M2M: Machine-to-Machine Communications (M2M)

One of the new technologies that's part of the Internet of Things is Machine-to-Machine (M2M) communications. M2M, though not well-defined, is a set of methods and protocols to allow devices to communicate and interact over the Internet (or other network) without human intervention. M2M is sometimes considered to be low-overhead short-range wireless communication between machines, utilizing protocols with much less overhead than full-blown TCP/IP. Many M2M applications involve low power wireless devices with limited computing power and narrowly- defined functionality. Low-overhead protocols have been devised for them, including Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and Open Mobile Alliance Light Weight M2M (OMA LWM2M). CoAP is actually a specialized web transfer protocol designed for applications such as smart energy and building automation. There is, of course, no reason why IoT devices cannot use high-powered CPUs and wide bandwidth, and in many applications, this is clearly necessary, such as smart cars interacting with external servers. So IoT spans a huge range from very simple low-powered specialized devices and sensors with low bandwidth needs to complex, high-powered devices in large high-bandwidth environments.

- M2M refers to communications and interactions between machines and devices.
- Such interactions can occur via a cloud computing infrastructure (e.g., devices exchanging information through a cloud infrastructure).
- M2M offers the means for managing devices and devices interaction, while also collecting machine and/or sensor data.
- M2M is a term introduced by telecommunication services providers and, pays emphasis on machines interactions via one or more telecom/communication networks (e.g., 3G, 4G, 5G, satellite, public networks).

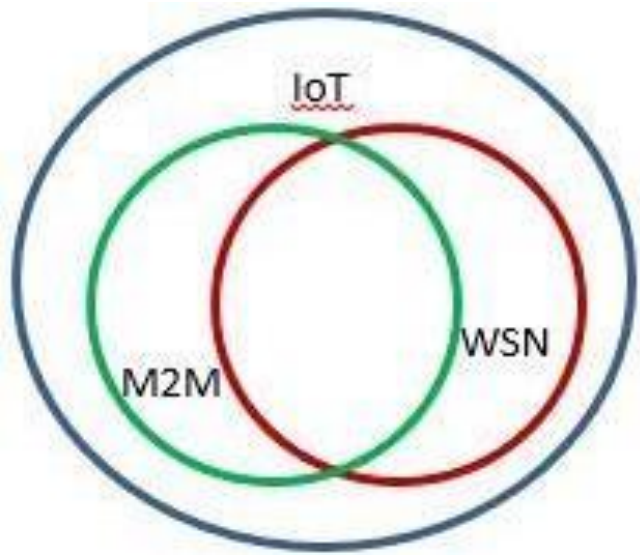
Wireless Sensor Networks (WSNs)

IoT configurations often involve sensors, which can be connected by wireless networks. Such sensor networks are termed "Wireless Sensor Networks" or WSNs. A WSN comprises spatially distributed autonomous devices equipped with sensors, connected through a wireless network to some type of gateway. The sensors typically monitor physical or environmental conditions. The gateway communicates with another set of devices that can act on the information from the sensors.

Applications

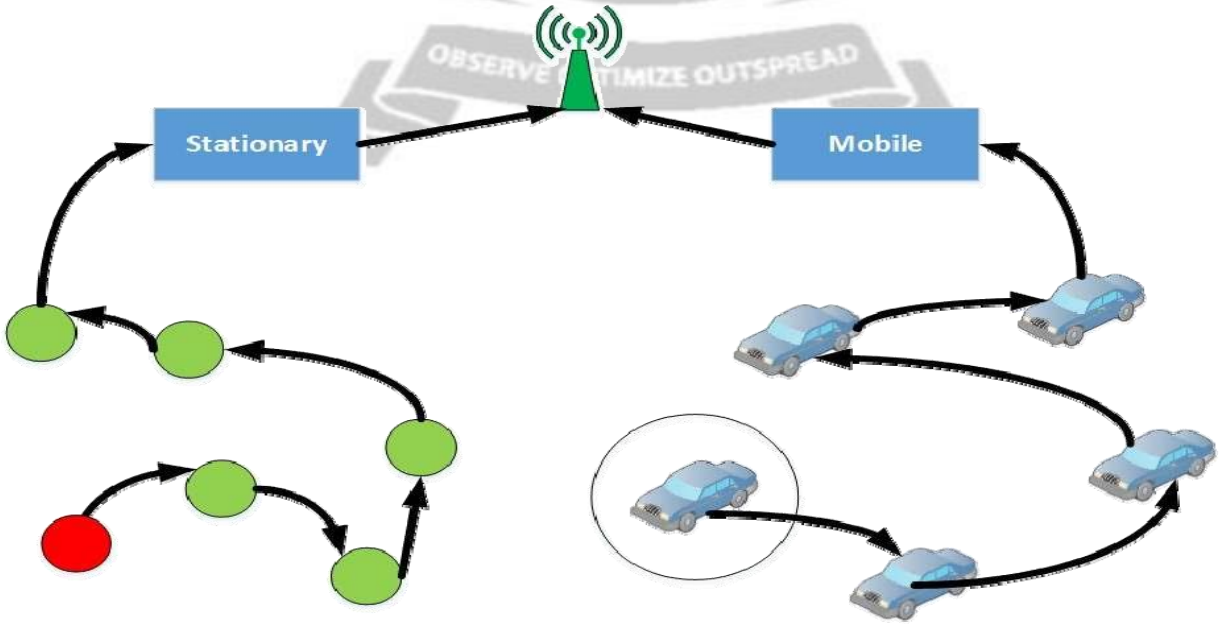
- patient monitoring
- environmental monitoring of air, water, and soil
- structural monitoring for buildings and bridges
- industrial machine monitoring and process monitoring.

The wireless network could be WiFi or Bluetooth, and the protocol one of the three listed above. The boundaries between these networks are not clearly drawn, and in practice they overlap considerably.

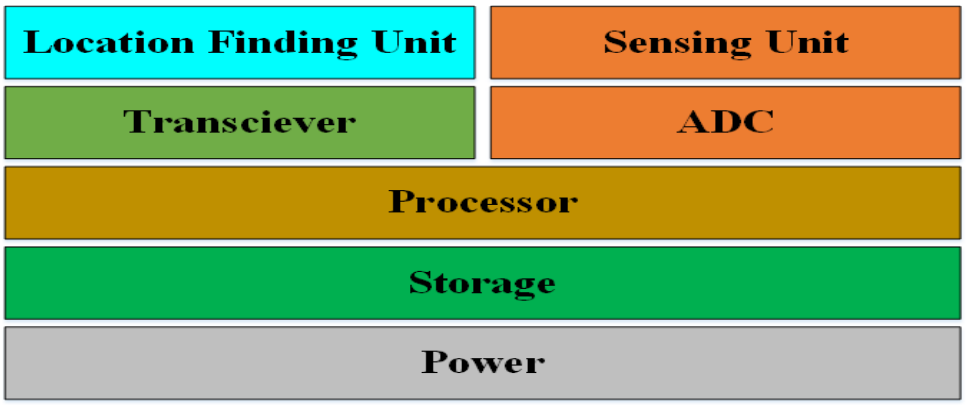


- Consists of a large number of sensor nodes, densely deployed over an area.
- Sensor nodes are capable of collaborating with one another and measuring the condition of their surrounding environments (i.e. Light, temperature, sound, vibration).
- The sensed measurements are then transformed into digital 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.

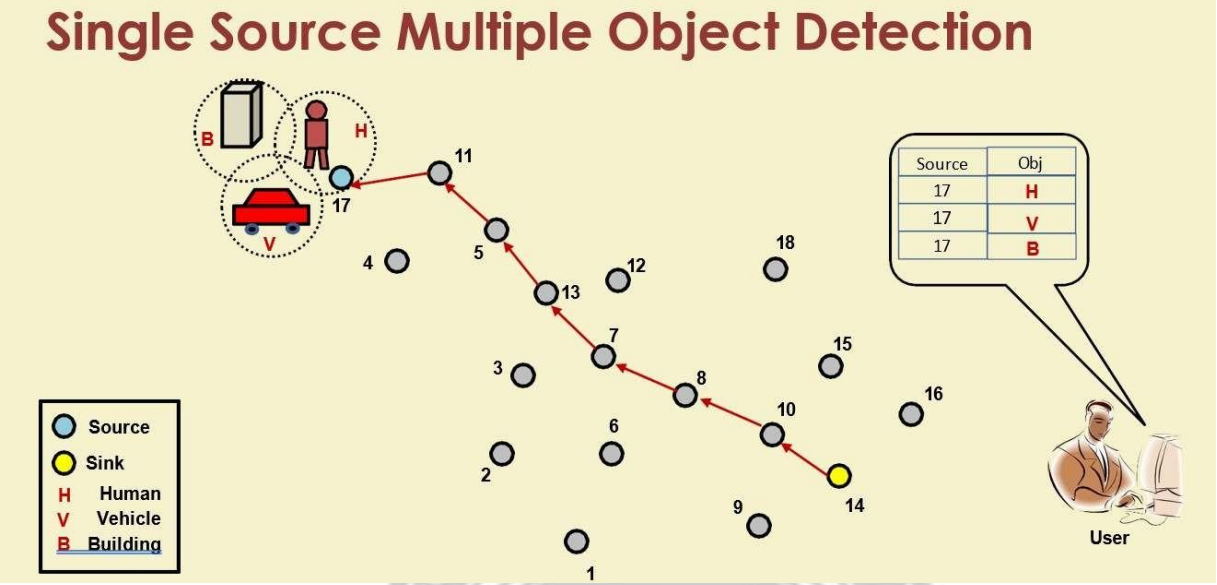
Constraints on Sensor Nodes

- ✓ 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

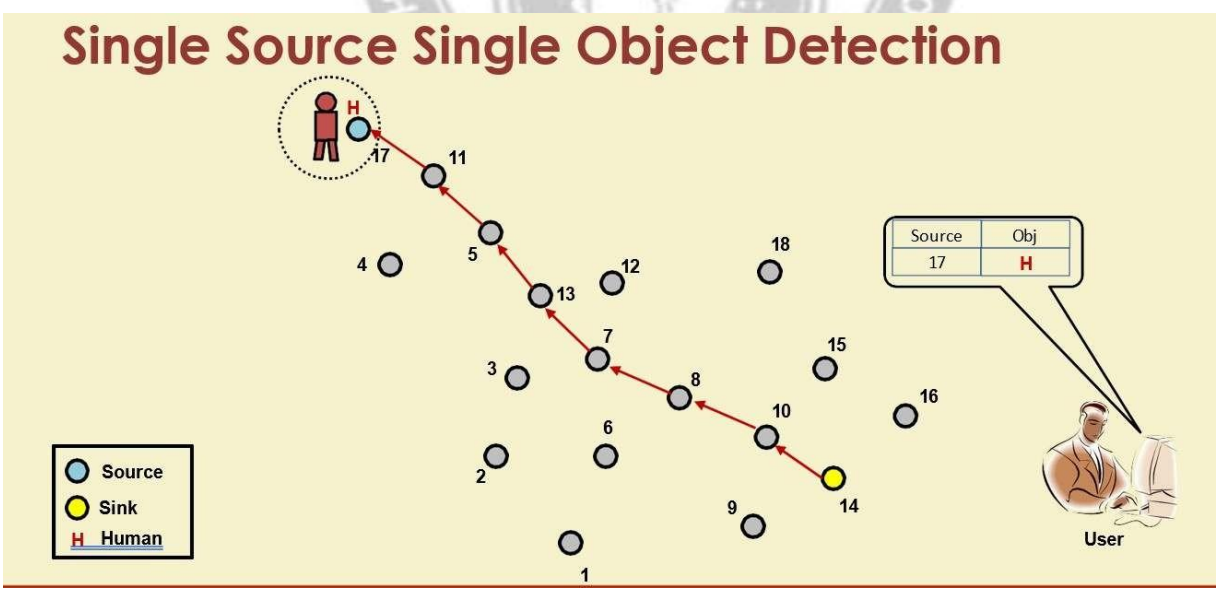
Applications

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

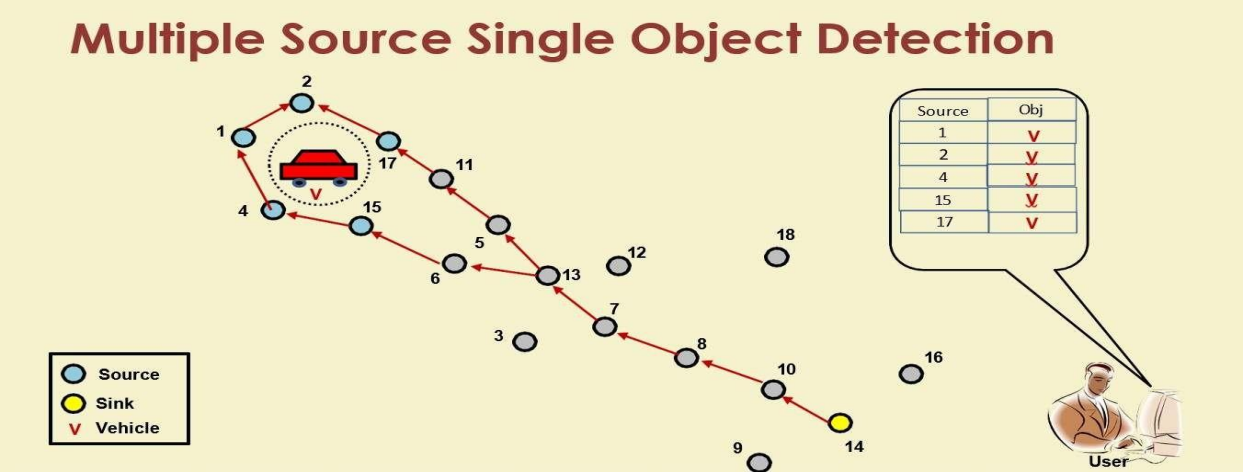
Detection Techniques



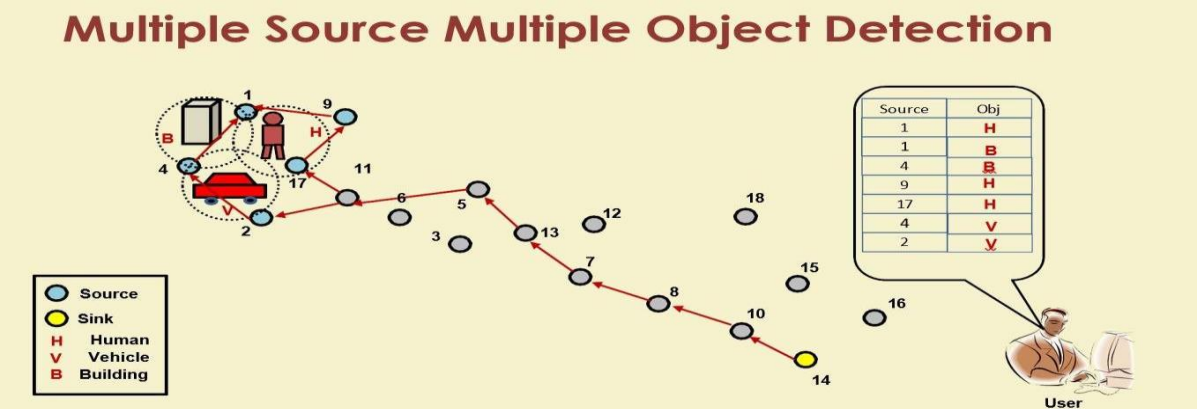
The Source node is only one and the object detected is also only one.



The source node is only one and the objects detected are multiple.



Only one object is detected by multiple sources.



Multiple objects are detected by multiple source nodes.

Challenges Scalability

- ✓ Providing acceptable levels of service in the presence of large 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.

Energy efficiency

- ✓ Nodes have limited battery power

Security

- ✓ Nodes need to cooperate with other nodes for relaying their information.
- ✓ Open medium.
- ✓ Nodes prone to malicious attacks, infiltration, eavesdropping, interference.