National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

M2M and IoT

Dr. Madhavi Dave
Assistant Professor
School of Cyber Security and Digital Forensics

Introduction

- Machine-to-machine, or M2M, is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.
- M2M technology was first adopted in manufacturing and industrial settings, and later found applications in healthcare, business, insurance and more.
- It is also the foundation for the internet of things.
- **M2M** and **IoT** both refer to devices communicating with each other.
- M2M refers to isolated instances of device-to-device communication.
- IoT refers to a grander scale, synergizing vertical software stacks to automate and manage communications between multiple devices.

Difference:

M2M	IoT
Machines	Sensors
Hardware-based	Software-based
Vertical applications	Horizontal applications
Deployed in a closed system	Connects to a larger network
Machines communicating with machines	Machines communicating with machines, humans with machines, machines with humans
Uses non-IP protocol	Uses IP protocols
Can use the cloud, but not required to	Uses the cloud
Machines use point-to-point communication, usually embedded in hardware	Devices use IP networks to communicate
Often one-way communication	Back and forth communication
Main purpose is to monitor and control	Multiple applications; multilevel communications
Operates via triggered responses based on an action	Can, but does not have to, operate on triggered responses
Limited integration options, devices must have complementary communication standards	Unlimited integration options, but requires software that manages communications/protocols
Structured data	Structured and unstructured data

How M2M Works?

- The main purpose of machine-to-machine technology is to tap into sensor data and transmit it to a network.
- M2M systems often use public networks and access methods - for example, cellular or Ethernet - to make it more cost-effective.
- Energy efficiency and wireless connectivity are the key for M2M / IoT.
- M2M Communication is a subset of IoT.
- IoT comprises M2M and H2M (Human to Machine) communication.
- In practice the IoT will consist of hybrid infrastructure of non IP and IP connected devices through IP connected gateways.

- One of the most well-known types of machine-to-machine communication is telemetry, which has been used since the early part of the last century to transmit operational data.
- Pioneers in telemetrics first used telephone lines, and later, radio waves, to transmit performance measurements gathered from monitoring instruments in remote locations.
- The internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday use in products such as heating units, electric meters and internet-connected devices, such as appliances.

Benefits of M2M

- Reduced costs by minimizing equipment maintenance and downtime.
- Boosted revenue by revealing new business opportunities for servicing products in the field.
- Improved customer service by proactively monitoring and servicing equipment before it fails or only when it is needed.

Network QoS Requirements

- M2M communication is different from the voice communication as size of data in M2M may vary from few bytes (meter reading) to several MBs (surveillance video).
- M2M services requirement
  - **Timely transmission is of utmost important.**
  - **Communication network is required to be more reliable with low latency**

Applications

- Machine-to-machine communication is often used for remote monitoring.
- M2M devices can enable the real-time monitoring of patients' vital statistics, dispensing medicine when required, or tracking healthcare assets.
- M2M is also an important aspect of remote control, robotics, traffic control, security, logistics and fleet management, and automotive.

S. No.	Industry / Vertical	M2M applications
1.	Smart City	Intelligent transport System, Waste management, Smart Street Light system, Electric vehicle charging, Water management, Smart Parking, Intelligent buildings, Safety & Surveillance,
2.	Automotive / Intelligent Transport System	Vehicle tracking, e-call, V2V and V2I applications, traffic control, Navigation, Infotainment, Fleet management, asset tracking, manufacturing and logistics
3.	Safety & Surveillance	Commercial and home security monitoring, Surveillance applications, Video analytics and sending alerts, Fire alarm, Police / medical alert
4.	Utilities / Energy	Smart metering, smart grid, Electric line monitoring, gas / oil / water pipeline monitoring.
5.	Health care	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, Tele-medicine, wearable health devices
6.	Smart Homes	Video monitoring of home, Security & Alarm, Door control, HVAC control, Smart lighting for efficiency, Controlling appliances through Smart phones etc.
7.	Financial /Retail	Point of sale (POS), ATM, Kiosk, Vending machines, digital signage and handheld terminals.
8.	Water	Smart metering, Water leakage management

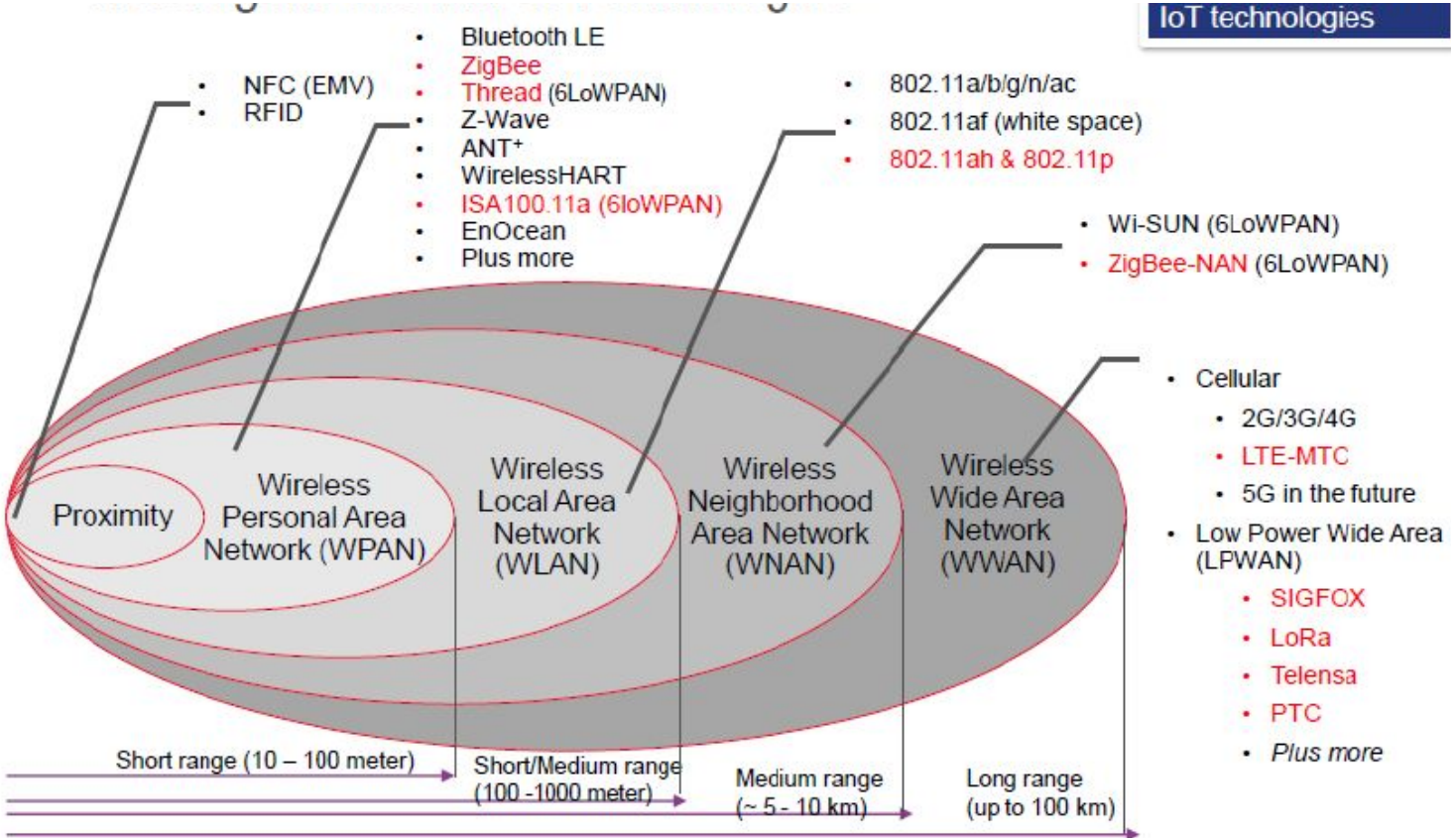
Enabling technologies for M2M

- Sensor networks, Radio frequency Identification (RFID) chips, GPS, Location-Based Services (LBS), nanotechnologies, cloud services, data analytics.
- WLAN (IEEE 802.11), Bluetooth Low Energy (BLE), NFC, DSRC for short range communication.
- Low Power RF for LAN / FAN such as 6LowPAN, Zigbee, Zwave, Wi-SUN etc
- Cellular 2G/ 3G/ LTE / Satellite for Long range communication depending upon the applications.
- Wire line BB / Lease line to connect infrastructure
- Power Line Communication Technologies: Narrowband PLC for LAN and Broadband PLC for WAN
- Low power RF for WAN: LoRa, Sigfox
- Embedded SIM
- Static IP (IPv4 / IPv6)
- Smart Phone
- High speed internet on fixed line and mobile phones.

Backbone network

- Smooth & high speed WiFi coverage, WiFi offloading with the TSPs.
- Control plane at the center whereas data may be in distributed servers.
- Data centers in the cloud for storing large amount of data from the devices.
- Big data analytics to create intelligence.
- Use of intelligence for different activities.
- Open APIs
- ICT Infrastructure
- RFID based system.

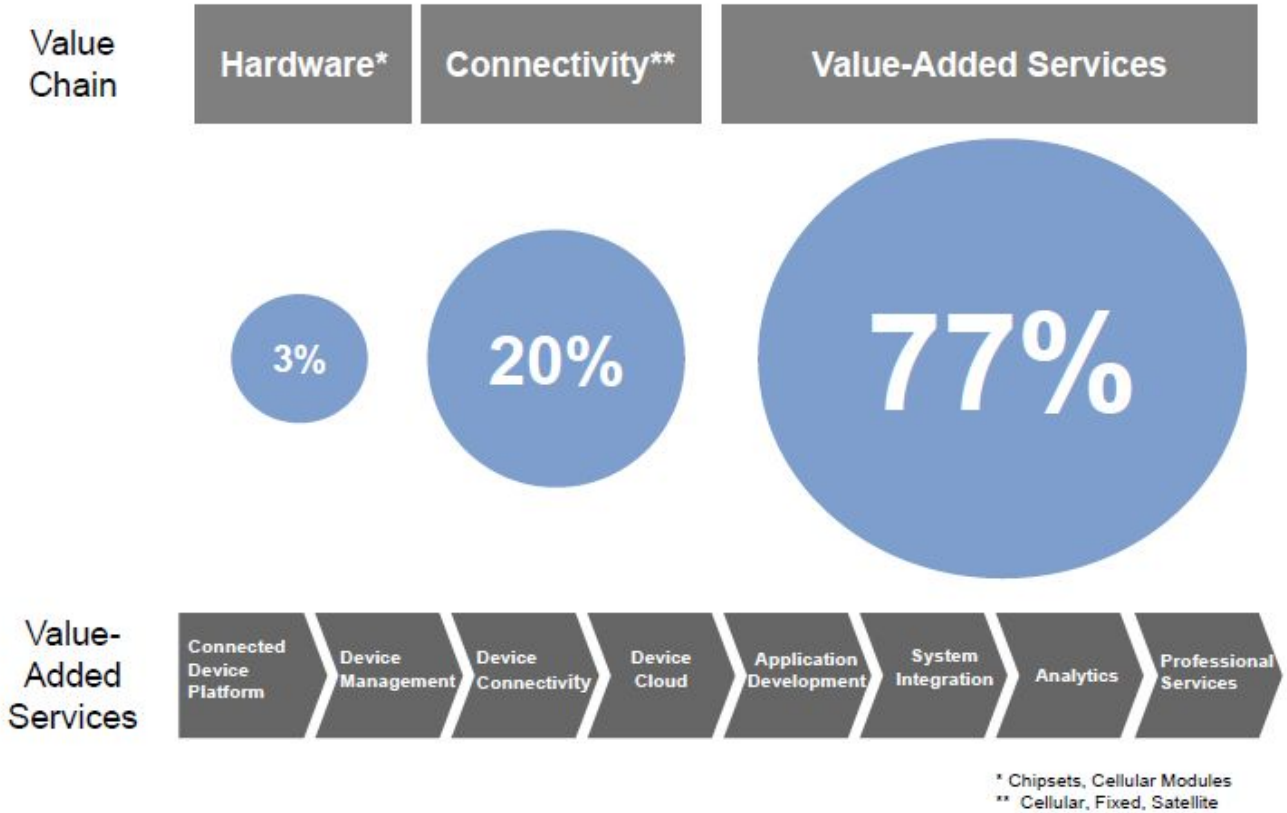
IoT technologies



Challenges and need for standards in M2M

- Lack of standards and interoperable technologies
- Technologies for sustainability or low power consumption / long life batteries required for sensors.
- There should be interoperability at device, network and application levels.
- Slow deployment of IPv6
- Low cost devices (affordability)
- Data Security & Privacy
- Health care regulations

M2M Value Chain



National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

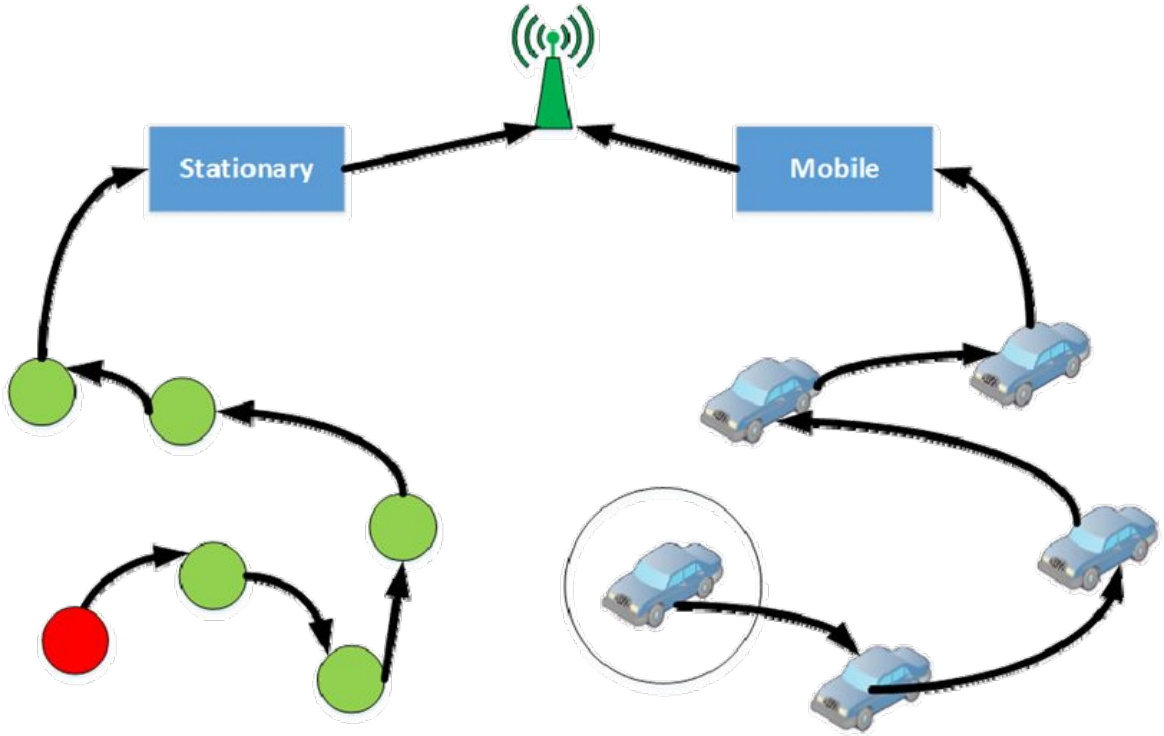
Wireless Sensor Network

Dr. Madhavi Dave
Assistant Professor
School of Cyber Security and Digital Forensics

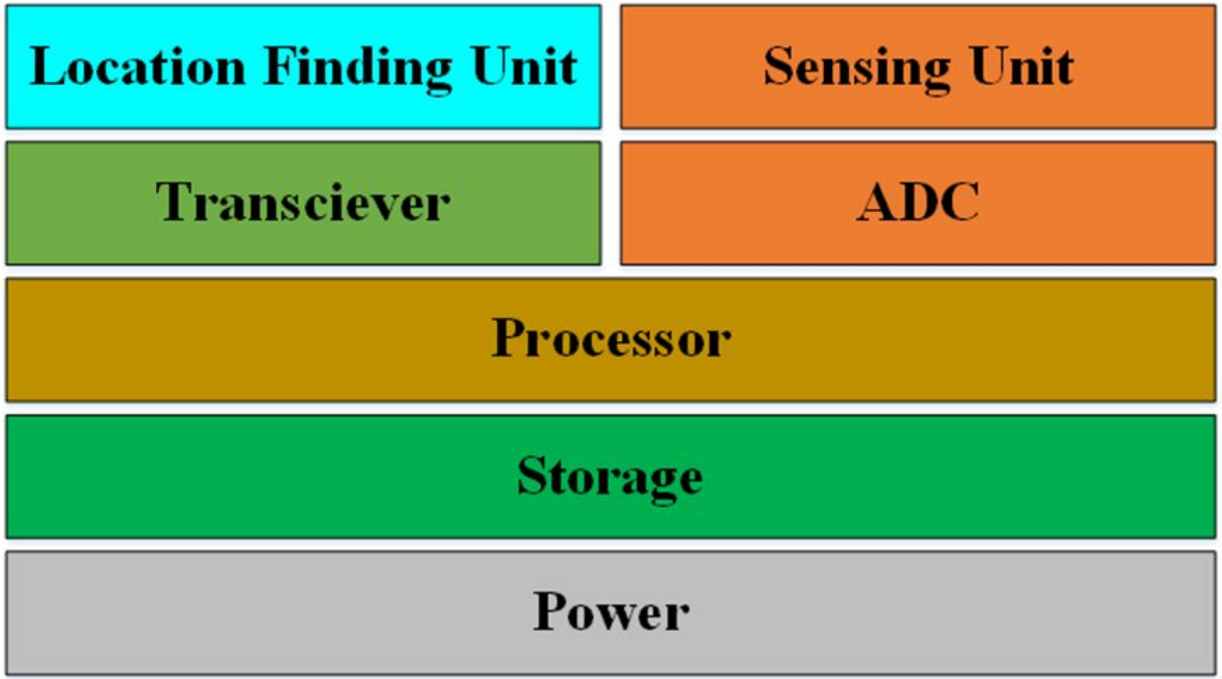
Wireless Sensor Network (WSN)

- 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.

Multihop Communication in WSN



Basic Components of Sensor Node



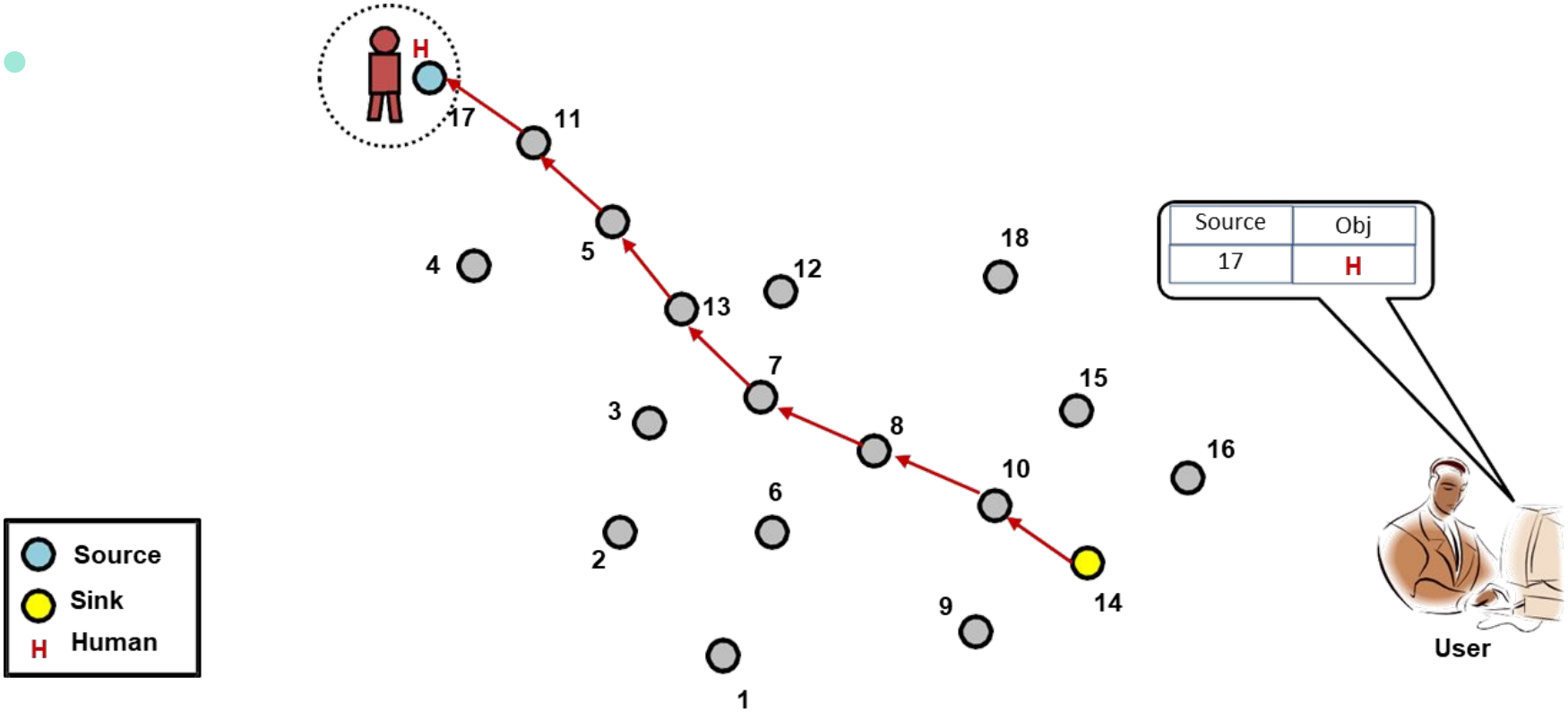
Sensor Node

- **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.

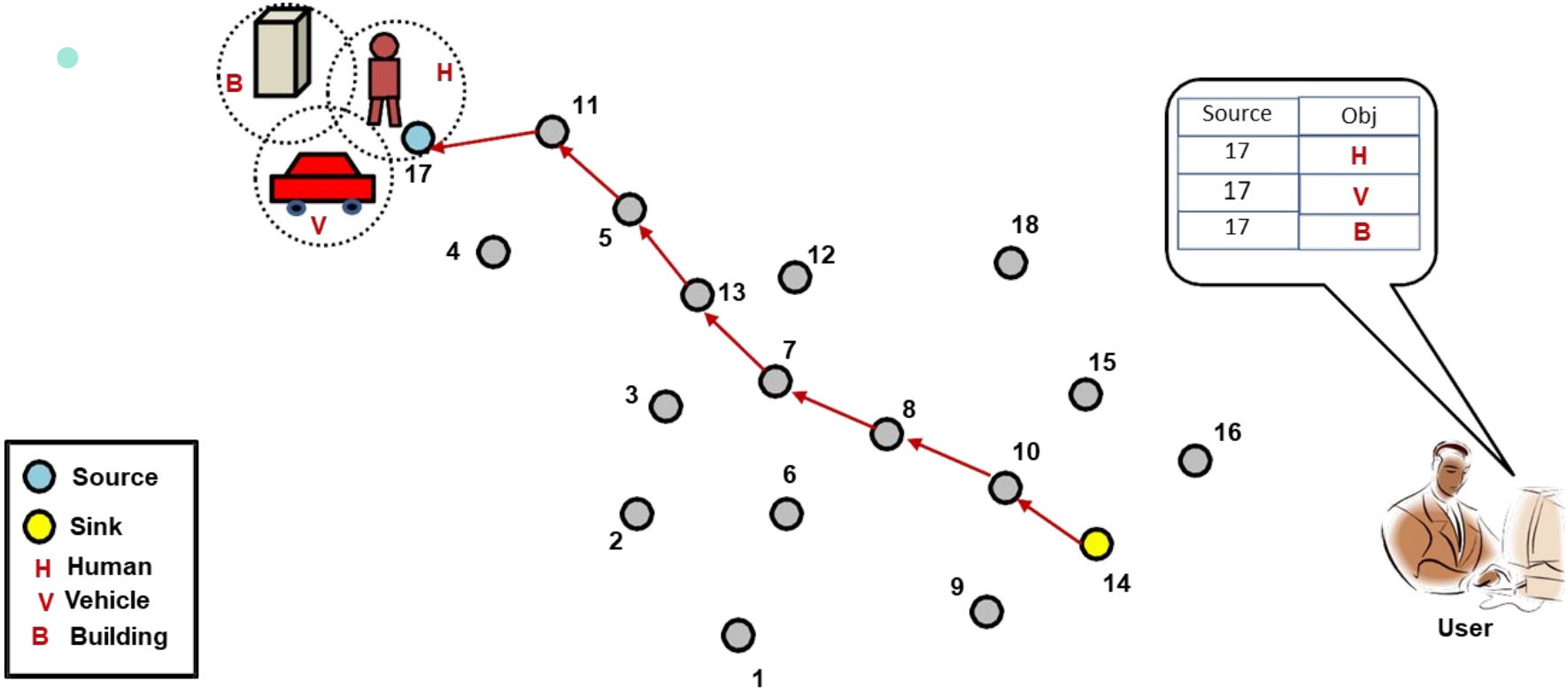
Constraint of Sensor Node

- 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

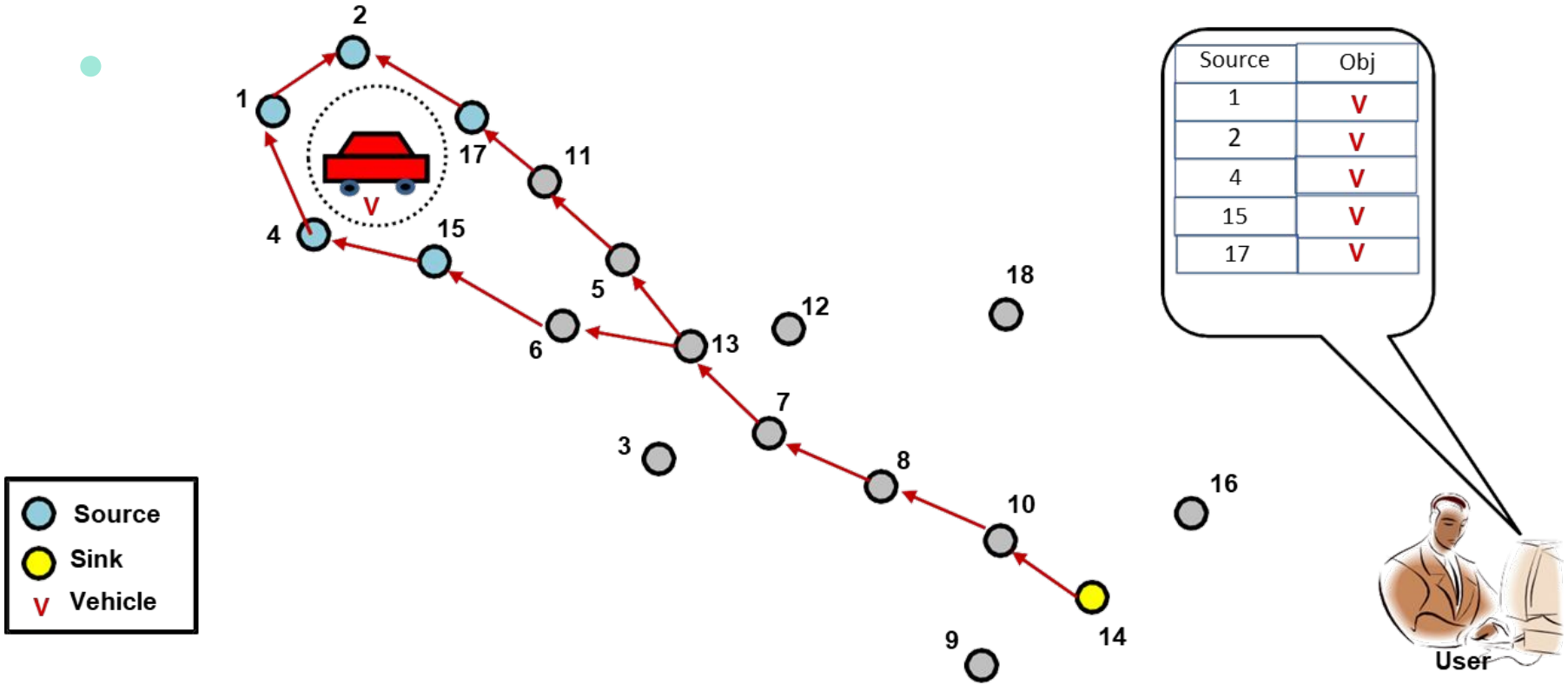
Single Source Single Object Detection



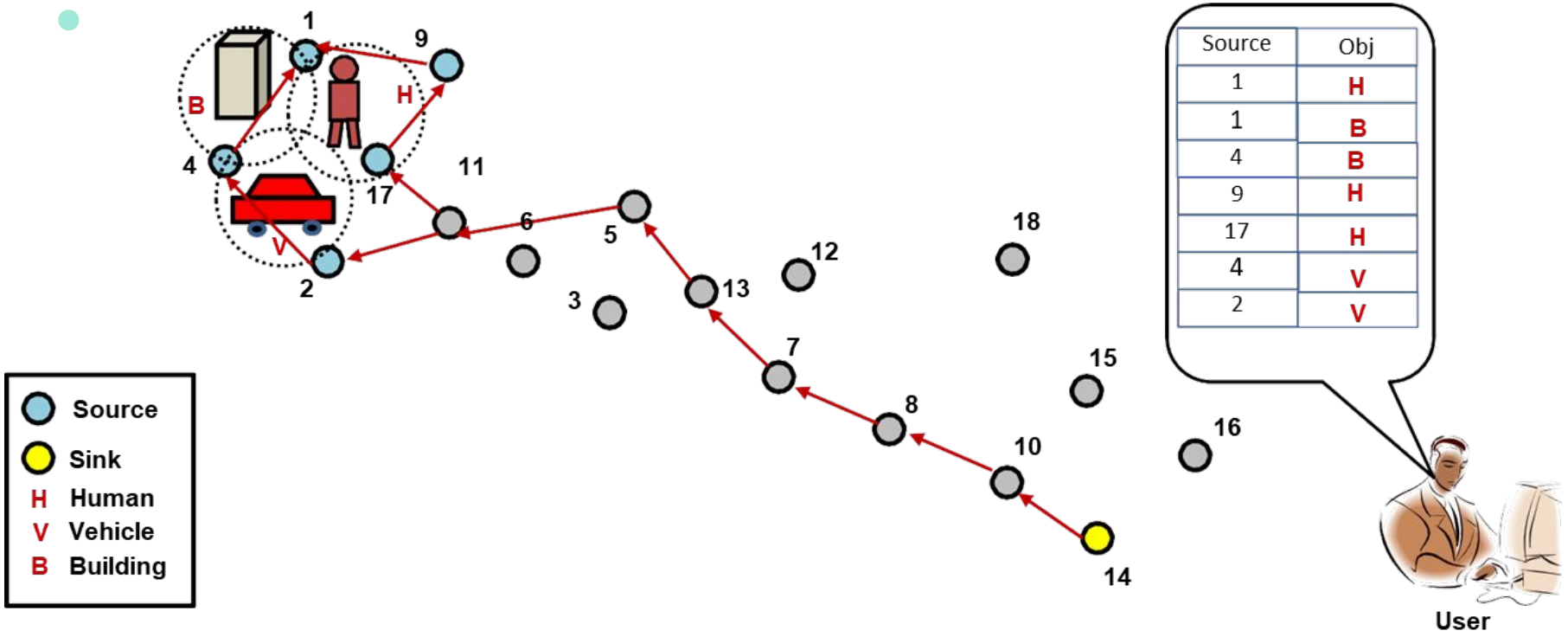
Single Source Multiple Object Detection



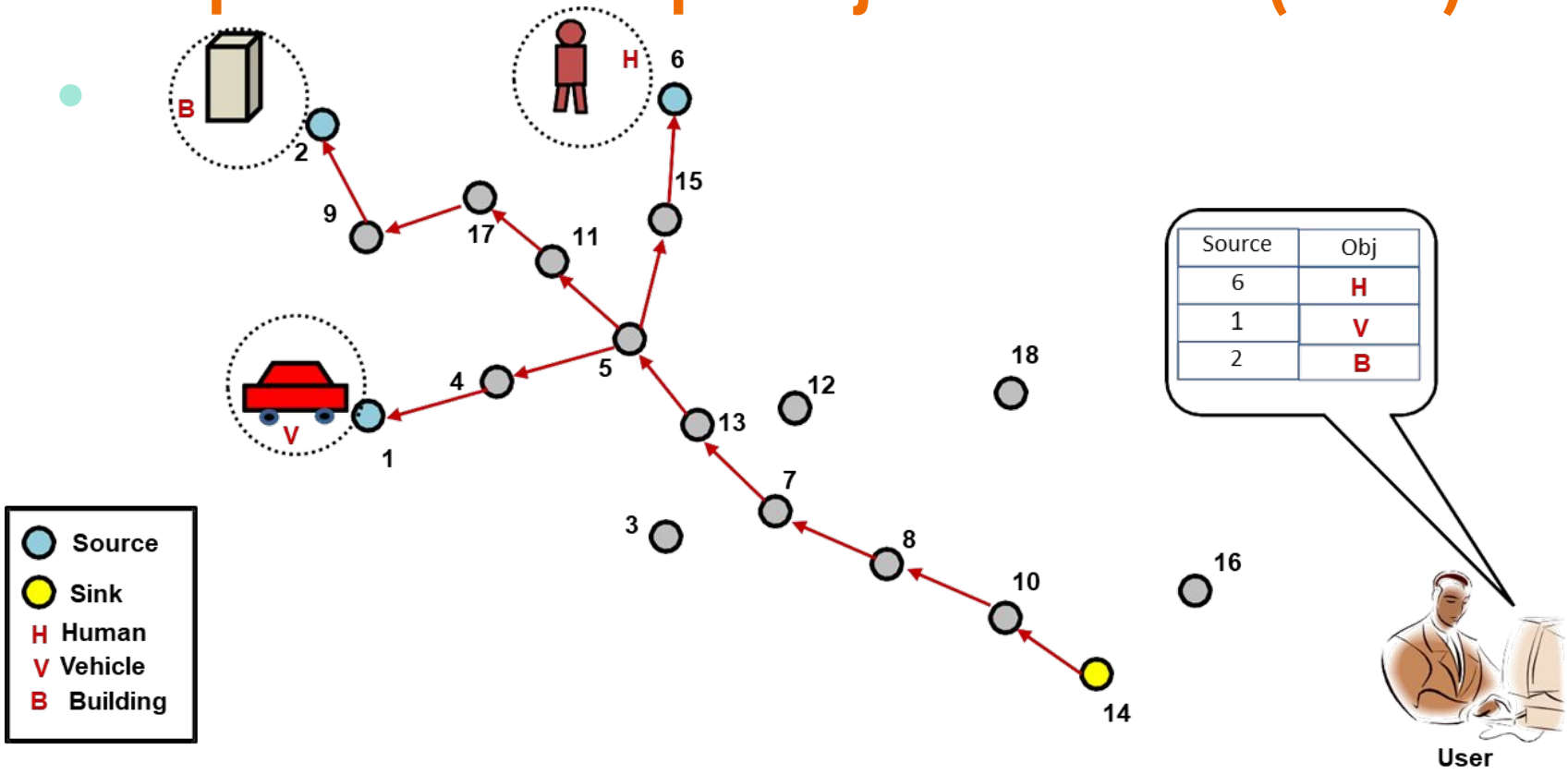
Multiple Source Single Object Detection



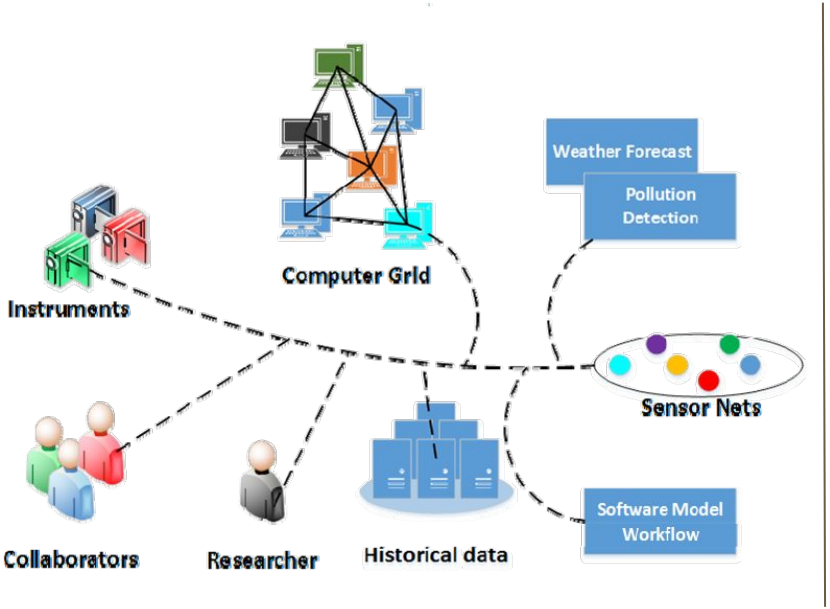
Multiple Source Multiple Object Detection

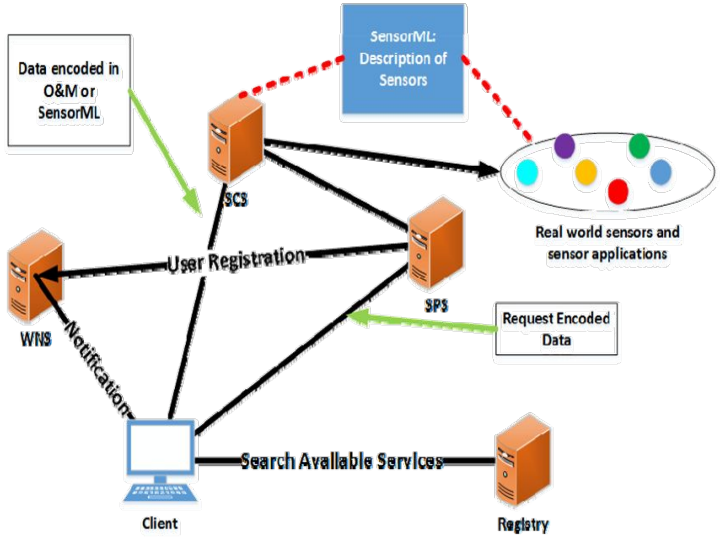


Multiple Source Multiple Object Detection (cont..)



Sensor Web





WNS: Web Notification Services

SCS: Sensor Collection Services

SPS: Sensor Planning Services

SensorML: Sensor Modeling language

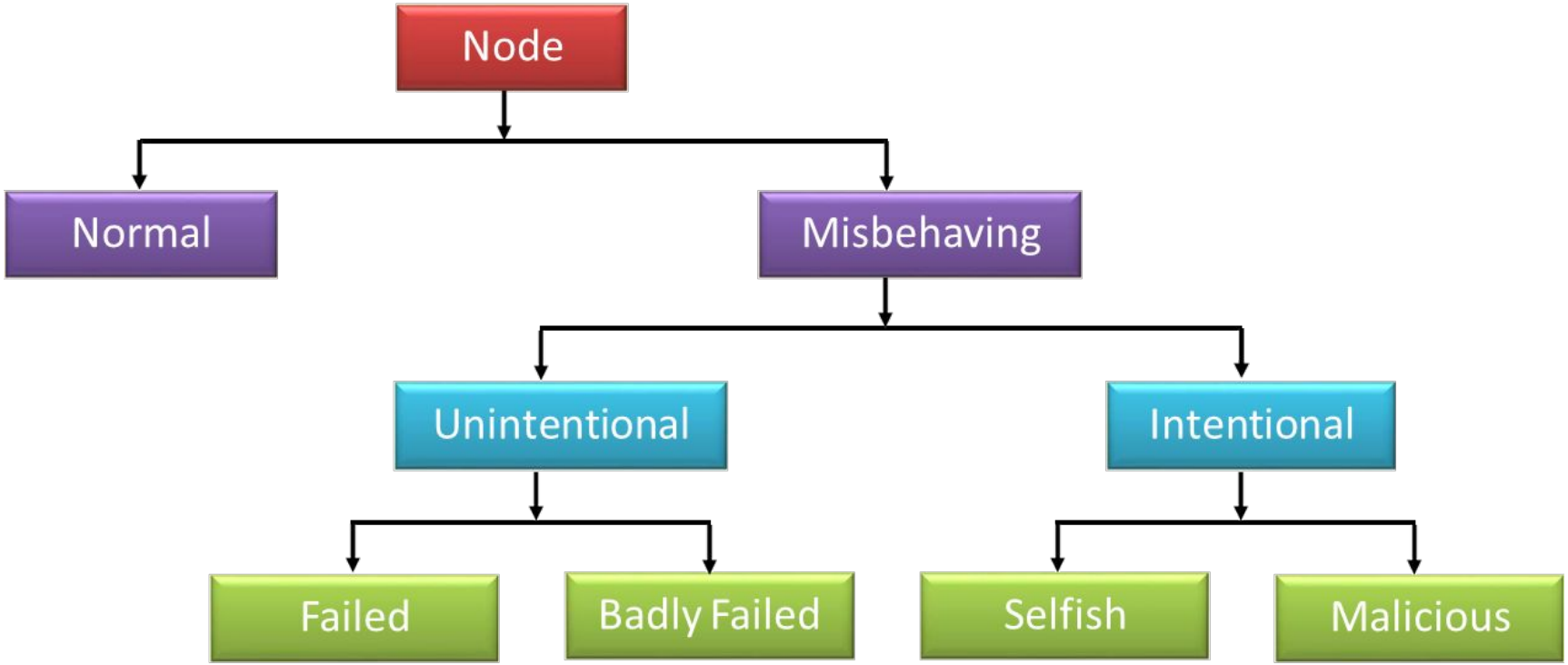
Challenges

- Scalability
  - Providing acceptable levels of service in the presence of large number of nodes.
  - Typically, throughput decreases at a rate of number of nodes increases.
- Quality of service
  - Offering guarantees in terms of bandwidth, delay, jitter, packet loss probability.
  - Limited bandwidth, unpredictable changes in RF channel characteristics.
- 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

Security Challenges

- 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.

Node Behaviour in WSN



Node Behaviour in WSN (cont..)

- **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.
- **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 Misbehaviour: Dumb Node

- 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 Connection 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 WSN

- 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