Unit 1

Textbook(s):

- 1) Protocols and Architectures for Wireless Sensor Network, Holger Kerl, Andreas Willig, John Wiley and Sons, 2005
- 2) Wireless Sensor Networks Technology, Protocols, and Applications ,Kazem Sohraby, Daniel Minoli and TaiebZnati, John Wiley & Sons, 2007
- 3) Mobile communications, Jochen Schiller,2nd Edition, Addison wisely , Pearson Education, 2012

- Sensor: A Sensor is a electronic device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument.

Introduction to Sensor Networks

- Wireless sensor are the class of networks where the nodes are sensor nodes.
- The nodes which sense or which have the capability of sensing the physical phenomenon that occurred around them.
- These sensing can be of different types. Like sensor node might be able to sense temperature ,colors, vibration and so on.
- These sensor nodes collectively they form a network which is called the wireless sensor networks.
- WSN are very popular now days because of diverse type of application .

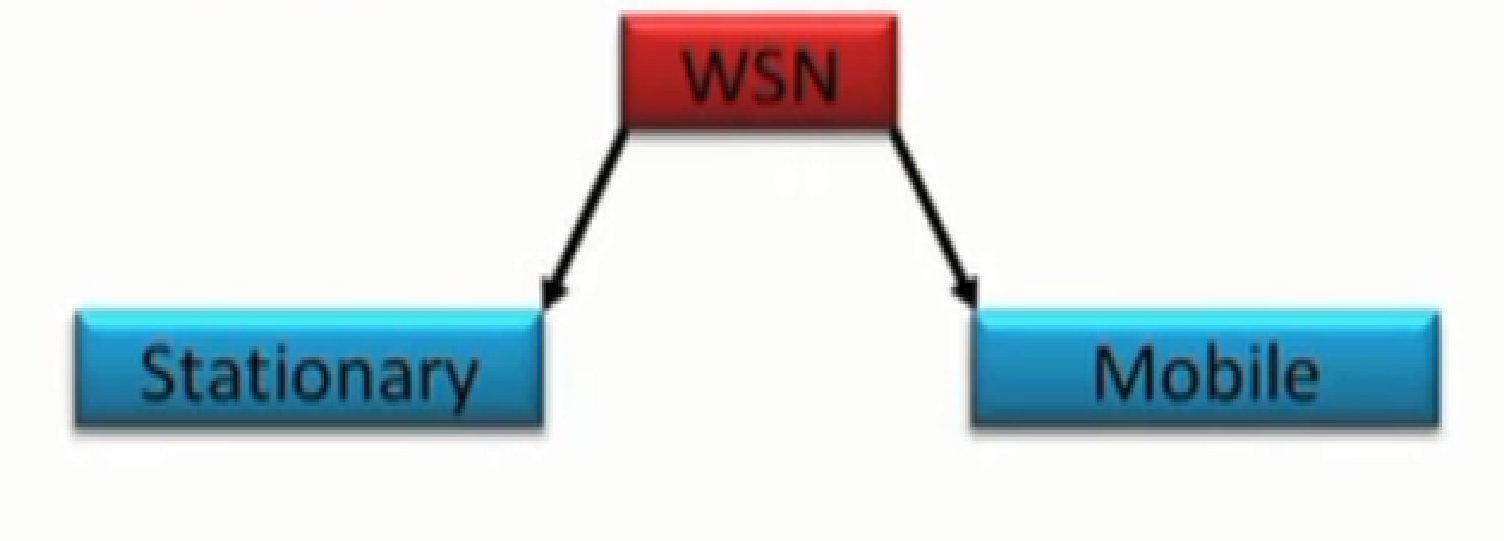
Wireless sensor networks

- Consists of 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(Light, temperature, sound, vibration).
- The sensed measurement 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 wsn have short radio transmission range, intermediate node act as relay nodes to transmit the data towards the sink node using a multi-hop path.

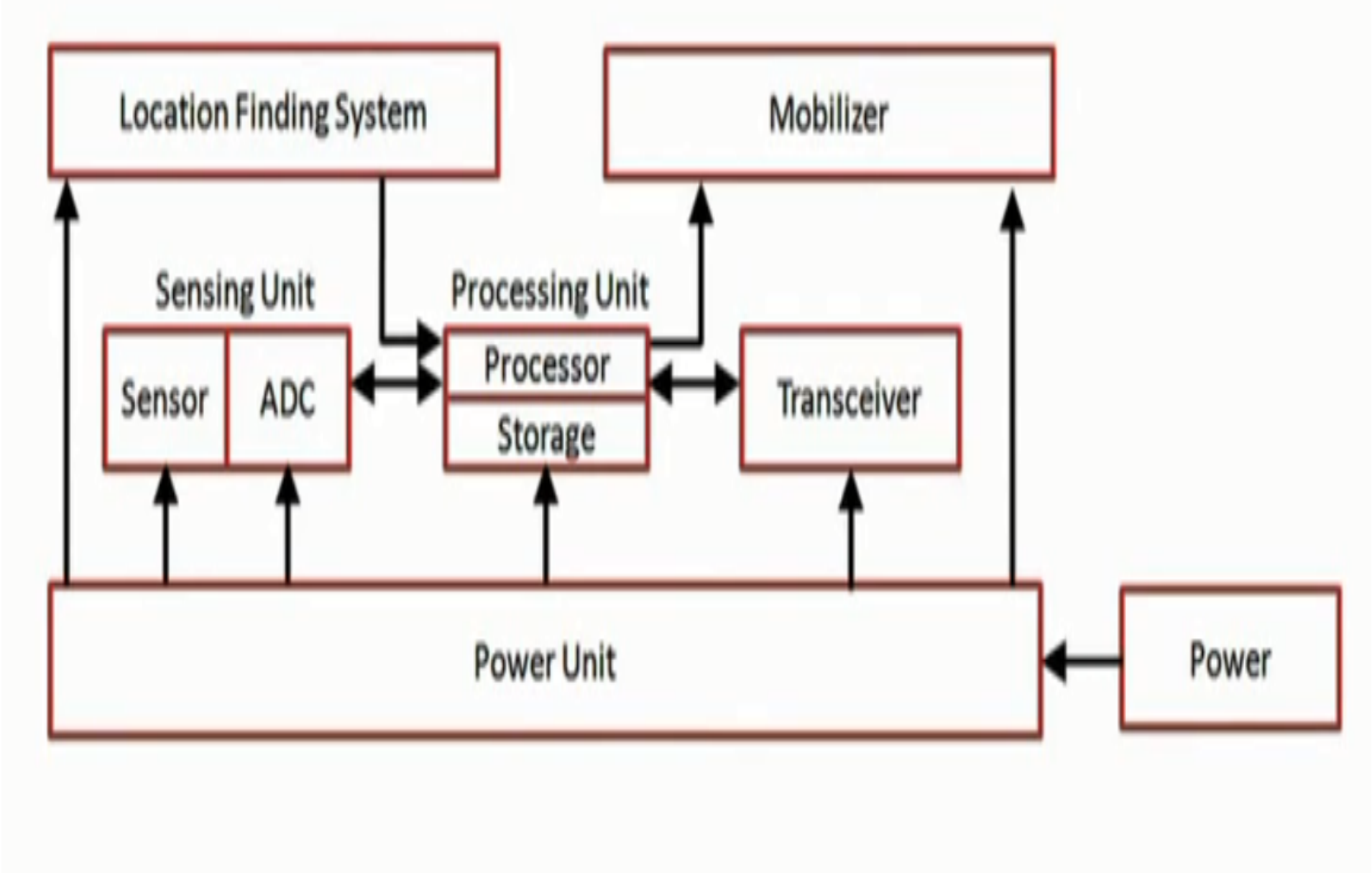
Why we need WSN? Instead of single sensor

- In WSN we can deploy multiple such sensors and sensor nodes over a large area to get an idea about what is occurring in that larger area so basically to have bigger sensing coverage over bigger area.

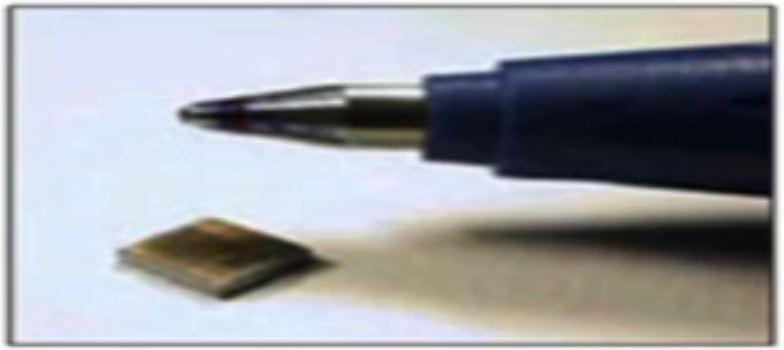
Classification



Basic Components of a Sensor Node



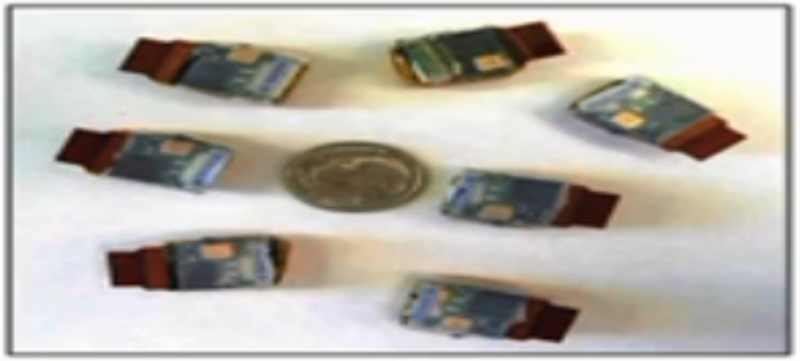
Sensor Nodes(Different Sizes and Shapes)



(a)

(b)

(a) Xbow mica mote [ZESS] (b) Eco [CHOU]



(c)

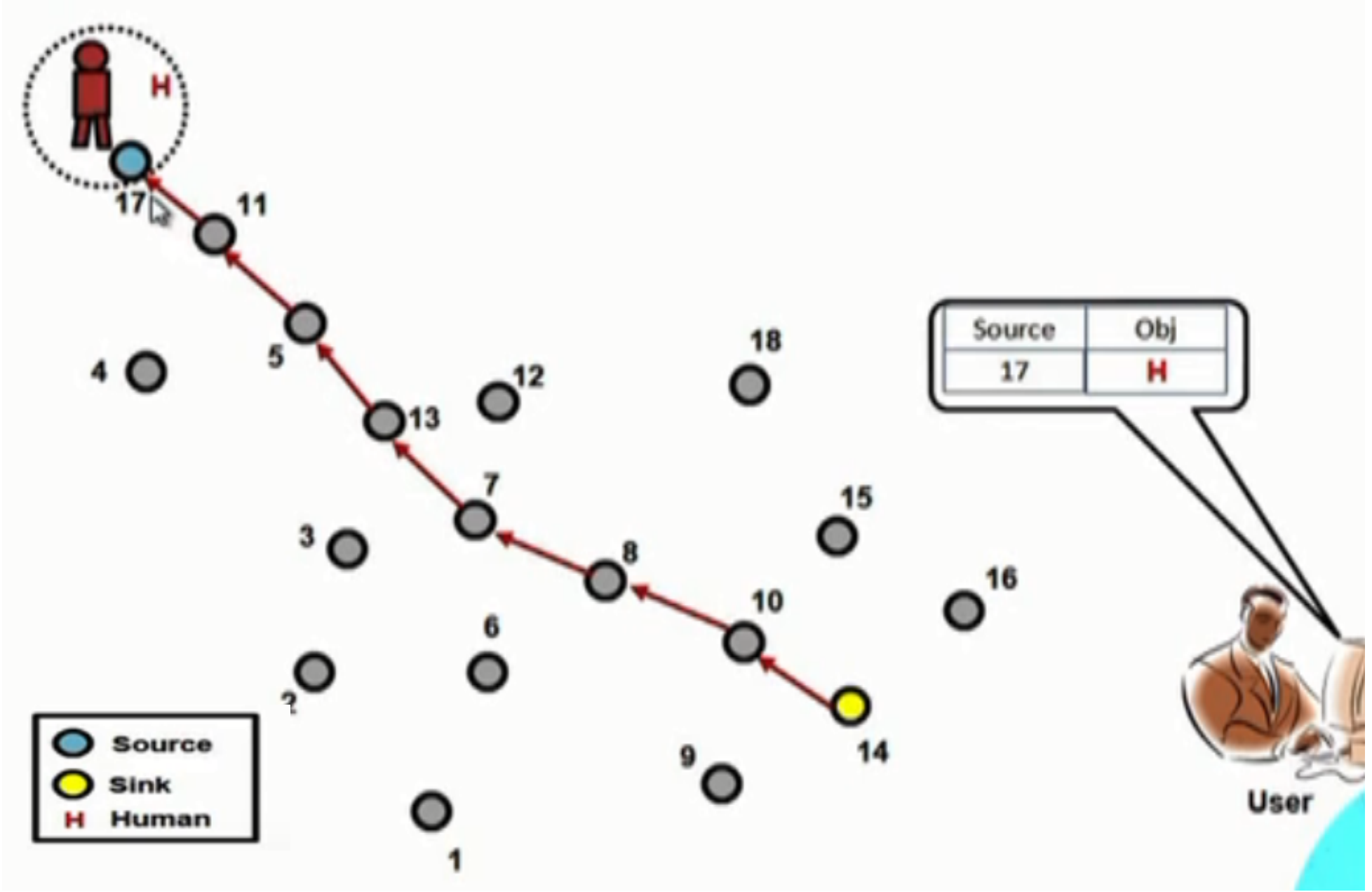
(d)

(c) Eco [MOTE] (d) dots [BERK]

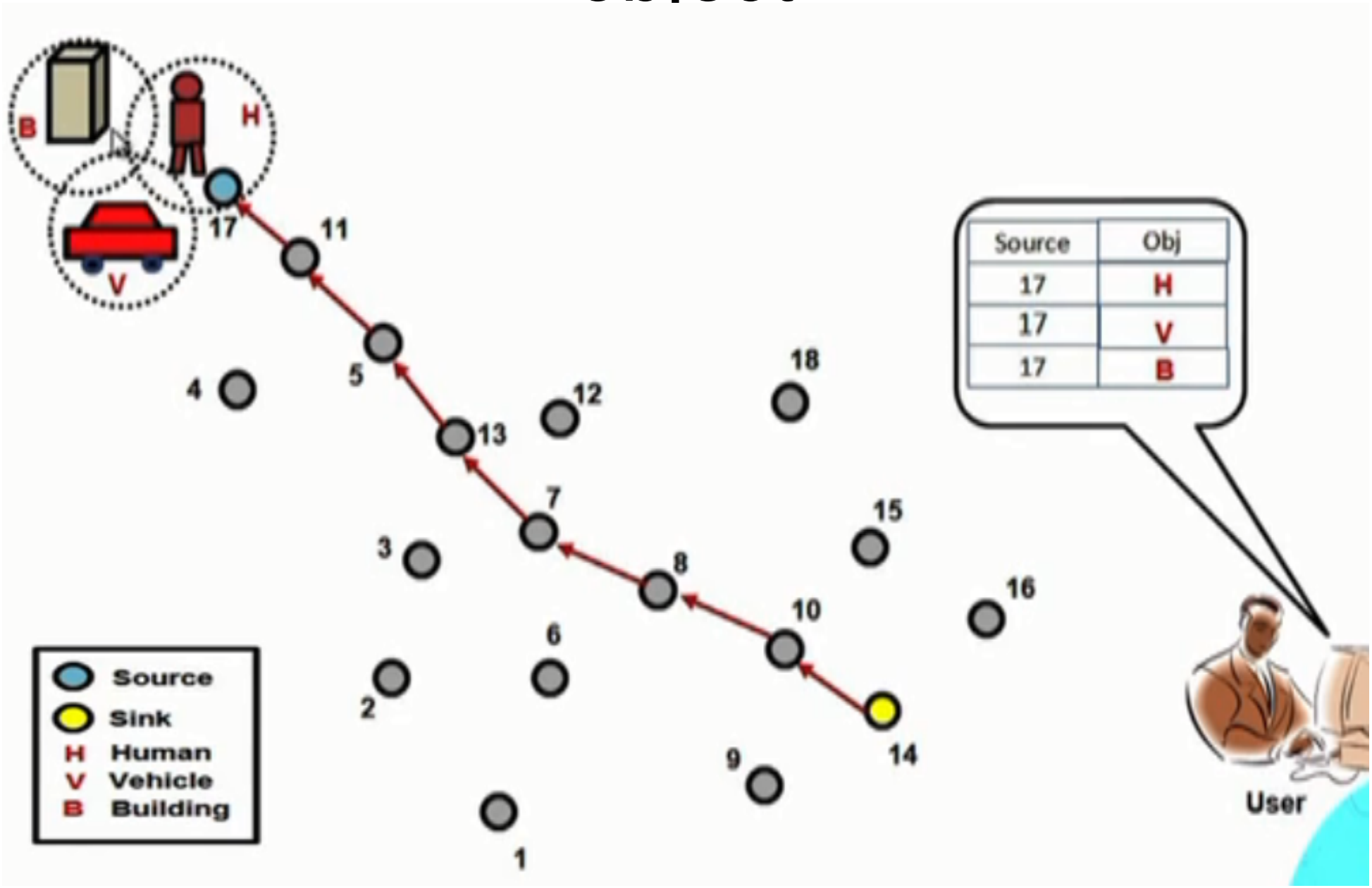
- Multifunctional: The number of sensor node used depends on the application type.
- Short transmission range.
- Have OS(e.g. Tiny O.S)
- Battery Powered Have limited life.

- **sources** of data – the actual nodes that sense data
- **sinks** – nodes where the data should be delivered to.

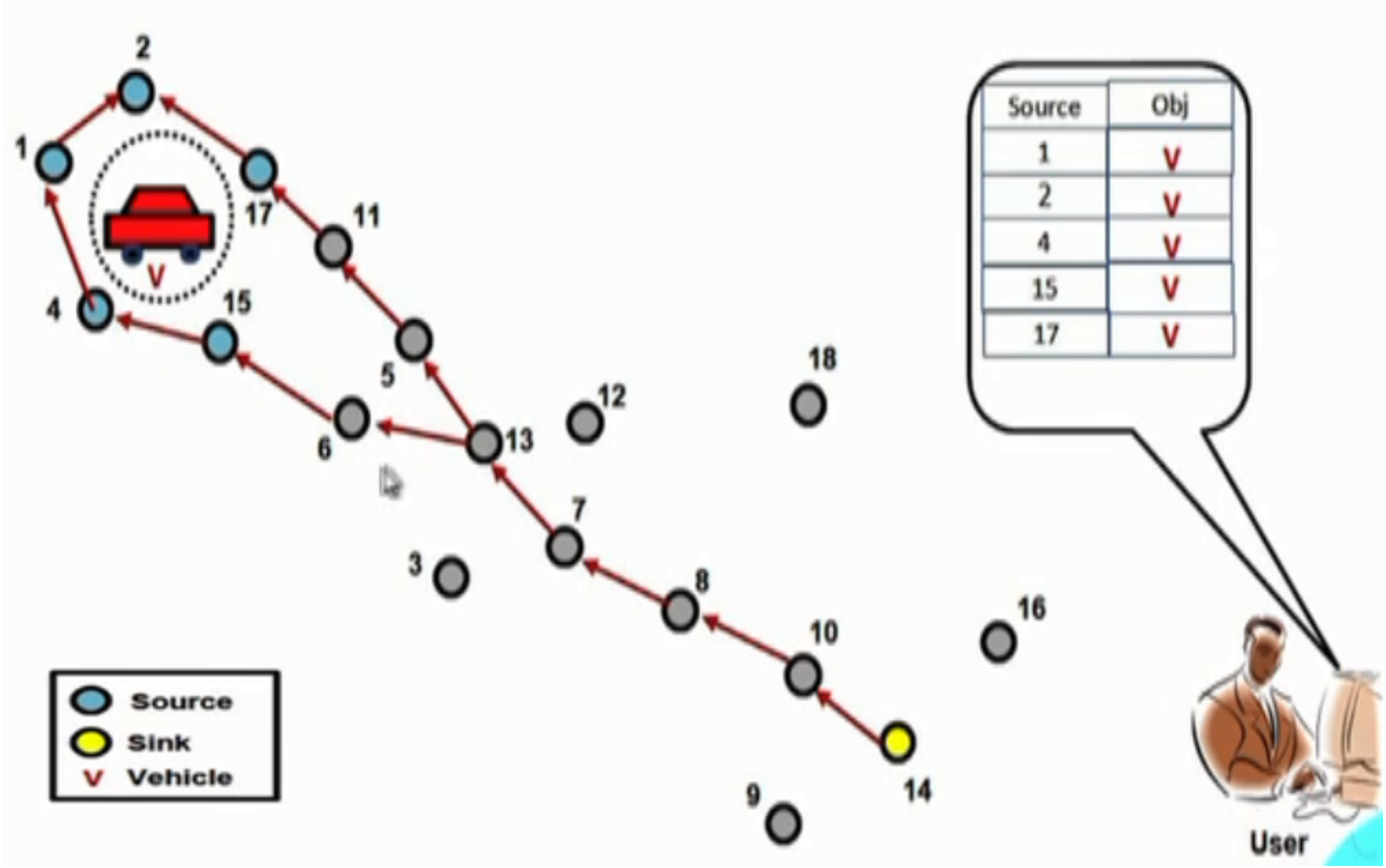
Single Source detects single object



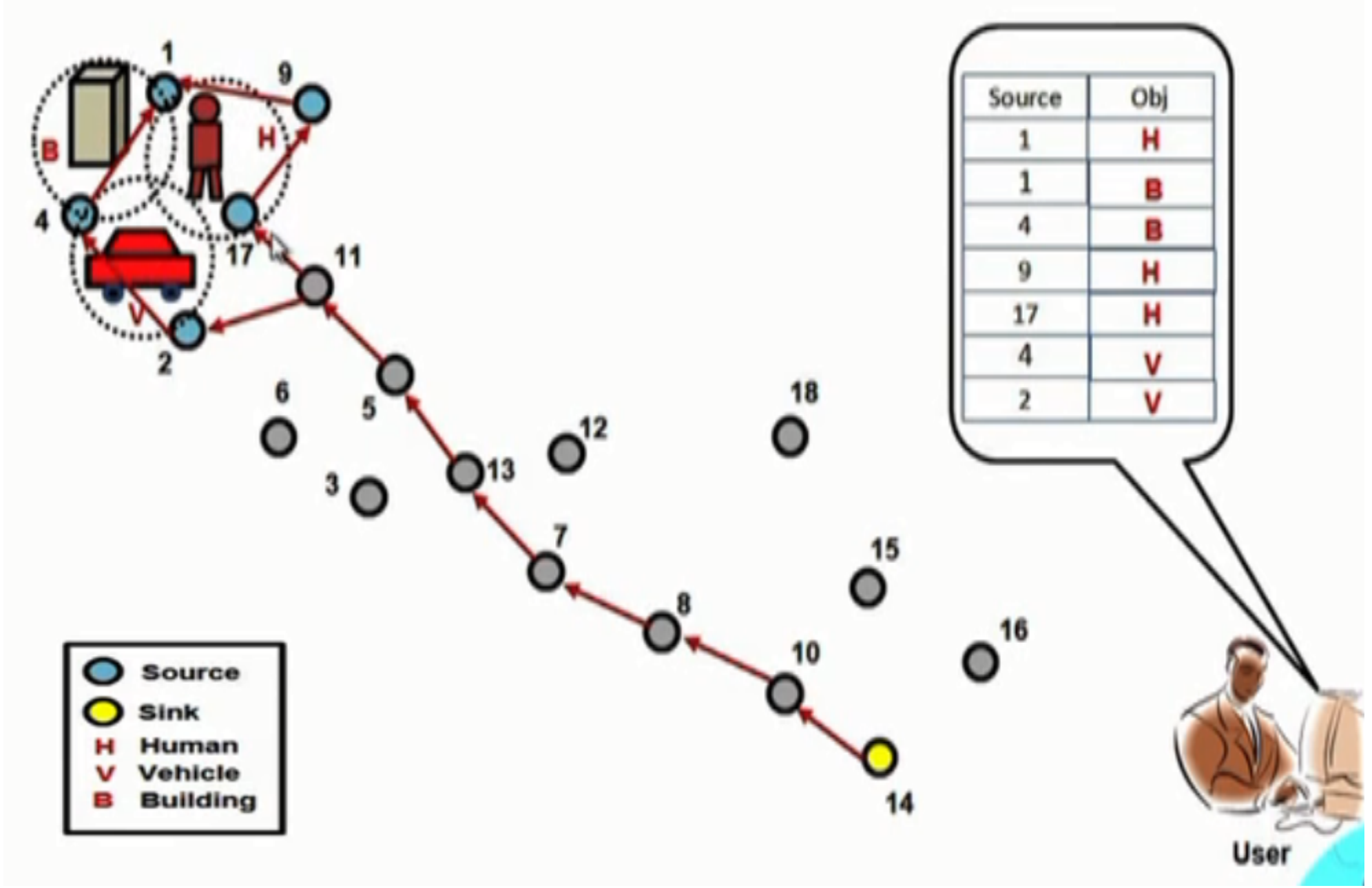
Single source detects multiple object



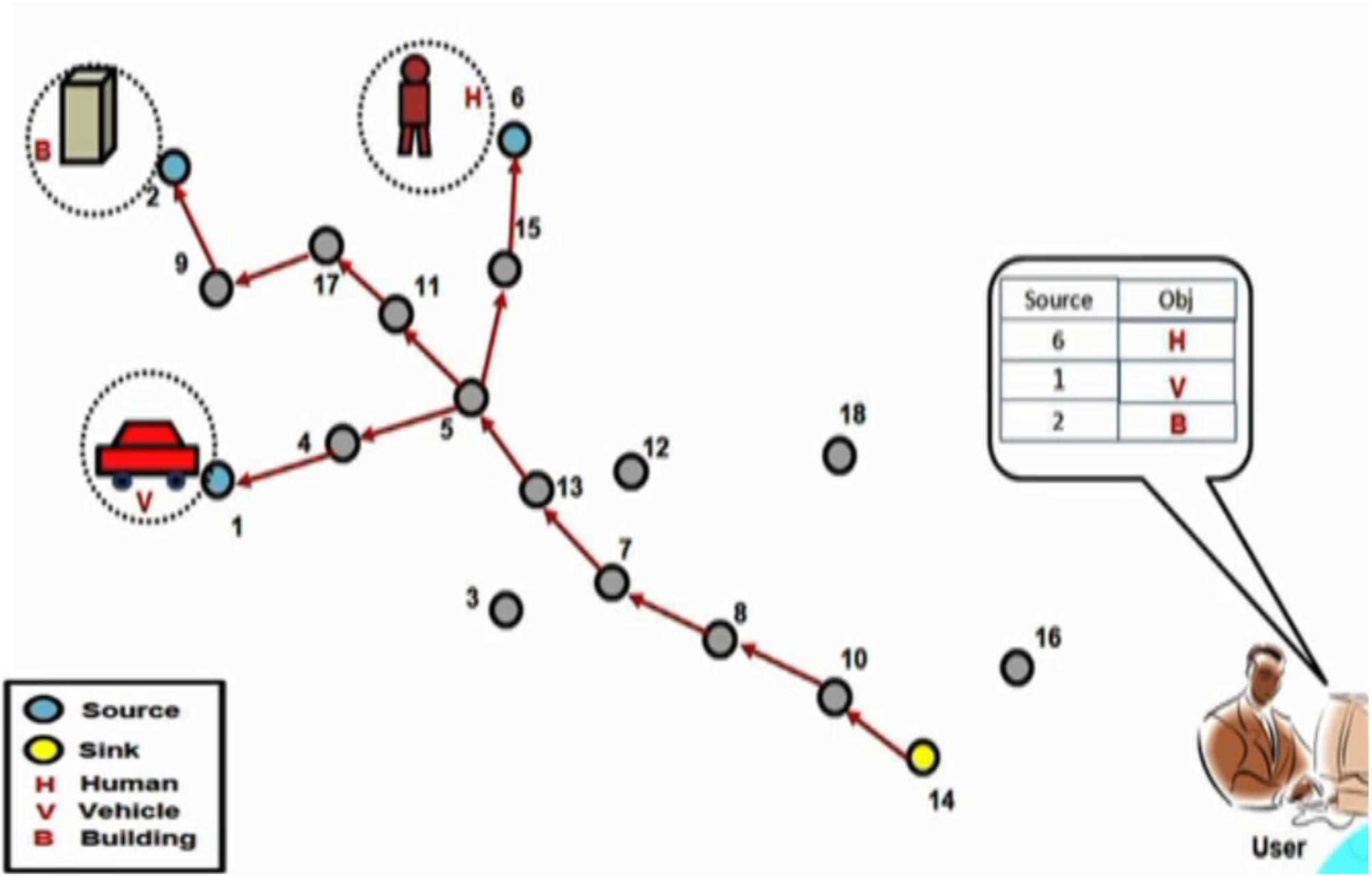
Multiple Sources Detecting Single Object



Multiple Sources detects Multiple Objects



Multiple Sources detects Multiple Objects



Constrains on the Sensor Node

- Small size typically less than a cubic cm.
- Must consume extremely low power.
- Operate in unattended manner in a highly dense area.
- Be adaptive to environment.
- Memory Limitation: Memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data and intermediate results of computations

Common Challenges

- Scalability
  1) Providing acceptable levels of service in presence of large number of nodes.
  2) Typically, throughput decreases at a rate of 1/ /N where N is number of nodes.
- Quality of service:

Offering guarantees in terms of bandwidth, delay, jitter, packet loss probability.

- Energy efficiency
  1) Nodes have limited battery power.
  2) Nodes need to cooperate with other nodes for relaying their information.

- **Maintainability:** As both the environment of a WSN and the WSN itself change (depleted batteries,failing nodes, new tasks), the system has to adapt. It has to monitor its own health and status
- **Programmability**

nodes should be programmable, and their programming must be changeable during operation when new tasks become important.

- **Wide range of densities**

In a WSN, the number of nodes per unit area – the *density* of the network – can vary considerably

Advantages of WSN over wired network

- Ease of deployment: wireless sensors can be deployed at the site of interest without any prior organization, thus reducing the installation cost and time, and also increasing the flexibility of deployment.
- Extended range: One huge wired sensor (macro-sensor) can be replaced by many smaller wireless sensors for the same cost.
- Fault tolerant: With macro-sensors, the failure of one node makes that area completely unmonitored till it is replaced. With wireless sensors, failure of one node does not affect the network operation substantially as there are other adjacent nodes collecting similar data.
- Mobility: Since these wireless sensors are equipped with battery, they can possess limited mobility (e.g., if placed on robots).

Ideal Sensor Network Features

- Attribute based addressing: in sensor networks where addresses are composed of a group of attribute-value pairs which specify certain physical parameters to be sensed. For example, an attribute address may be (temperature > 35°C, location = “Dadar"). So, all sensor nodes located in “Dadar" which sense a temperature greater than 35°C should respond;
- Location awareness: Since most data collection is based on location, it is desirable that the nodes know their position whenever needed
- Time-critical application: the sensors should react immediately to drastic changes in their environment, for example, in *time-critical applications.*
- Query handling: Users should be able to request data from the network through some base station (also known as sink) or through any of the nodes, whichever is closer.

Types of applications

- Event detection
- Periodic measurements
- Function approximation:
- Tracking.

- Temperature Measurement
- Humidity level
- Lighting Condition
- Air Pressure
- Soil makeup
- Noise level
- vibration
- Agriculture
- Healthcare

WSN Applications

- Forest Fire detection
- Air Pollution monitoring
- Water quality monitoring
- Land Slide Detection
- Military application

Forest Fire detection

- A network of Sensor Nodes can be installed in a forest to detect when a fire has started.
- The nodes can be equipped with sensors to measure temperature , humidity and gases which are produced by fire in the trees or vegetation.
- If the node detects fire, it sends an alarm message (along with its l
station.

Air Pollution monitoring

- Traditional air quality monitoring methods, such as building air quality monitoring stations are typically expensive.
- The Solution to these is air quality monitoring system based on the technology of wireless sensor networks.
- Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens.

Water quality monitoring

- Water quality monitoring involves analyzing water properties in dams, river, lakes and oceans as well as underground water reserves.
- Parameters considered include – temperature, turbidity and pH.

Land Slide Detection

- A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide.
- Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.

Military Surveillance

- Enemy tracking , battlefield surveillance
- Target detection
- Monitoring, tracking and surveillance of borders
- Nuclear ,biological and chemical attack detection.

MANET(Mobile Ad hoc Networks)

- Mobile ad hoc networks are formed dynamically by an autonomous system of mobile node that are connected via wireless links.
- No existing fixed infrastructure or centralized administration-No base station.
- Mobile nodes are free to move randomly.

(Network topology changes frequently.)

May operate as standalone fashion or also can be connected to the larger internet.

Each node work as router.

- ad hoc networks are basically peer-to-peer multi-hop mobile wireless networks where information packets are transmitted in a store-and-forward manner from a source to an arbitrary destination, via intermediate nodes as shown in Figure.

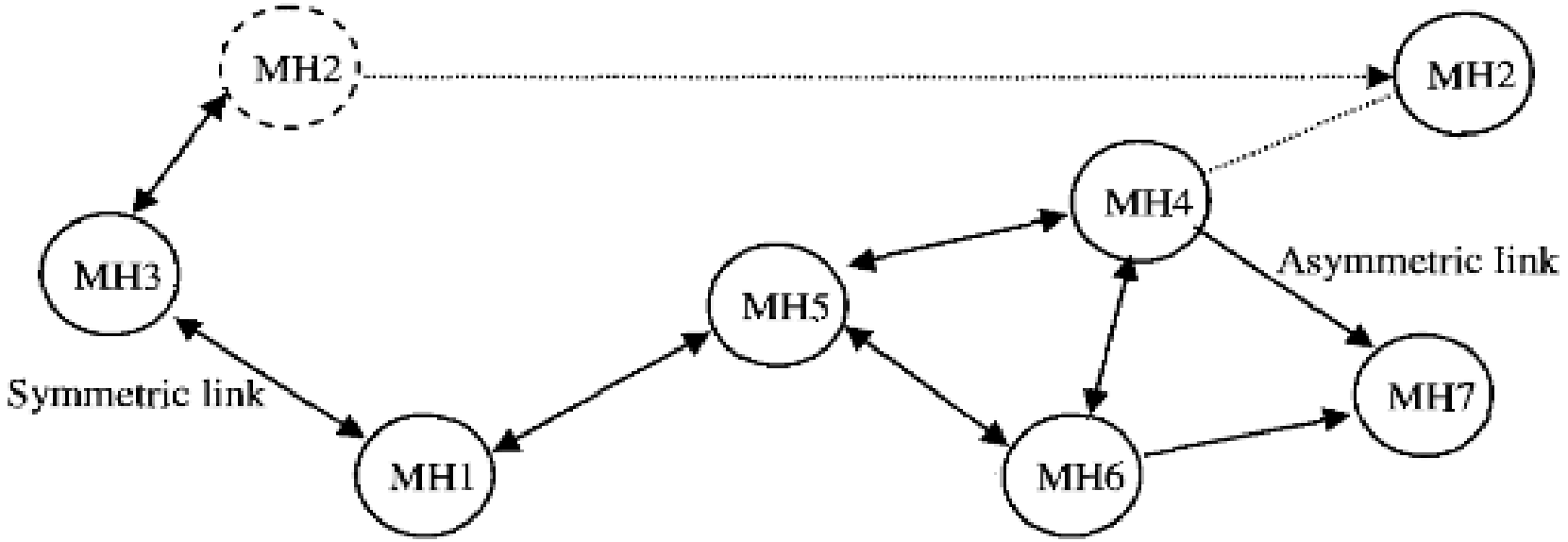


Figure 1.1 – A mobile ad hoc network (MANET)

Applications

) Tactical Networks

military communication, automated battlefields

2) Emergency Services

search and rescue operations, Disaster recovery- Earthquakes, hurricanes.

3) Educational

virtual classrooms or conference rooms.

set up ad hoc communication during conferences, meeting or lectures.

4) Home and Entertainment

Home/Office wireless networking, Personal Area network, Multiuser games, outdoor internet access.

Challenges

- Infrastructure less

Brings new network designing challenges.

- Dynamically changing topologies

Cause route changes, frequent network partitions and packet loss.

- Physical layer limitations

Limited wireless range, packet loss during transmission, Broadcast nature of communication.

- Limitation of mobile nodes

Short battery life, limited capacities

Enabling technologies for wireless sensor networks

- Building such wireless sensor networks has only become possible with some fundamental advances in enabling technologies.
- 1) miniaturization of hardware: Reduced chip

size and improved energy efficiency is accompanied by reduced cost.

2) processing and communication

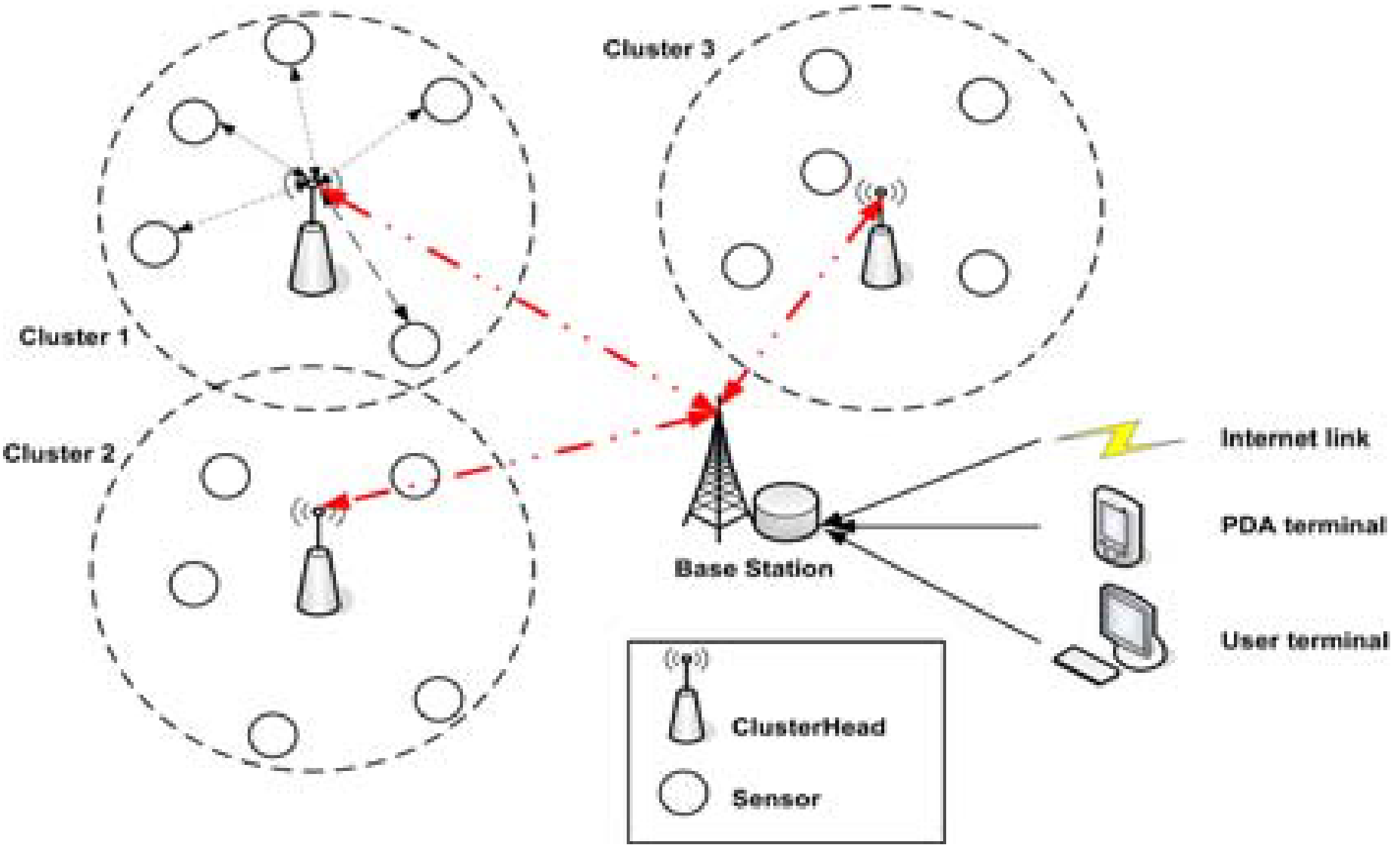
3) actual sensing equipment

Clustering of SNs

- WSN base station always needs to generate an aggregated value to the end users and the aggregation of the data to be forwarded can also help in reducing the transmission overhead and the energy consumption.
- To support the data aggregation in the network the nodes can be accommodated in the small groups called the Clusters.
- Clustering can be defined as the division of the nodes in the groups on the basis of some mechanism.
- Clustering has been shown to improve network lifetime, a primary metric for evaluating the performance of a sensor network.
- Clustering is done to achieve the energy efficiency and the scalability of the network.

- Formation of the cluster also involves the assigning the role to the node on the basis of their perimeters.
- The coordinator of the cluster which is responsible for the processing, aggregation and transmission of the data to the base station is called the Cluster Head (CH) or the leader, whereas the other nodes which are responsible for sensing and forwarding the collected data to the CH are called the Member Nodes.

- Figure represents the basis hierarchy of Clustering:



- In clustering the 2 tier hierarchy is adopted where in first phase the member nodes sense the data and forward to the CH and in second phase the CH aggregates and process the data to deliver it to the Base Station.
- The CH node looses more energy as compared to the MN because it performs the fusion on the entire collected data and sends that aggregated report to the BS located far from the cluster location.
- In a cluster organization both the Intra-cluster and the Inter cluster communication takes place.

- Clustering in WSNs involves grouping nodes into clusters and electing a CH such that:

1) The members of a cluster can communicate with their CH directly.

2) A CH can forward the aggregated data to the central base Station through other CHs

- ***A. Perimeters of the clustering***

 Cluster count/Number of clusters

 Cluster size uniformity

 Inter-clustering routing

 Intra-clustering routing

- **Cluster count:** On the basis of cluster count the network can be divided into two categories: fixed and variable. Fixed cluster count is that in which the number of clusters in the network are fixed whereas in variable sizes network the number of clusters is not fixed.
- **Cluster size uniformity:** Cluster size uniformity deals with the size of cluster. It is of two types: Even and Odd. In even cluster size the number of nodes is same in all the clusters of the network and in odd uniformity the cluster size is different.

- **Inter-cluster Routing:** Inter-cluster routing describes the communication mode of the different cluster. It can be of two types: Single hop and multi hop. Single hop is that type in which the CH communicates with the BS directly. In multi hop clustering the CH communicates with the BS through various intermediate CHs.
- **Intra-cluster Routing:** It describes the mode of communication between the member nodes and the CH. It can be of two types: single hop and multi hop. In single hop the MN directly deal with the CH whereas in the multi hop the MN don’t directly deal with the CH.

Advantages of Clustering

- Scalability: As the node is divided into various assignment levels, it makes it easy to add new nodes to the cluster.
- Data aggregation: Data aggregation helps in reducing the redundant data collected from member nodes.
- Less load: Aggregated data avoids the load of the transmission of data from CH to the BS.
- Reduced energy consumption: the energy is used less when only non redundant and aggregated data is to be transferred.
- Collision Avoidance: By dividing the resources orthogonally to each cluster can leads to a collision free data transmission.
- Load Balancing: Equal sized cluster adapt the prolonging of network by balancing the load and prevents from premature energy exhaustion.
- Fault tolerance: Whenever a node suffers from energy depletion the reclustering can be done.
- QoS: Clustering protocol helps in delivering a quality and non redundant data to the end user.

Sensor Node Hardware and Network Architecture

- **Controller** A controller to process all the relevant data, capable of executing arbitrary code.
- **Memory** Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.
- **Sensors and actuators** The actual interface to the physical world: devices that can observe or control physical parameters of the environment.
- **Communication** Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

Hardware Components

- A basic sensor node comprises five main components

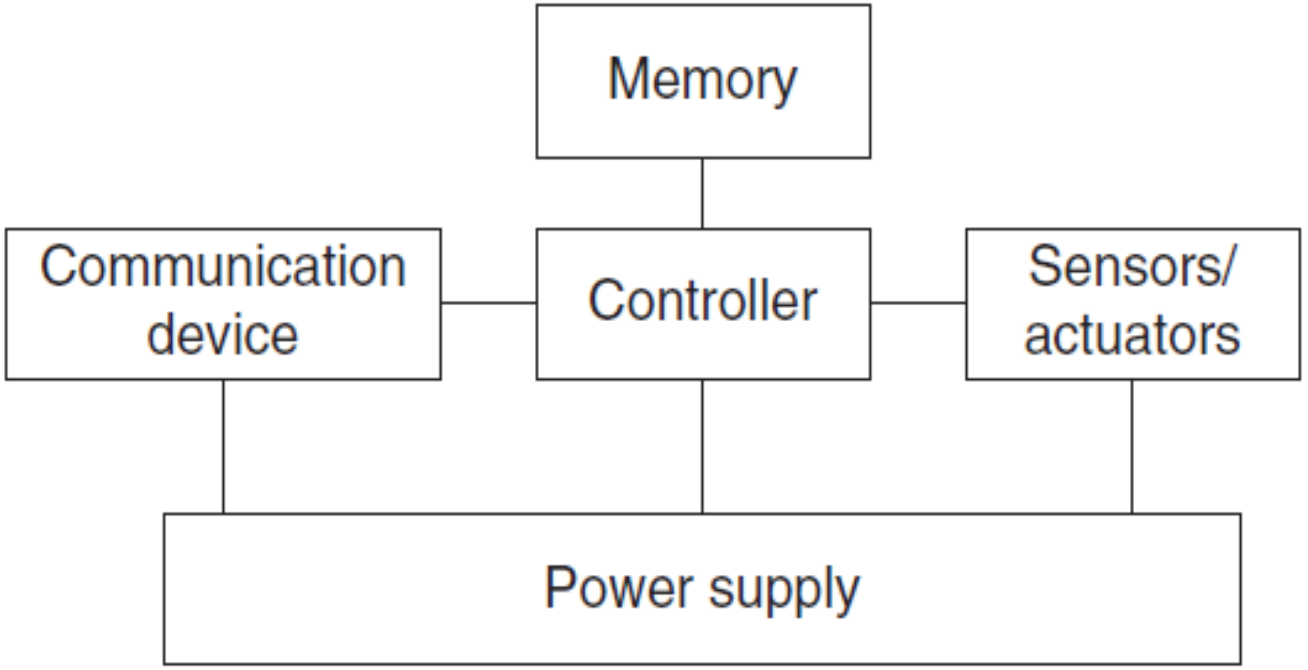


Figure 2.1 Overview of main sensor node hardware components

Controller

- The Controller is the core of wireless sensor node.
- It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes, and decides on the actuator’s behavior.
- It has to execute various programs, ranging from time-critical signal processing and communication protocols to application programs; it is the Central Processing Unit (CPU) of the node.

general-purpose processors

- known from desktop computers
- highly overpowered, and their energy consumption is excessive

Microcontrollers

- flexibility in connecting with other devices(like sensors)
- instruction set responsible to time-critical signal processing.
- low power consumption
- Have memory built in
- freely programmable and hence very flexible
- reduce their power consumption by going into **sleep states** where only parts of the controller are active.

Some examples for microcontrollers

- Microcontrollers that are used in several wireless sensor node

1)Intel StrongARM

2) Texas Instruments MSP 430

3) Atmel ATmega

Memory

- there is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on.
- While RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted.
- Program code can be stored in Read-Only Memory (ROM) or, more typically, in Electrically Erasable Programmable Read-Only Memory (EEPROM) or flash memory.
- Flash memory can also serve as intermediate storage of data in case RAM is insufficient or when the power supply of RAM should be shut down for some time.

Communication device

Choice of transmission medium: The communication device is used to exchange data between individual nodes.

- The usual choices of the transmission medium in wireless communication include radio frequencies, optical communication, and ultrasound;
- Radio Frequency (RF)-based communication is by far the most relevant one as it best fits the requirements of most WSN applications:
- It provides relatively long range and high data rates, acceptable error rates at reasonable energy expenditure, and does not require line of sight between sender and receiver.
- wireless sensor networks typically use communication frequencies between about 433 MHz and 2.4 GHz.

Transceivers

- For actual communication, both a transmitter and a receiver are required in a sensor node.
- The essential task is to convert a bit stream coming from a microcontroller (or a sequence of bytes or frames) and convert them to and from radio waves.
- For practical purposes, it is usually convenient to use a device that combines these two tasks in a single entity. Such combined devices are called **transceivers**.
- Usually, half-duplex operation since transmitting and receiving at the same time on a wireless medium is impractical in most cases.

Sensors and actuators

- Sensors can be roughly categorized into three categories
- 1) **Passive, omnidirectional sensors**
- 2) **Passive, narrow-beam sensors**
- 3) **Active sensors**

Passive, omnidirectional sensors

- These sensors can measure a physical quantity at the point of the sensor node without actually manipulating the environment by active probing – in this sense, they are passive.
- some of these sensors actually are self-powered in the sense that they obtain the energy they need from the environment.
- There is no notion of “direction” involved in these measurements.
- Typical examples for such sensors include thermometer, light sensors, vibration, smoke detectors, air pressure.

Passive, narrow-beam sensors

- These sensor have well-defined notion of direction of measurements.
- A typical example is a camera, which can “take measurements” in a given direction, but has to be rotated if needed.

Active sensors

- These sensors actively probes the environment, for example, a sonar or radar sensor or some types of seismic sensors, which generate shock waves by small explosions.

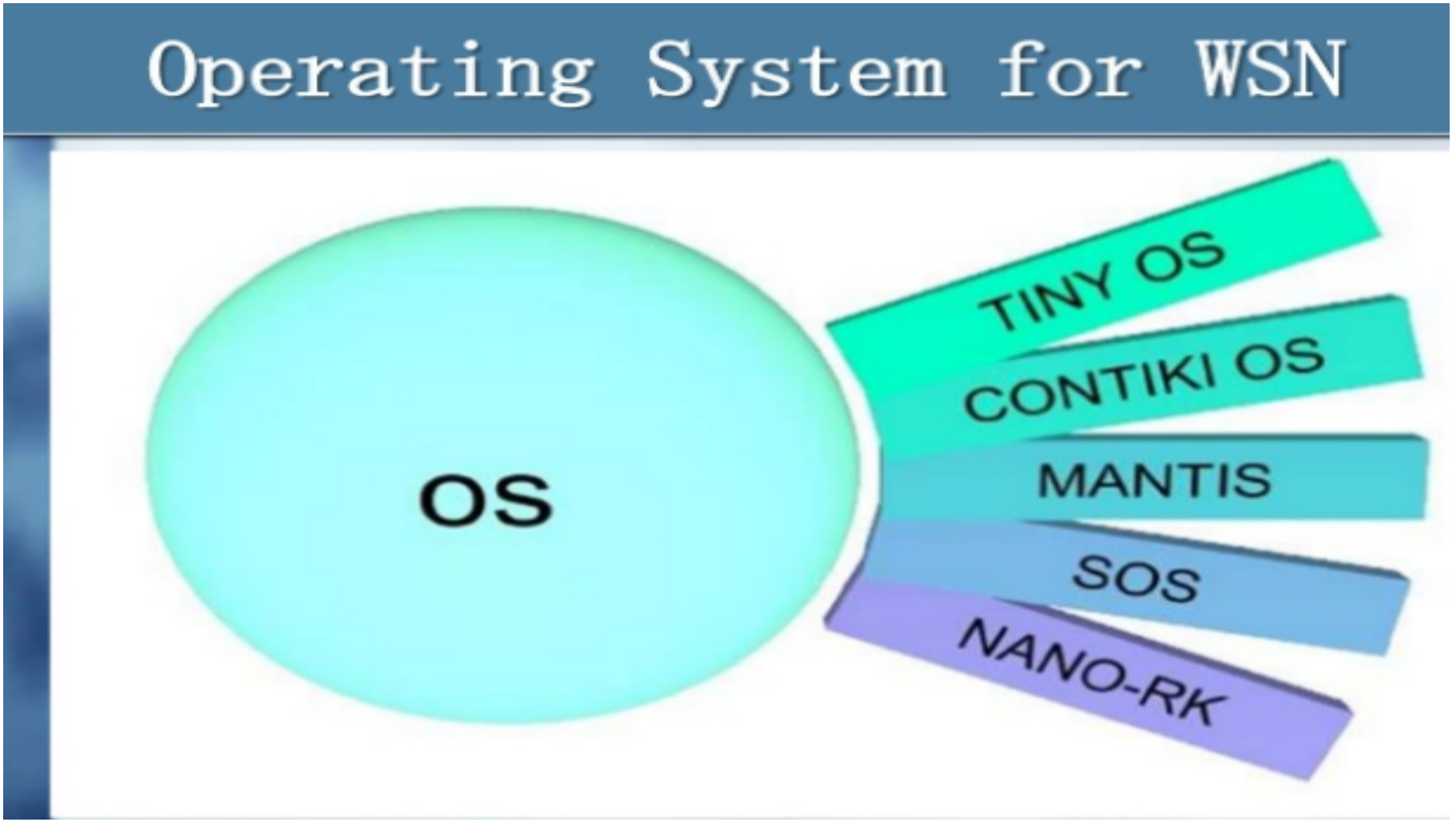
Power supply of sensor nodes

- There are essentially two aspects:

1) storing energy and providing power in the required form(Traditional batteries)
2) replenish consumed energy by “scavenging”

(the process by which energy is derived from external sources (e.g., solar power, thermal energy, wind energy, salinity gradients, and kinetic energy, also known as ambient energy))

Operating systems and execution environments



Tiny OS and NesC

- Tiny OS is free open source operating system.
- Designed for wireless sensor networks.
- Tiny OS having BSD license.
- Developed at UC, Berkeley.
- Support NesC programming language.

Why do we need Tiny OS?

- Lower Power
- Limited memory
- Slow CPU
- Size Small
- Communication using Radio
- Short Range

- Huge
- Multi threaded architecture(large memory)
- Typically no energy constraint.

Tiny OS Solution

- Support Concurrency: Event driven architecture.
- Software modularity(Component based model): A components contains commands, event handlers, internal storage and tasks.

  Task are non-preemptive and run in FIFO order.
- Efficiency: get done quickly and then sleep
- Static Memory allocation

Optimization goals and figures of merit

- Quality of service
- Energy efficiency
- Scalability
- Robustness

Quality of service

- QoS attributes in WSN highly depend on the application. Some generic possibilities are:
- 1) **Event detection/reporting probability:** What is the probability that an event that actually occurred is not detected or, more precisely, not reported to an information sink that is interested in such an event? For example, not reporting a fire alarm to a surveillance station would be a severe shortcoming.
- **2) Event classification error:** If events are not only to be detected but also to be classified, the error in classification must be small.
- **3) Event detection delay:** What is the delay between detecting an event and reporting it to any/all interested sinks?

- **4) Missing reports:** In applications that require periodic reporting, the probability of undelivered reports should be small.
- **5) Approximation accuracy:** For function approximation applications, what is the average/maximum absolute or relative error with respect to the actual function?
- **6) Tracking accuracy:** Tracking applications must not miss an object to be tracked, the reported position should be as close to the real position as possible, and the error should be small.

Energy efficiency

- The most commonly considered aspects are:
- 1) **Energy per correctly received bit:** How much energy, counting all sources of energy consumption at all possible intermediate hops, is spent on average to transport one bit of information (payload) from the source to the destination? This is often a useful metric for periodic monitoring applications.
- **2) Energy per reported (unique) event:** Similarly, what is the average energy spent to report one event? Since the same event is sometimes reported from various sources, it is usual to normalize this metric to only the unique events.
- **3) Delay/energy trade-offs:** Some applications have a notion of “urgent” events, which can justifyan increased energy investment for a speedy reporting of such events.

- **4) Network lifetime:** The time for which the network is operational or, put another way, the time during which it is able to fulfill its tasks.

Possible definitions are:

- **Time to first node death** When does the first node in the network run out of energy or fail and stop operating?
- **Network half-life** When have 50% of the nodes run out of energy and stopped operating?
- **Time to partition** When does the first partition of the network in two (or more) disconnected parts occur?

Scalability

- The ability to maintain performance characteristics irrespective of the size of the network is referred to as scalability

Robustness

- Related to QoS and somewhat also to scalability requirements, wireless sensor networks should also exhibit an appropriate robustness. They should not fail just because a limited number of nodes run out of energy, or because their environment changes and severs existing radio links between two nodes – if possible, these failures have to be compensated for, for example, by finding other routes.

Design Principles of WSN

Distributed organization

- The disadvantages of a centralized approach are obvious as it introduces exposed points of failure and is difficult to implement in a radio network, where participants only have a limited communication range.
- Rather, the WSNs nodes should cooperatively organize the network, using distributed algorithms and protocols.

In-network processing

- When organizing a network in a distributed fashion, the nodes in the network are not only passing on packets or executing application programs, they are also actively involved in taking decisions about how to operate the network.
- This is a specific form of information processing that happens in the network, but is limited to information about the network itself.

- Several techniques for in-network processing exist
- **Aggregation:** The name **aggregation** stems from the fact that in nodes intermediate between sources and sinks, information is aggregated into a condensed form out of information provided by nodes further away from the sink.
- aggregation function to be applied in the intermediate nodes must satisfy some conditions for the result to be meaningful; most importantly, this function should be **composable**.

- Figure 3.7 illustrates the idea of aggregation. In the left half, a number of sensors transmit readings to a sink, using multihop communication. In total, 13 messages are required (the numbers in the figure indicate the number of messages traveling across a given link).
- When the highlighted nodes perform aggregation – for example, by computing average values (shown in the right half of the figure) – only 6 messages are necessary.

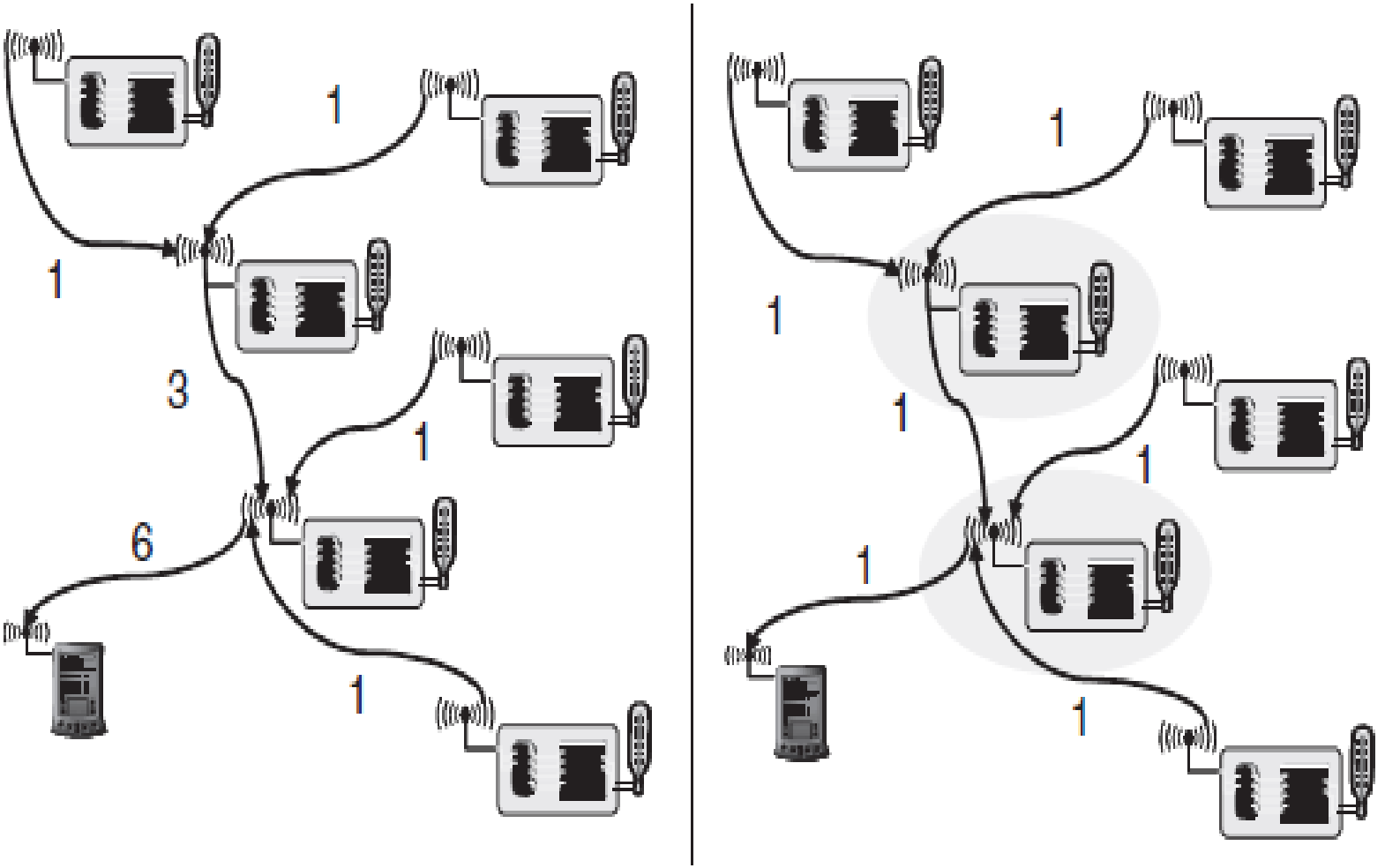


Figure 3.7 Aggregation example

Data centricity

- **Address data, not nodes**
- In traditional communication networks, the focus of a communication relationship is usually the pair of communicating peers – the sender and the receiver of data.
- In a wireless sensor network, on the other hand, the interest of an application is not so much in the *identity* of a particular sensor node, it is much rather in the actual information reported about the physical environment.
- it is of no concern to the application precisely which of these nodes is providing data.
- The Network in which data are at the center of attention is called **data-centric networking**.

Exploit location information

- Another useful technique is to exploit location information in the communication protocols whenever such information is present.
- Since the location of an event is a crucial information for many applications, there have to be mechanisms that determine the location of sensor nodes.

Exploit activity patterns

- Once an event has happened, it can be detected by a larger number of sensors, breaking into a frenzy of activity, causing a well-known event shower effect.
- Hence, the protocol design should be able to handle such bursts of traffic by being able to switch between modes of quiescence and of high activity.

Exploit heterogeneity

- Related to the exploitation of activity patterns is the exploitation of heterogeneity in the network.
- Sensor nodes can be heterogeneous by constructions, that is, some nodes have larger batteries, farther-reaching communication devices, or more processing power.
- They can also be heterogeneous by evolution, that is, all nodes started from an equal state, but because some nodes had to perform more tasks during the operation of the network, they have depleted their energy resources or other nodes had better opportunities to scavenge energy from the environment.

Gateway concepts

- **The need for gateways:**
- a sensor network only concerned with itself is insufficient.
- The network rather has to be able to interact with other information devices, for example, a user equipped with a PDA(Personal digital assistant) moving in the coverage area of the network or with a remote user, trying to interact with the sensor network via the Internet (the standard example is to read the temperature sensors in one's home while traveling and accessing the Internet via a wireless connection). Figure 3.9 shows this networking scenario.

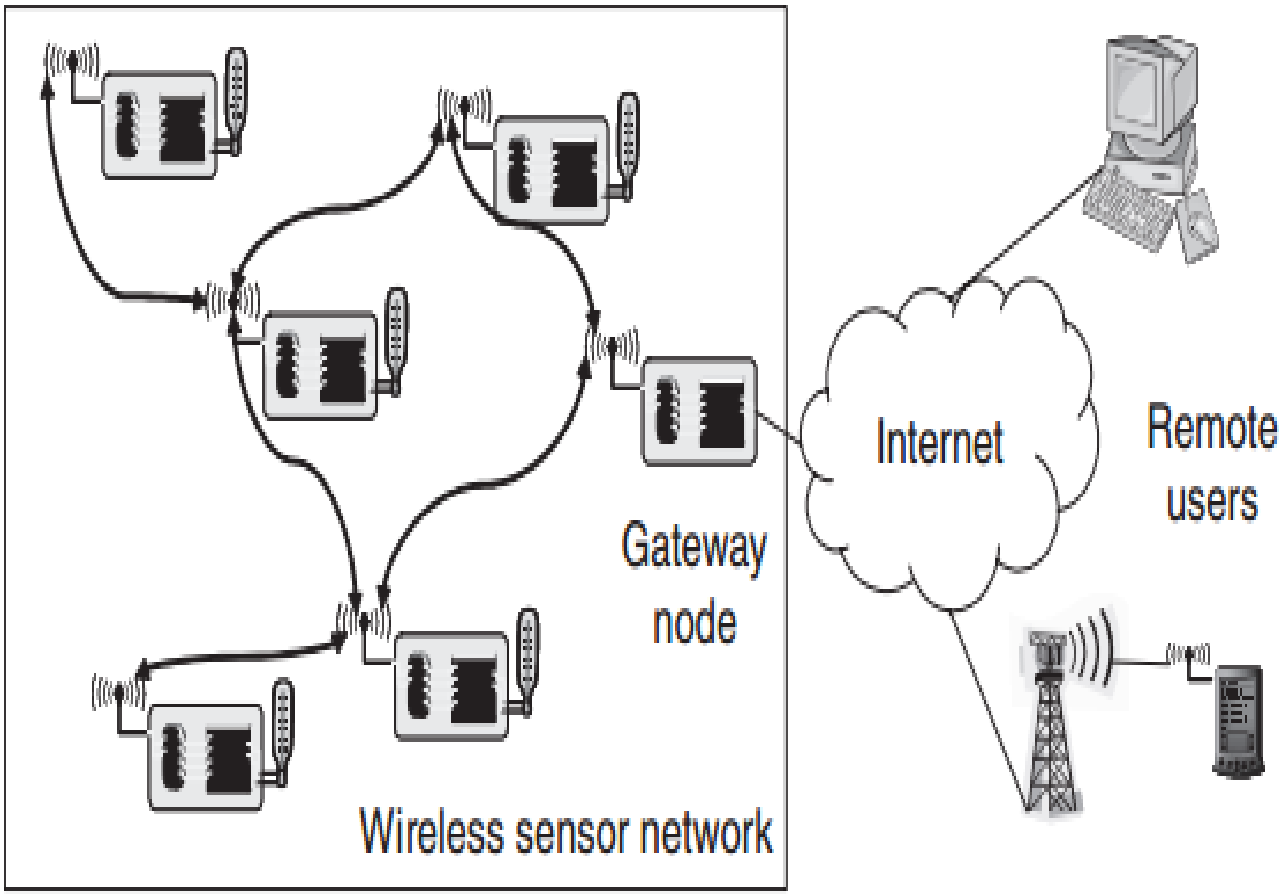


Figure 3.9 A wireless sensor network with gateway node, enabling access to remote clients via the Internet

- To this end, the WSN first of all has to be able to exchange data with such a mobile device or with some sort of gateway, which provides the physical connection to the Internet.
- This is relatively straightforward on the physical, MAC, and link layer – either the mobile device/the gateway is equipped with a radio transceiver as used in the WSN, or some (probably not all) nodes in the WSN support standard wireless communication technologies .

WSN to Internet communication

- If several such gateways are available, how to choose between them? In particular, if not all Internet hosts are reachable via each gateway or at least if some gateway should be preferred for a given destination host? How to handle several gateways, each capable of IP networking, and the communication among them? One option is to build an IP overlay network on top of the sensor network
- How does a sensor node know to which Internet host to address such a message? Or even worse, how to map a semantic notion (“Alert Alice”) to a concrete IP address? Even if the sensor node does not need to be able to process the IP protocol, it has to include sufficient information (IP address and port number, for example) in its own packets; the gateway then has to extract this information and translate it into IP packets. An ensuing question is which source address to use here – the gateway in a sense has to perform tasks similar to that of a Network Address Translation (NAT) device.

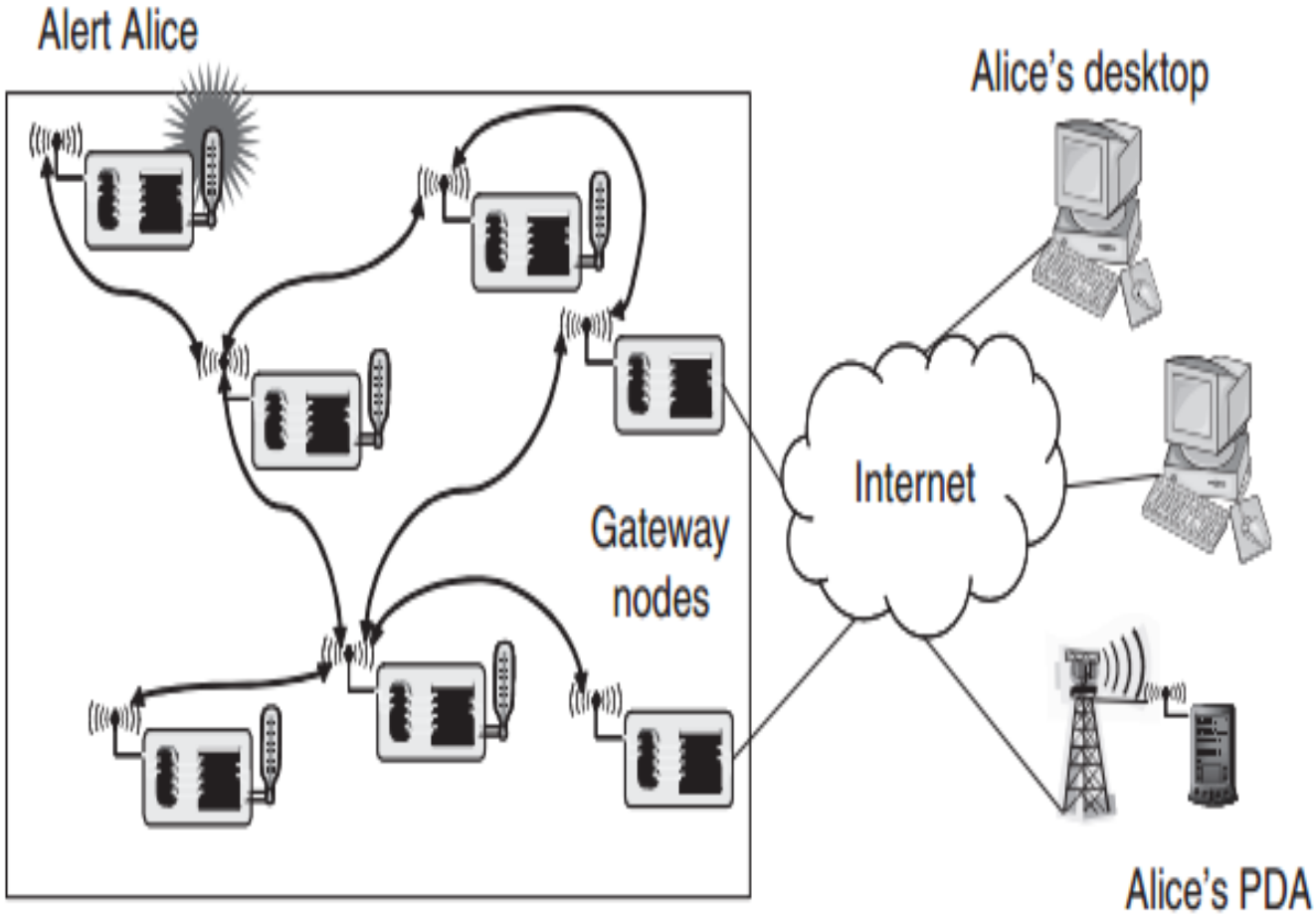


Figure 3.10 An event notification to "Alice" needs decisions about, among others, gateway choice, mapping "Alice" to a concrete IP address, and translating an intra-WSN event notification message to an Internet application message

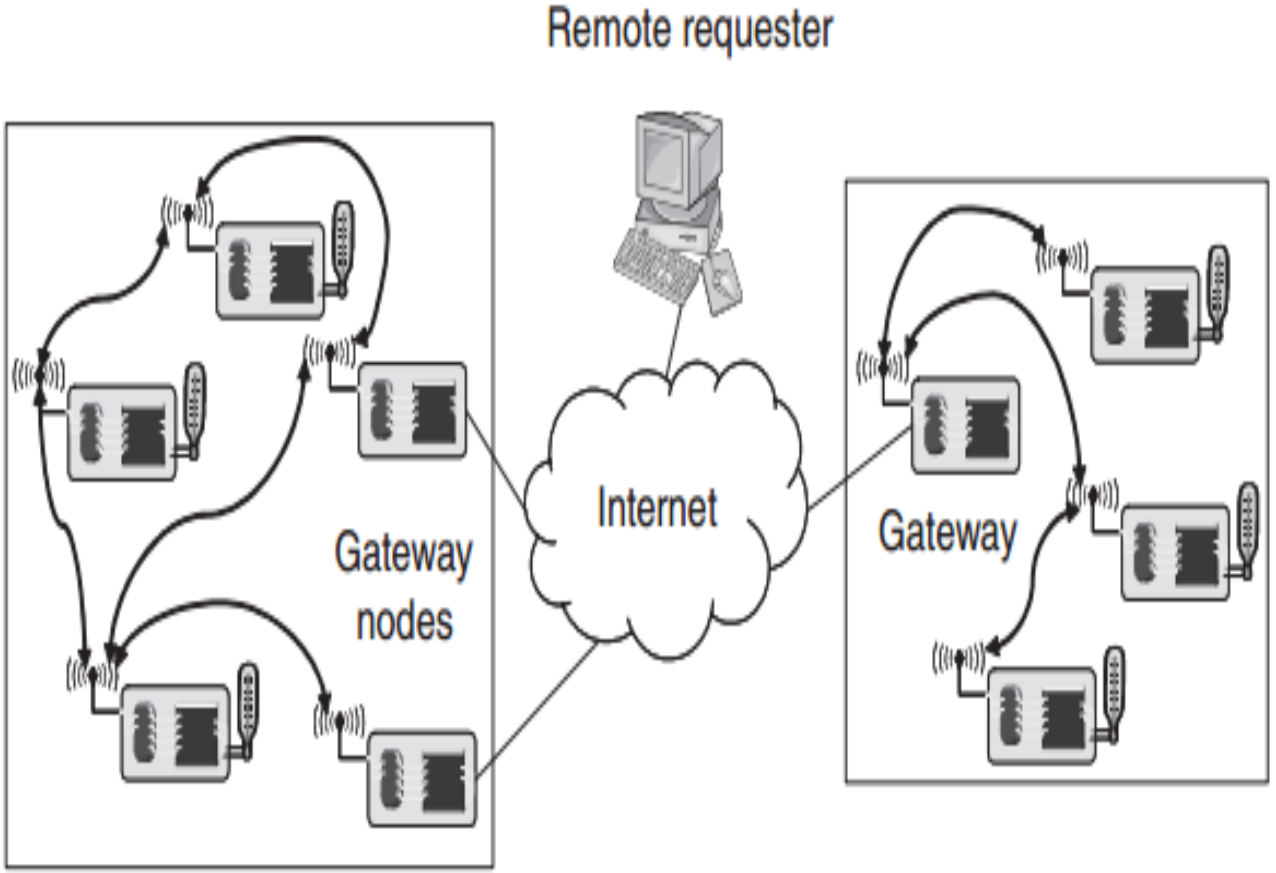


Figure 3.11 Requesting sensor network information from a remote terminal entails choices about which network to address, which gateway node of a given network, and how and where to adapt application-layer protocol in the Internet to WSN-specific protocols

Internet to WSN communication

- The idea is to build a larger, “virtual” WSN out of separate parts, transparently “tunneling” all protocol messages between these two networks and simply using the Internet as a transport network (Figure 3.12) [751].
- This can be attractive, but care has to be taken not to confuse the virtual link between two gateway nodes with a real link; otherwise, protocols that rely on physical properties of a communication link can get quite confused (e.g. time synchronization or localization protocols).
- Such tunnels need not necessarily be in the form of fixed network connections; even mobile nodes carried by people can be considered as means for intermediate interconnection of WSNs.

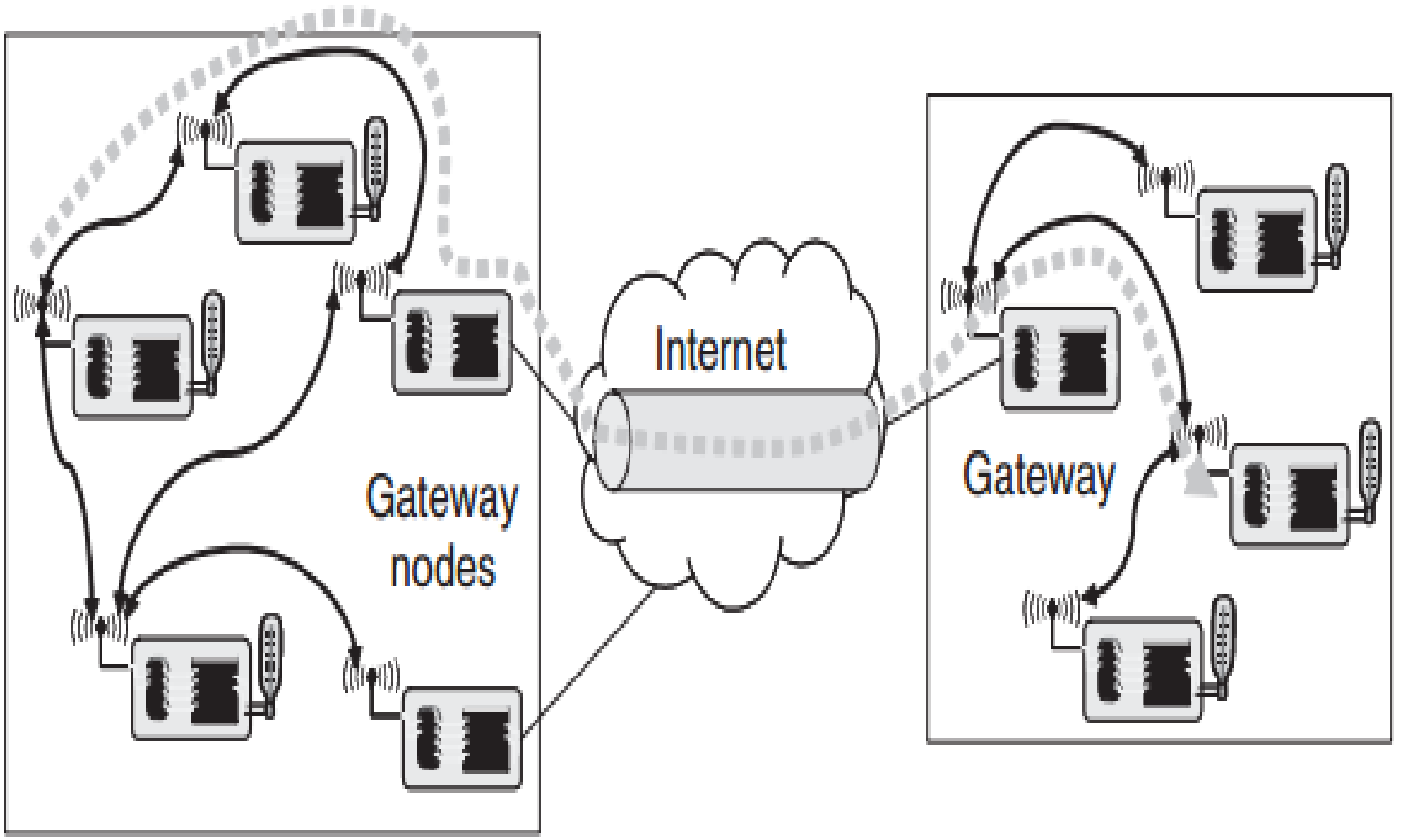


Figure 3.12 Connecting two WSNs with a tunnel over the Internet