep their home automation secure, efficient, simple to use, and easy to maintain.

Zigbee

- ✓ Requires so little power that devices can last up to seven years on one set of batteries.
- ✓ Ideal for technology experts who want a system they can customize with their preferences and install themselves.

Source: Sarah Brown, "ZigBee vs. Z-Wave Review: What's the Best Option for You?", The SafeWise Report (Online), Mar 2016

Zwave vs. Zigbee

Zwave

- ✓ Expensive.
- ✓ Nine out of ten leading security and communication companies in the U.S. use Z-Wave in their smart home solutions

Zigbee

- ✓ Cheaper than Zwave.
- ✓ ZigBee Alliance consists of nearly 400 member organizations that use, develop, and improve ZigBee's open-standard wireless connection

Source: Sarah Brown, "ZigBee vs. Z-Wave Review: What's the Best Option for You?", The SafeWise Report (Online), Mar 2016

ISA 100.11A

Introduction

- ✓ International Society of Automation.
- ✓ Designed mainly for large scale industrial complexes and plants.
- ✓ More than 1 billion devices use ISA 100.11A
- ✓ ISA 100.11A is designed to support native and tunneled application layers.
- ✓ Various transport services, including ‘reliable,’ ‘best effort,’ ‘real-time’ are offered.

Source: “The ISA 100 Standards : Overview and Status” ISA, 2008

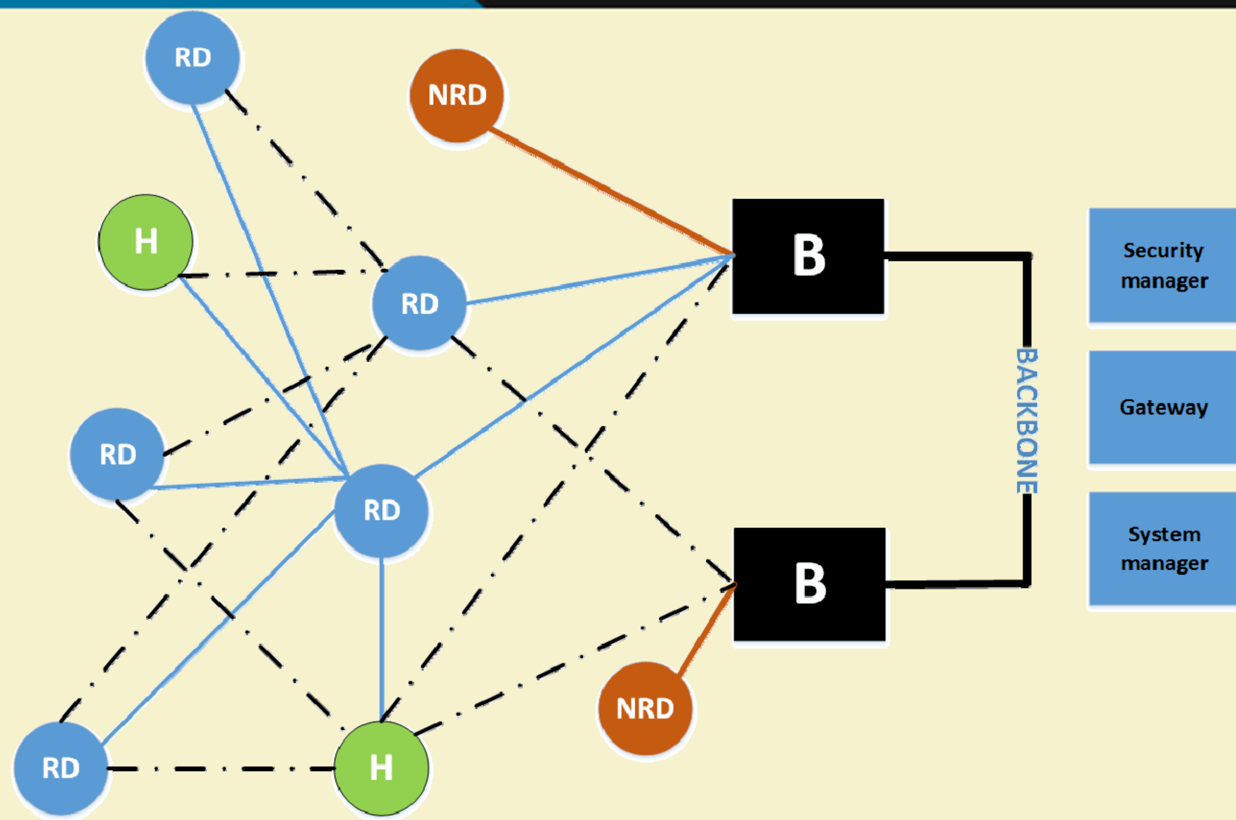
- ✓ Network and transport layers are based on TCP or UDP / IPv6.
- ✓ Data link layer supports mesh routing and Frequency hopping.
- ✓ Physical and MAC layers are based on IEEE 802.15.4
- ✓ Topologies allowed are:
  - Star/tree
  - Mesh
- ✓ Permitted networks include:
  - Radio link
  - ISA over Ethernet
  - Field buses

Source: Cambridge Whitepaper, http://portal.etsi.org/docbox/Workshop/2008/200812_WIRELESSFACTORY/CAMBRIDGE_WHITTAKER.pdf

- ✓ Application Support Layer delivers communications services to user and management processes.
- ✓ It can pass objects (methods, attributes) natively within the ISA 100.11A protocol.
- ✓ A tunneling mode is available to allow legacy data through the ISA100.11A network.

Source: Tim Whittaker , "What do we expect from Wireless in the Factory?"Cambridge Whitepaper, Cambridge Consultants, 2008

- ✓ RD=routing device
- ✓ NRD=Non-routing device
- ✓ H=Handheld device
- ✓ B=backbone device



Source: Tim Whittaker , "What do we expect from Wireless in the Factory?"Cambridge Whitepaper, Cambridge Consultants, 2008

Features

- ✓ Flexibility
- ✓ Support for multiple protocols
- ✓ Use of open standards
- ✓ Support for multiple applications
- ✓ Reliability (error detection, channel hopping)
- ✓ Determinism (TDMA, QoS support)
- ✓ Security

Security

- ✓ Security is fully built-in to the standard.
- ✓ Authentication and confidentiality services are independently available.
- ✓ A network security manager manages and distributes keys.
- ✓ Twin data security steps in each node:
  - Data link layer encrypts each hop.
  - Transport layer secures peer-to-peer communications.

Source: Tim Whittaker , "What do we expect from Wireless in the Factory?"Cambridge Whitepaper, Cambridge Consultants, 2008

ISA100.11A Usage Classes

Category	Class	Application	Description
Safety	0	Emergency action	Always critical
Control	1	Closed loop regulatory control	Often critical
	2	Closed loop supervisory control	Usually non-critical
	3	Open loop control	Human-in-the-loop
Monitoring	4	Alerting	Short term operational consequence
	5	Logging/ Downloading	No immediate operational consequence

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

NPTEL

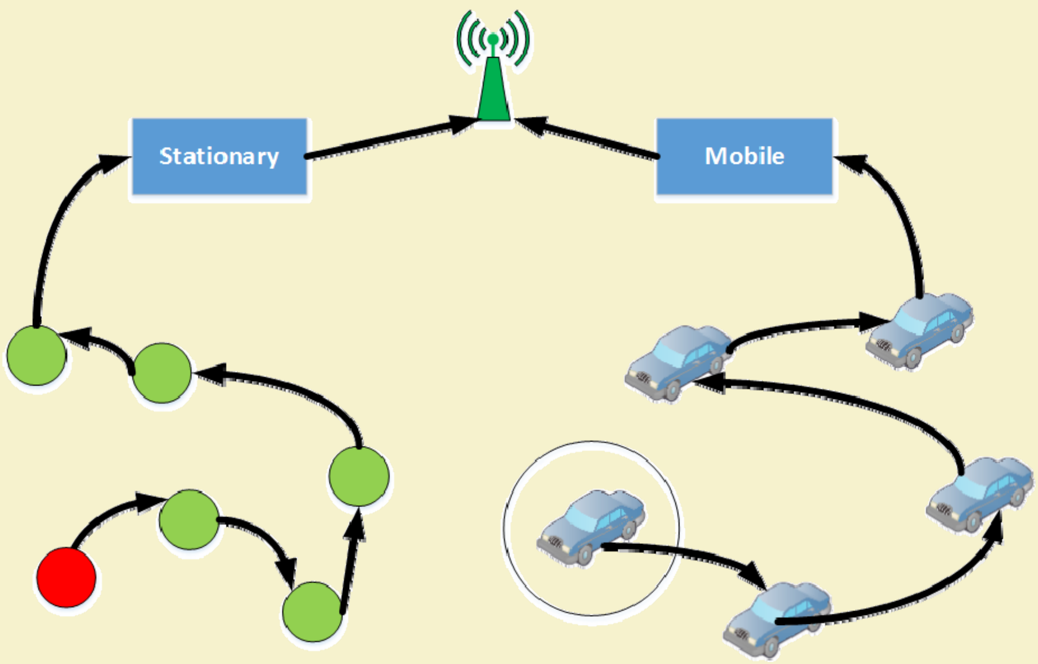
Sensor Networks – Part I

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

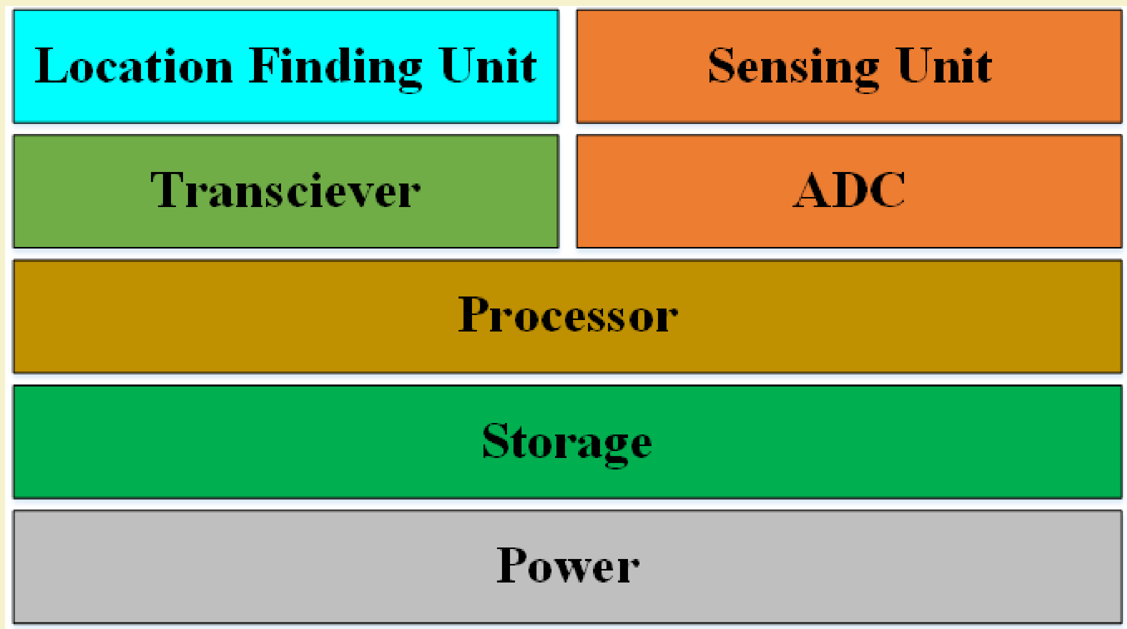
Wireless Sensor Networks (WSNs)

- Consists of a large number of sensor nodes, densely deployed over an area.
- Sensor nodes are capable of collaborating with one another and measuring the condition of their surrounding environments (i.e. Light, temperature, sound, vibration).
- The sensed measurements are then transformed into digital signals and processed to reveal some properties of the phenomena around sensors.
- Due to the fact that the sensor nodes in WSNs have short radio transmission range, intermediate nodes act as relay nodes to transmit data towards the sink node using a multi-hop path.

Multi-hop Path in WSNs



Basic Components of a Sensor Node



Sensor Nodes

- **Multifunctional**
  - The number of sensor nodes used depends on the application type.
- **Short transmission ranges**
- **Have OS** (e.g., TinyOS).
- **Battery Powered** – Have limited life.

Image source: Wikimedia Commons

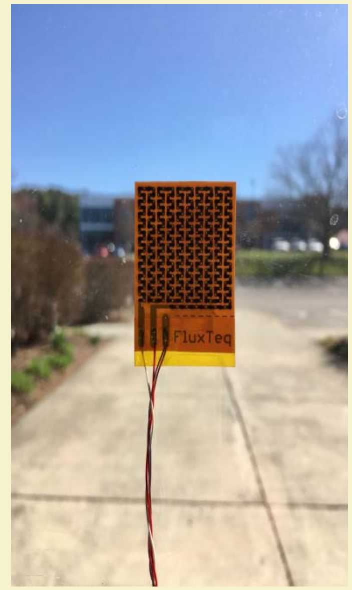
Constraints on Sensor Nodes

- Small size, typically less than a cubic cm.
- Must consume extremely low power
- Operate in an unattended manner in a highly dense area.
- Should have low production cost and be dispensable
- Be autonomous
- Be adaptive to the environment

Applications

- Temperature measurement
- Humidity level
- Lighting condition
- Air pressure
- Soil makeup
- Noise level
- Vibration

a) Soil sensor node

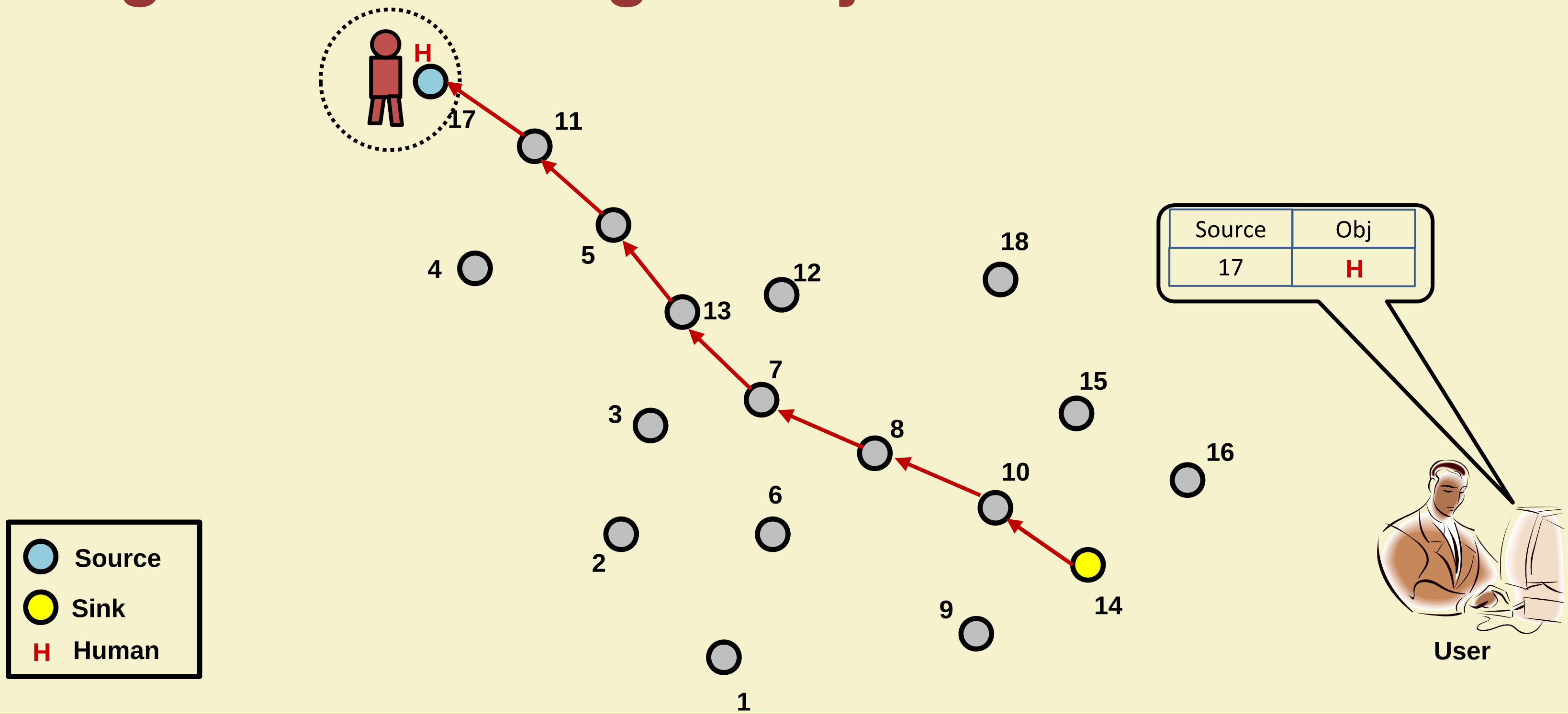


b) Temperature Flux sensor node

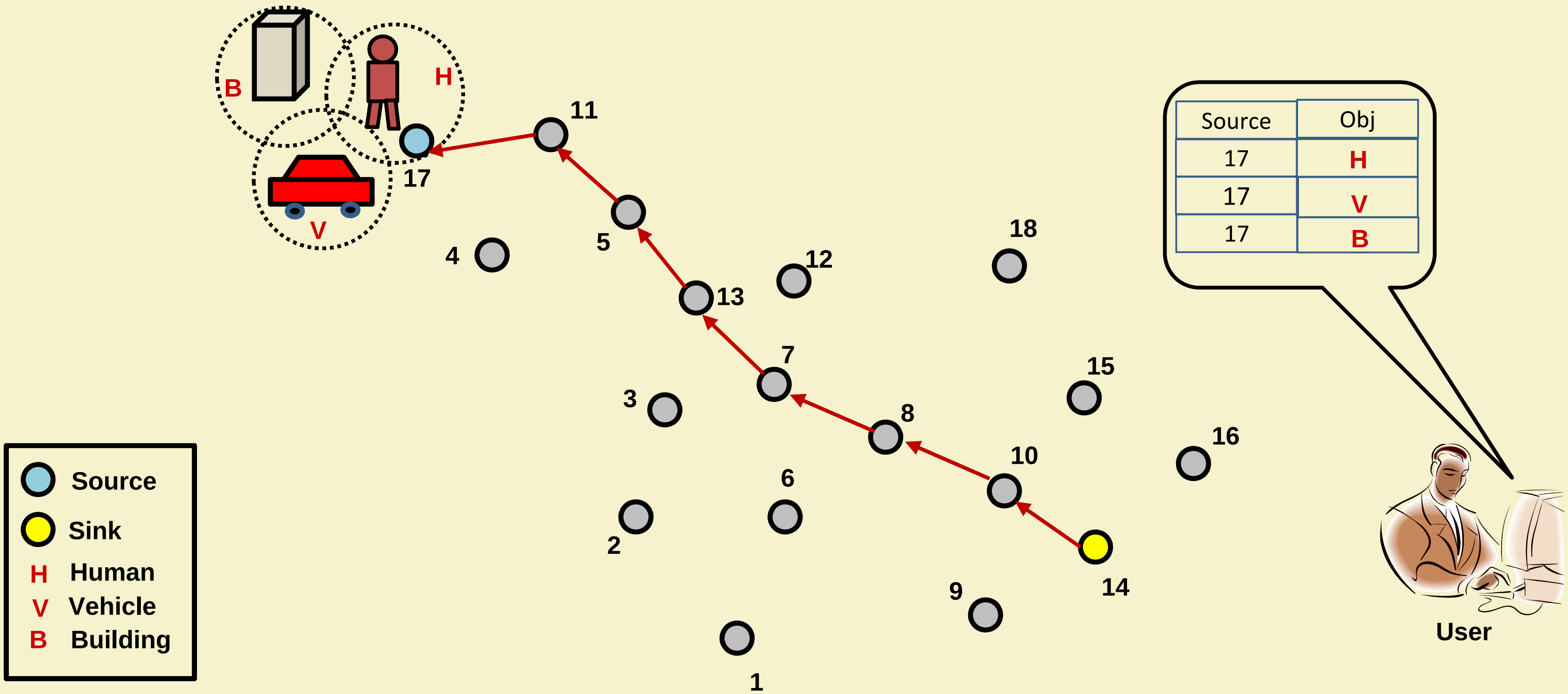
c) Weather sensor node

Image source: Wikimedia Commons

Single Source Single Object Detection

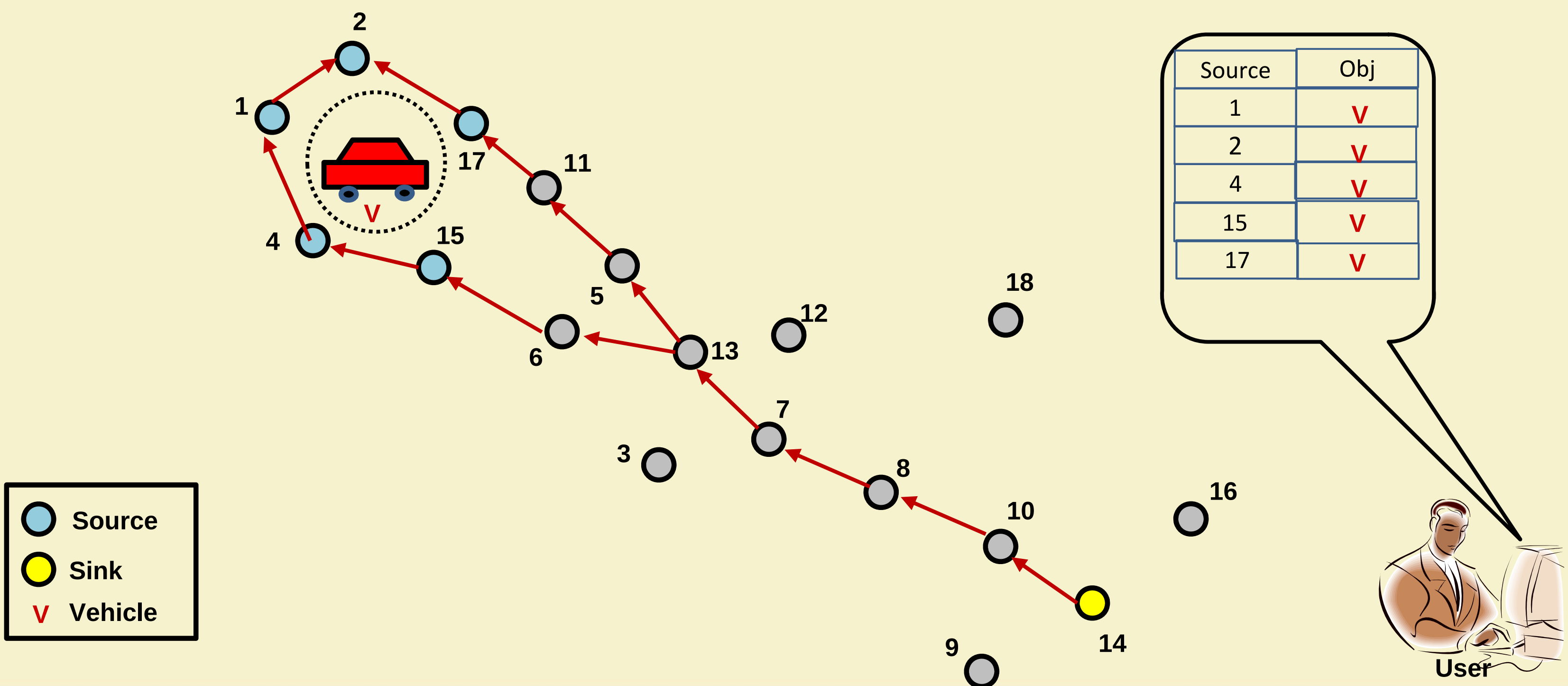


Single Source Multiple Object Detection



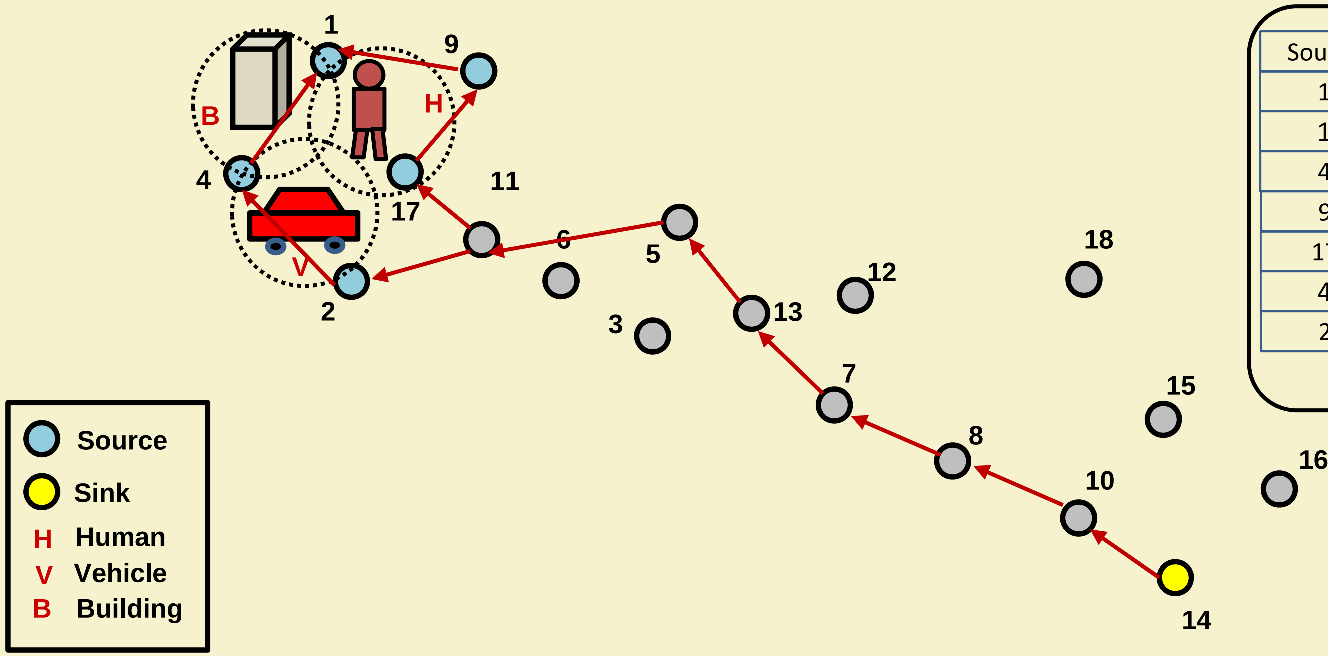
Source	Obj
17	H
17	V
17	B

Multiple Source Single Object Detection

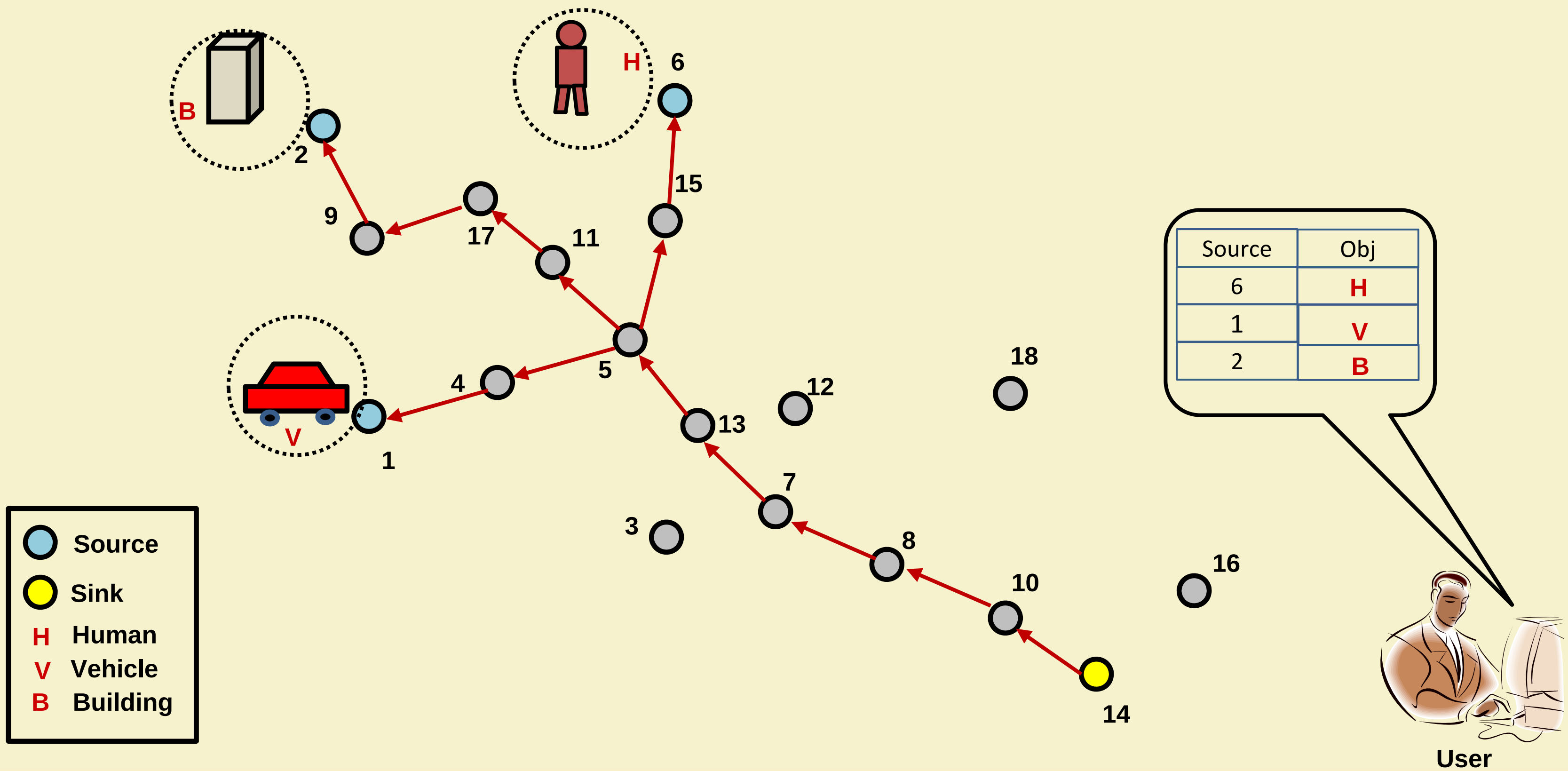


Source	Obj
1	V
2	V
4	V
15	V
17	V

Multiple Source Multiple Object Detection



Source	Obj
1	H
1	B
4	B
9	H
17	H
4	V
2	V



Source	Obj
6	H
1	V
2	B

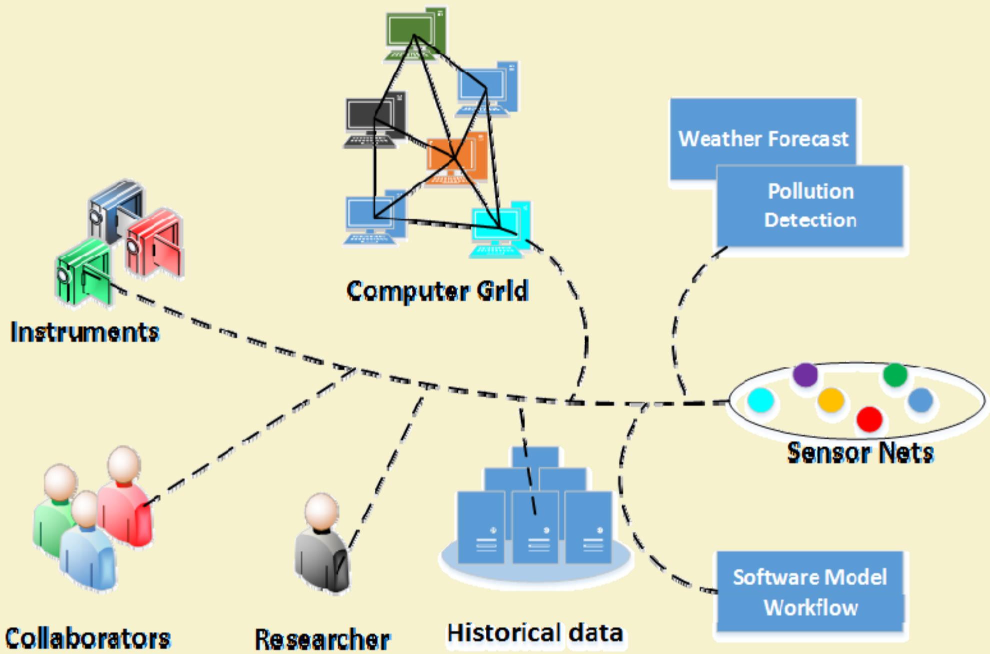
Challenges

- Scalability
  - Providing acceptable levels of service in the presence of large number of nodes.
  - Typically, throughput decreases at a rate of $1/\sqrt{N}$, N = number of nodes.
- Quality of service
  - Offering guarantees in terms of bandwidth, delay, jitter, packet loss probability.
  - Limited bandwidth, unpredictable changes in RF channel characteristics.

Challenges (contd.)

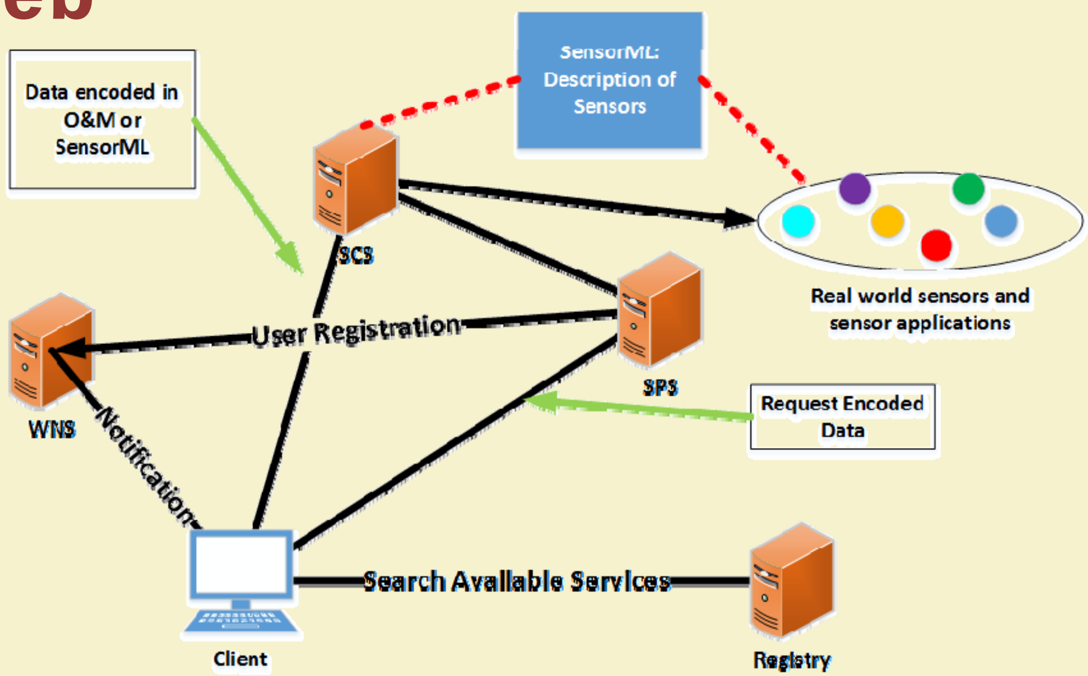
- Energy efficiency
  - Nodes have limited battery power
  - Nodes need to cooperate with other nodes for relaying their information.
- Security
  - Open medium.
  - Nodes prone to malicious attacks, infiltration, eavesdropping, interference.

Sensor Web



Source: X. Chu and R. Buyya, “Service Oriented Sensor Web”, Sensor Networks and Configuration, Springer, 2007, pp. 51-74.

Sensor Web



WNS: Web Notification Services

SCS: Sensor Collection Services

SPS: Sensor Planning Services

SensorML: Sensor Modeling language

Source: X. Chu and R. Buyya, "Service Oriented Sensor Web", Sensor Networks and Configuration, Springer, 2007, pp. 51-74.

Sensor Web Entanglement

- Observations & measurements (O&M)
- Sensor model language (sensorml)
- Transducer model language (transducerml or TML)
- Sensor observations service (SOS)
- Sensor planning service (SPS)
- Sensor alert service (SAS)
- Web notification services (WNS)

Cooperation in Wireless Ad Hoc and Sensor Networks

- Nodes communicate with other nodes with the help of intermediate nodes.
- The intermediate nodes act as relays.
- Wireless nodes are energy-constrained.
- Nodes may or may not cooperate.

Cooperation in Wireless Ad Hoc and Sensor Networks

- Two extremities:
  - **Total cooperation:** if all relay requests are accepted, nodes will quickly exhaust limited energy.
  - **Total non-cooperation:** if no relay requests are accepted, the network throughput will go down rapidly.
- Issues:
  - Selfishness, self-interests, etc.
  - Symbiotic dependence
  - Tradeoff: individual node’s lifetime vs. Throughput.

Security Challenges in Cooperation

- Open, shared radio medium by the nodes, which dynamically change positions.
- No centralized network management or certification authority.
- Existence of malicious nodes.
- Nodes prone to attacks, infiltration, eavesdropping, interference.
- Nodes can be captured, compromised, false routing information can be sent – paralyzing the whole network.
- The cooperating node or the node being cooperated might be victimized.

Thank You!!

IIT KHARAGPUR

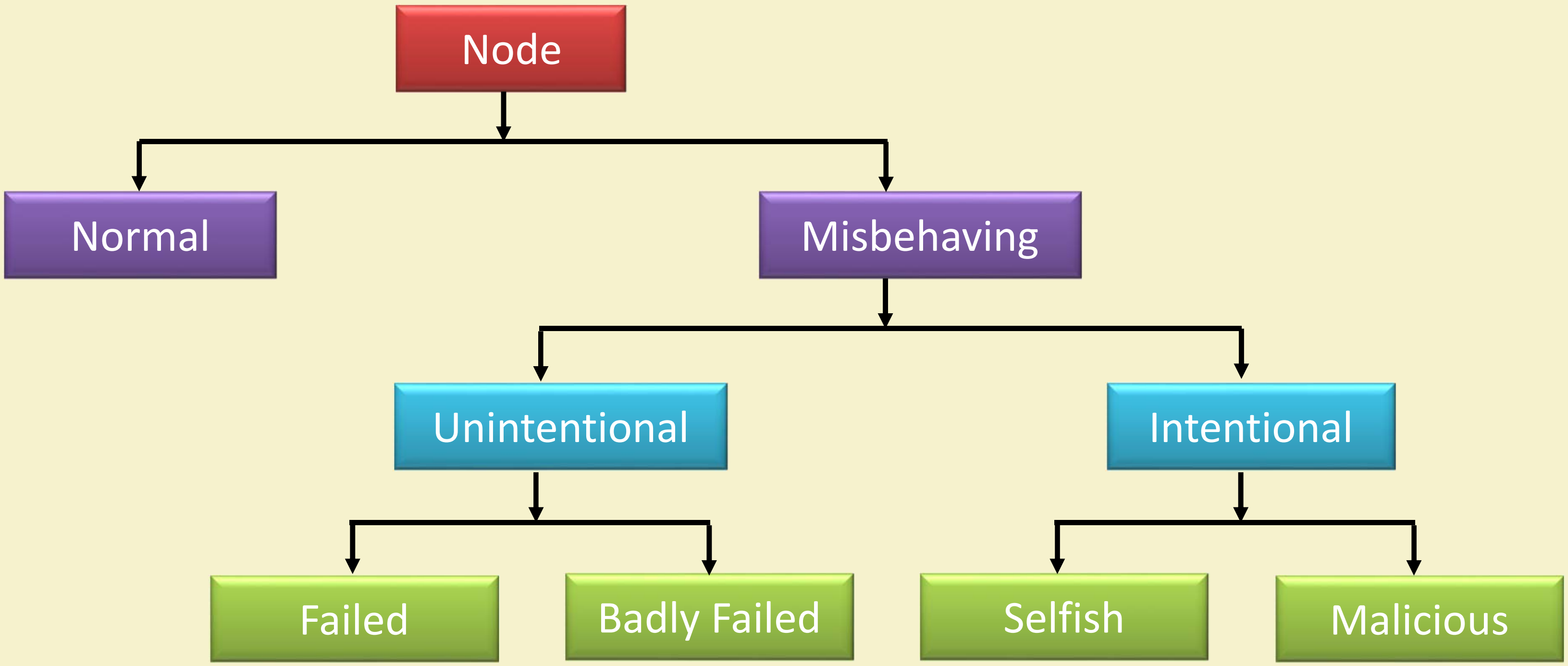
NPTEL ONLINE
CERTIFICATION COURSES

NPTEL

Sensor Networks – Part II

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

Node Behavior in WSNs



Node Behavior in WSNs (contd.)

- Normal nodes work perfectly in ideal environmental conditions
- Failed nodes are simply those that are unable to perform an operation; this could be because of power failure and environmental events.
- Badly failed nodes exhibit features of failed nodes but they can also send false routing messages which are a threat to the integrity of the network.

Node Behavior in WSNs (contd.)

- Selfish nodes are typified by their unwillingness to cooperate, as the protocol requires whenever there is a personal cost involved. Packet dropping is the main attack by selfish nodes.
- Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network service if possible.

Dynamic Misbehavior: Dumb Behavior

- Detection of such temporary misbehavior in order to preserve normal functioning of the network – coinage and discovery of dumb behavior
- In the presence of adverse environmental conditions (high temperature, rainfall, and fog) the communication range shrinks
- A sensor node can sense its surroundings but is unable to transmit the sensed data
- With the resumption of favorable environmental conditions, dumb nodes work normally
- Dumb behavior is temporal in nature (as it is dependent on the effects of environmental conditions)

Detection and Connectivity Re-establishment

- The presence of dumb nodes impedes the overall network performance
- Detection, and, subsequently, the re-establishment of network connectivity is crucial
- The sensed information can only be utilized if the connectivity between each dumb node with other nodes in the network could be re-established
- Before restoration of network connectivity, it is essential to detect the dumb nodes in the network.
- CoRD and CoRAD are two popular schemes that re-establish the connectivity between dumb nodes with others.

Event-Aware Topology Management in Wireless Sensor Networks

- Timely detection of an event of interest
- Monitoring the event
- Disseminating event-data to the sink
- Adapting with the changes of event state
    - Event location
    - Event area
    - Event duration

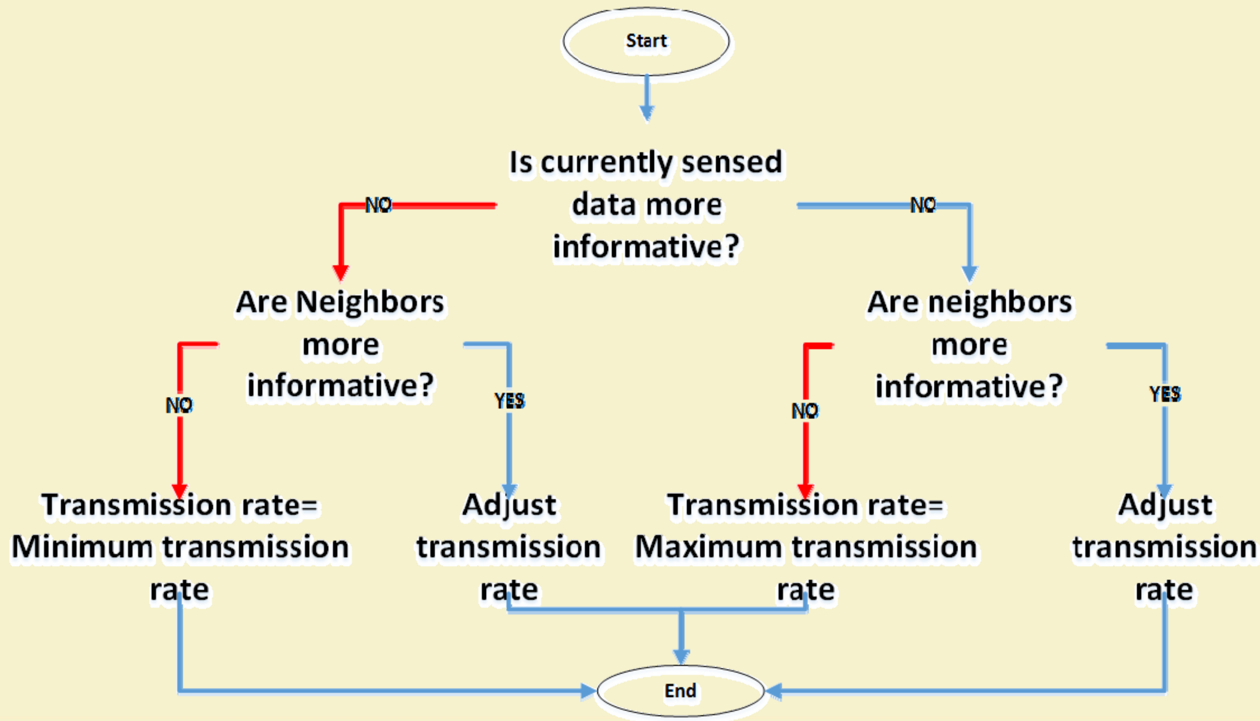
Source: S. N. Das, S. Misra, M. S. Obaidat, "Event-Aware Topology Management in Wireless Sensor Networks", Proceedings of Ubiquitous Information Technologies and Applications (CUTE 2013), Springer Lecture Notes in Electrical Engineering, Vol. 214, 2013, pp. 679-687

Information Theoretic Self-Management of Wireless Sensor Networks

- A WSN is deployed with the intention of acquiring information
- The sensed information are transmitted in the form of packets
- Information theoretic self-management (INTSEM) controls the transmission rate of a node by adjusting a node's sleep time
- Benefits
  - Reduce consumption of transmission energy of transmitters
  - Reduce consumption of receiving energy of relay nodes

S. N. Das and S. Misra, "Information theoretic self-management of Wireless Sensor Networks", Proceedings of NCC 2013.

General Framework of InTSeM



Social Sensing in WSNs

✓ Social Sensing-based Duty Cycle Management for Monitoring Rare Events in Wireless Sensor Networks

- WSNs are energy-constrained
- Scenario:
  - Event monitoring using WSNs
  - WSNs suffer from ineffective sensing for rare events
  - Event monitoring or sensing, even if there is no event to monitor or sense
  - Example: Submarine monitoring in underwater surveillance

Social Sensing in WSNs (contd.)

- Possible Solution Approach: Duty-cycle management

- SMAC [Ye *et al*., INFOCOM, 2002]
- DutyCon [Wang *et al*., ACM TSN, 2013]
- PW-MAC [Tang *et al*., INFOCOM, 2011]

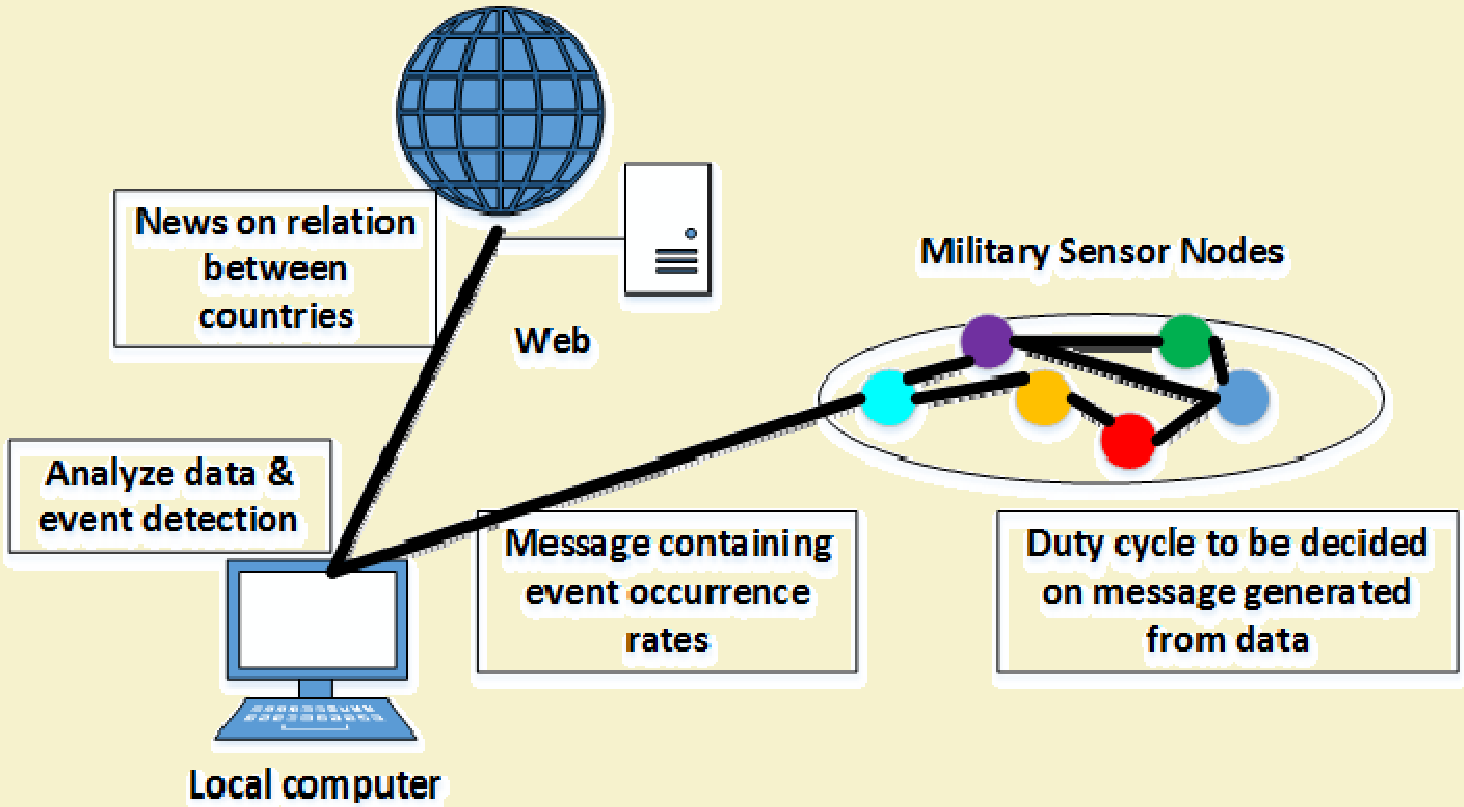
Limitations:

- Do not distinguish the rare events from regular events
- Ineffective wakeup and sensing under rare event monitoring scenario

Source: S. Misra, S. Mishra, M. Khatua, "Social Sensing-based Duty Cycle Management for Monitoring Rare Events in Wireless Sensor Networks", IET Wireless Sensor Systems

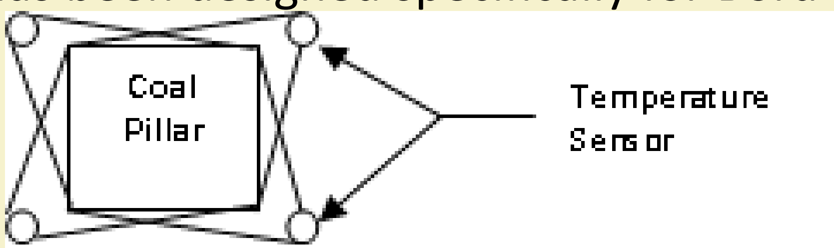
Social Sensing in WSNs (contd.)

- **Challenges**:
  - Distinguish rare events and regular events
  - Adapt the duty-cycle with the event occurrence probability.
- **Contribution**:
  - Probabilistic duty cycle (PDC) in WSNs
  - Accumulates information from the social media to identify the occurrence possibility of rare events
  - Adjusts the duty cycles of sensor nodes using weak estimation learning automata


News on relation between countries
Web
Military Sensor Nodes
Analyze data & event detection
Message containing event occurrence rates
Duty cycle to be decided on message generated from data
Local computer

Applications of WSNs: Mines

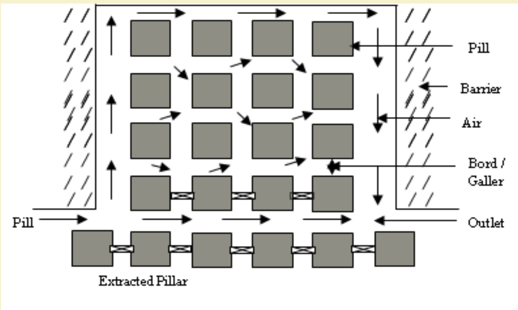
- ✓ Fire Monitoring and Alarm System for Underground Coal Mines Bord-and-Pillar Panel Using Wireless Sensor Networks
  - WSN-based simulation model for building a fire monitoring and alarm (FMA) system for Bord & Pillar coal mine.
  - The fire monitoring system has been designed specifically for Bord & Pillar based mines

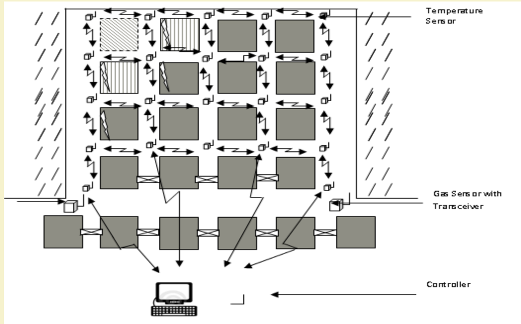


Source: S. Bhattacharjee, P. Roy, S. Ghosh, S. Misra, M. S. Obaidat, "Fire Monitoring and Alarm System for Underground Coal Mines Bord-and-Pillar Panel Using Wireless Sensor Networks", Journal of Systems and Software (Elsevier), Vol. 85, No. 3, March 2012, pp. 571-581.

Applications of WSNs: Mines (contd.)

- It is not only capable of providing real-time monitoring and alarm in case of a fire, but also capable of providing the exact fire location and spreading direction by continuously gathering, analysing, and storing real time information



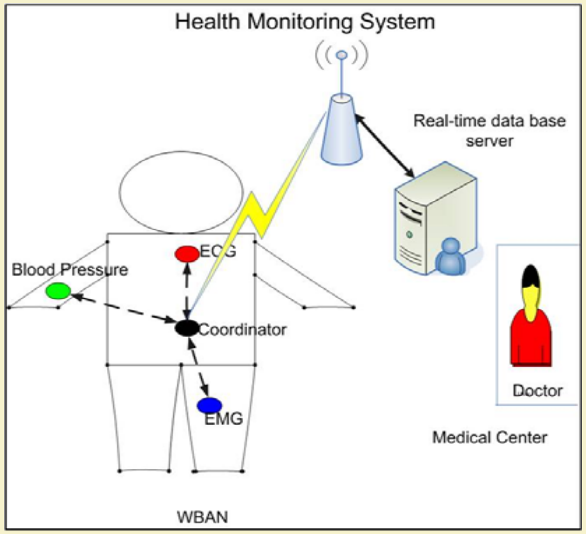


Source: S. Bhattacharjee, P. Roy, S. Ghosh, S. Misra, M. S. Obaidat, "Fire Monitoring and Alarm System for Underground Coal Mines Bord-and-Pillar Panel Using Wireless Sensor Networks", Journal of Systems and Software (Elsevier), Vol. 85, No. 3, March 2012, pp. 571-581.

Applications of WSNs: Healthcare

✓ Wireless Body Area Networks

- Wireless body area networks (WBANs) have recently gained popularity due to their ability in providing innovative, cost-effective, and user-friendly solution for continuous monitoring of vital physiological parameters of patients.
- Monitoring chronic and serious diseases such as cardiovascular diseases and diabetes.
- Could be deployed in elderly persons for monitoring their daily activities.



Applications of WSNs: Healthcare (contd.)

Social Choice Considerations in Cloud-Assisted WBAN Architecture

- A proper aggregation function necessarily needs to be “fair", so that none of the eligible elements are ignored unjustly.
- In a post-disaster environment, it is required to monitor patients' health conditions remotely.
- This includes ambulatory healthcare services where the health status of a patient is examined continuously over time, while the patient is being moved to the emergency healthcare center.

Source: S. Misra, S. Chatterjee, "Social Choice Considerations in Cloud-Assisted WBAN Architecture for Post-Disaster Healthcare: Data Aggregation and Channelization",Information Sciences (Elsevier), 2016

Applications of WSNs: Healthcare (contd.)

- The work focuses on the formation of pseudo-clusters so that the aggregation is not biased towards the leader nodes.
- Data aggregation among the LDPUs is done in a “fair" manner following the Theory of Social Choice.
- Aggregation is performed at mobile aggregation centers, thereby increasing the scalability of the system.
- After the aggregation of data, the gateways are allocated dynamically.

Source: S. Misra, S. Chatterjee, "Social Choice Considerations in Cloud-Assisted WBAN Architecture for Post-Disaster Healthcare: Data Aggregation and Channelization",Information Sciences (Elsevier), 2016

Applications of WSNs: Healthcare (contd.)

✓ **Payload tuning mechanism for WBANs**

- In addition to the actual health condition, there exists indirect influence of external parameters such as – age, height, weight, and sex on health parameters.
- In crisp set theory, we are unable to interpret how much ‘low’, ‘moderate’, or ‘high’, a particular health parameter is.
- Exclusion of the important external parameters while assessing health and the usage of traditional crisp set theory may result into inefficient decision making.

Source: S. Moulik, S. Misra, C. Chakraborty, M. S. Obaidat, "Prioritized Payload Tuning Mechanism for Wireless Body Area Network-Based Healthcare Systems", Proceedings of IEEE GLOBECOM, 2014

Applications of WSNs: Healthcare (contd.)

- Challenge is to design a dynamic decision making model that can optimize the energy consumption of each physiological sensor
- Fuzzy inference system (FIS) and markov decision process (MDP) are used to optimize energy consumption

Source: S. Moulik, S. Misra, C. Chakraborty, M. S. Obaidat, "Prioritized Payload Tuning Mechanism for Wireless Body Area Network-Based Healthcare Systems", Proceedings of IEEE GLOBECOM, 2014

Applications of WSNs: Healthcare (contd.)

✓ **Priority-Based Time-Slot Allocation in WBANs**

- In medical emergency situations, it is important to discriminate the WBANs transmitting critical heath data from the ones transmitting data of regular importance.
- Existing frequency division-based transmission in a multisource-single-sink network results in flooding of the sink's receiver buffer.
- This leads to packet loss and consequent retransmission of the regenerated packets.

Source: S. Misra, S. Sarkar, "Priority-Based Time-Slot Allocation in Wireless Body Area Networks During Medical Emergency Situations: An Evolutionary Game Theoretic Perspective", IEEE Journal of Biomedical and Health Informatics, 2014

Applications of WSNs: Healthcare (contd.)

- Transmission priority of an local data processing unit (LDPU) is indifferent to the criticality of the health data that is being transmitted by the LDPU.
- Based on LDPU-properties, such as the criticality of health data, energy dissipation factor, and time elapsed since last successful transmission, a fitness parameter is formulated which is a relative measure of node-importance.
- The priority-based allocation of time slots (PATS) algorithm allows the LDPUs to choose their strategies based on their fitness.
- LDPUs with higher fitness are given higher preference, while ensuring minimum waiting time between successive transmission of data-packets.

Source: S. Misra, S. Sarkar, "Priority-Based Time-Slot Allocation in Wireless Body Area Networks During Medical Emergency Situations: An Evolutionary Game Theoretic Perspective", IEEE Journal of Biomedical and Health Informatics, 2014

Thank You!!