CET4004B: Wireless and Mobile Device Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. COMPUTER SCIENCE AND ENGINEERING

CET4004B: Wireless and Mobile Device Security

Teaching Scheme
Theory: 3Hrs. / Week

Credits: 03 + 01 = 04
Practical: 2 Hrs./Week

Course Objectives:

1) Knowledge:

i. To understand wireless networks technologies and applications
ii. To study Ad-Hoc, sensor networks architecture, challenges and applications
iii. To understand basic security needs and issues in wireless networks
iv. To understand mobile device security architecture and security dynamics

2) Skills:

i. This course gives understanding of how to design and configure your own network

3) Attitude:

i. To deploy the network as well as provide various security aspects to the mobile device

Course Outcomes:

i. Compare different wired and wireless technologies
ii. Simulate and analyze wireless Ad-Hoc networks for different protocols
iii. Analyze the security threats in wireless sensor networks
iv. Configure or Program security needs in mobile devices

Module 3
Wireless Sensor Networks

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

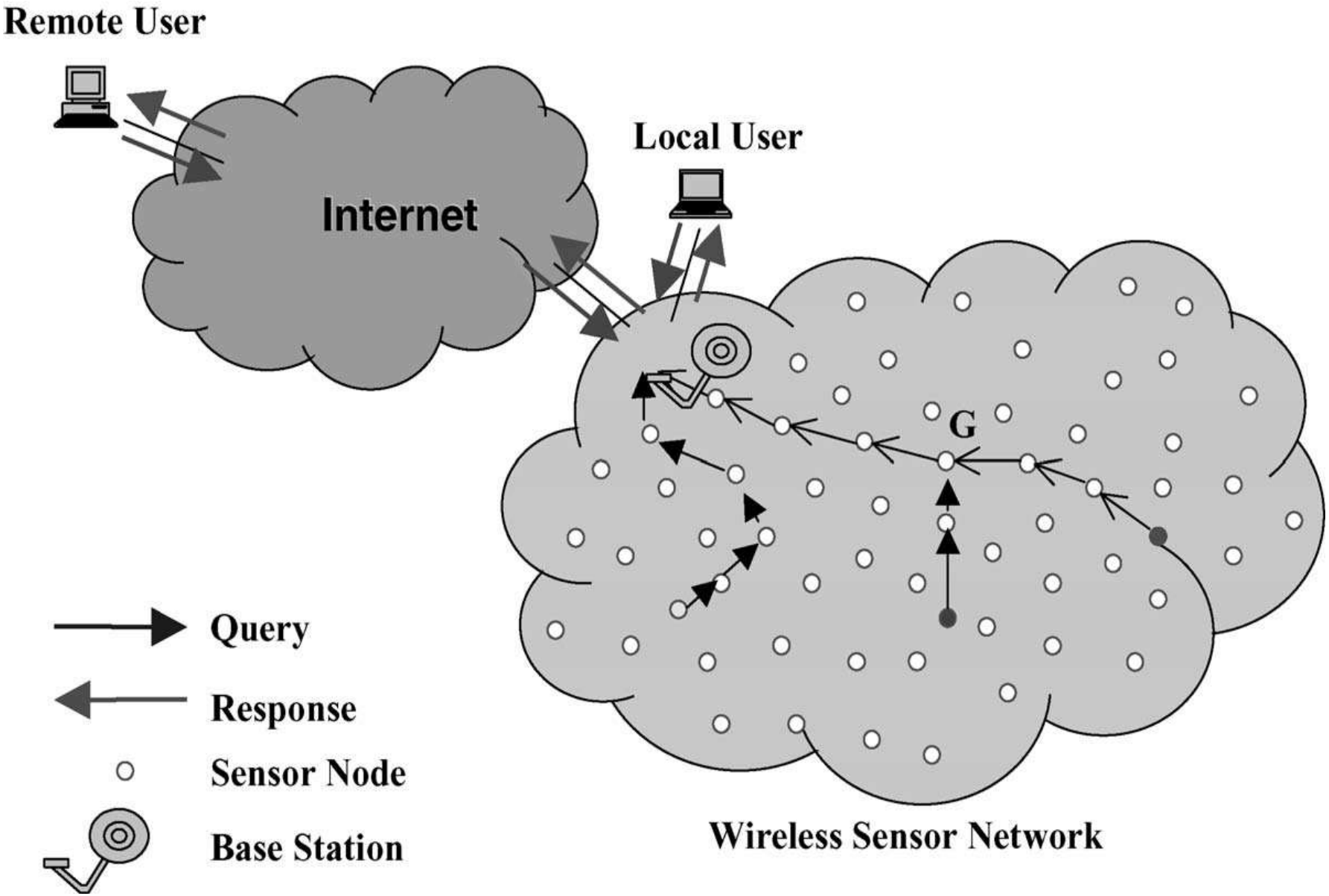
Points to be covered

- Introduction to WSN
- Applications
- Challenges, Design issues in sensor networks
- Architecture of sensor networks: Layered Architecture, Clustered Architecture
- Overview of Data Dissemination techniques
- Introduction to Data Gathering techniques
- Overview of Positioning, Localization and Synchronization in Sensor networks
- LoRa WANs
- RFID technologies

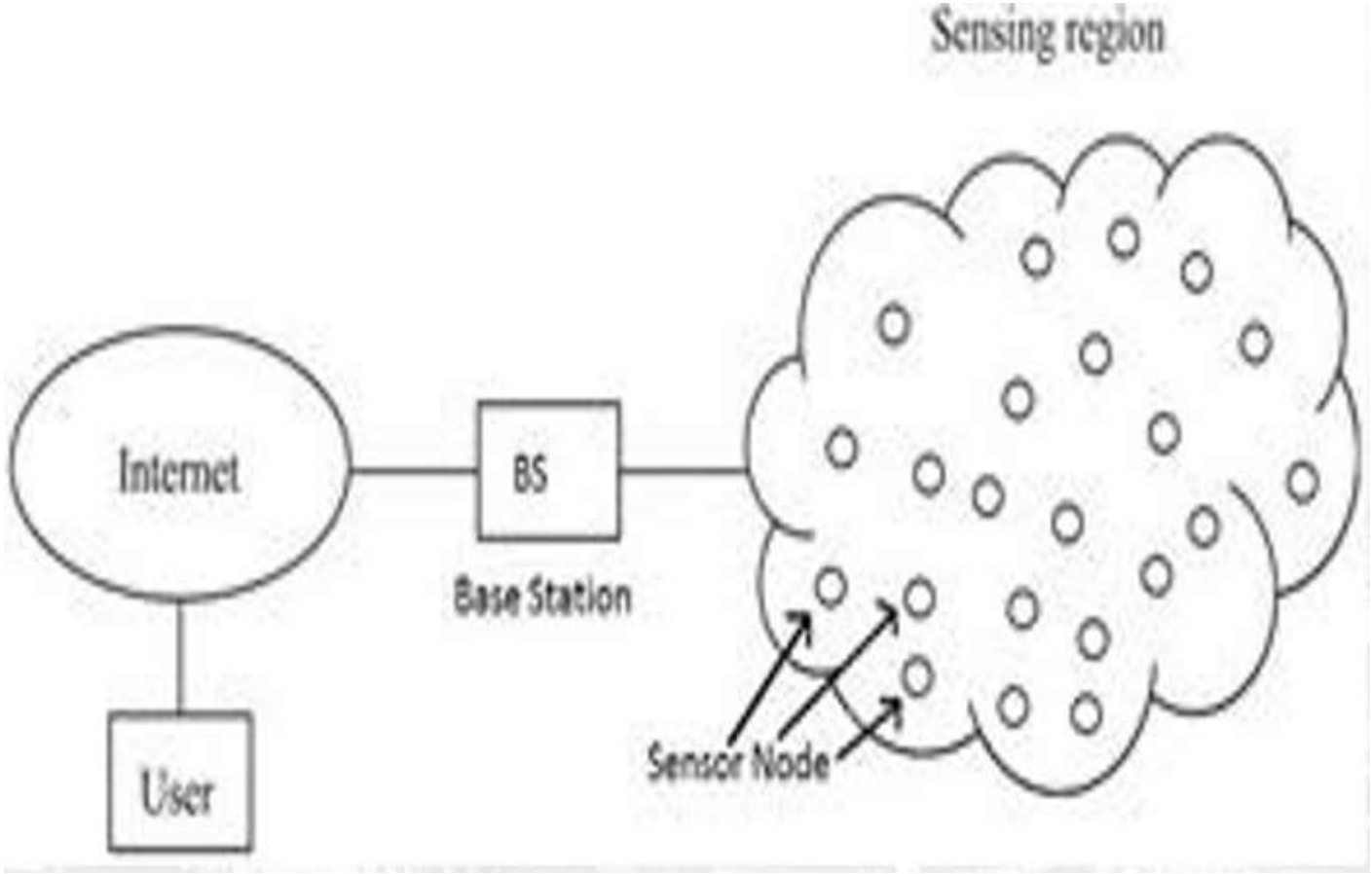
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Introduction to Wireless Sensor Networks

- Sensor networks are highly distributed networks of small, lightweight wireless node, deployed in large numbers to monitor the environment or system.
- Each node of the sensor networks consist of three subsystem:
  - Sensor subsystem: senses the environment
  - Processing subsystem: performs local computations on the sensed data
  - Communication subsystem: responsible for message exchange with neighboring sensor nodes
- The features of sensor nodes
  - Limited sensing region, processing power, energy


Remote User
Internet
Local User
G
Query
Response
Sensor Node
Base Station
Wireless Sensor Network

Background: Basic Architecture: WSN



- The advantage of sensor networks
  - Robust: a large number of sensors
  - Reliable
  - Accurate: sensor networks covering a wider region
  - Fault-tolerant: many nodes are sensing the same event
- Two important operations in a sensor networks
  - Data dissemination: the propagation of data/queries throughout the network
  - Data gathering: the collection of observed data from the individual sensor nodes to a sink
- The different types of sensors
  - Seismic, thermal, visual, infrared etc.

Applications of Sensor Networks

- Using in military
  - Battlefield surveillance and monitoring, guidance systems of intelligent missiles, detection of attack by weapons of mass destruction such as chemical, biological, or nuclear

- Using in nature
  - Forest fire, flood detection, habitat exploration of animals

- Using in health
  - Monitor the patient's heart rate or blood pressure, and sent regularly to alert the concerned doctor, provide patients a greater freedom of movement

- Using in home (smart home)
  - Sensor node can built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled

- Using in office building
  - Airflow and temperature of different parts of the building can be automatically controlled

- Using in warehouse
  - Improve their inventory control system by installing sensors on the products to track their movement

Comparison between
Wireless Senor Networks and Ad Hoc Wireless Networks

- The number of nodes in sensor network can be several orders of magnitude large than the number of nodes in an ad hoc network.
- Sensor nodes are more easy to failure and energy drain, and their battery sources are usually not replaceable or rechargeable.
- Sensor nodes may not have unique global identifiers(ID), so unique addressing is not always feasible in sensor networks.
- Sensor networks are data-centric, the queries in sensor networks are addressed to nodes which have data satisfying some conditions.
- Ad Hoc networks are address-centric, with queries addressed to particular nodes specified by their unique address.
- Data fusion/aggregation: the sensor nodes aggregate the local information before relaying.
- The goals are reduce bandwidth consumption, media access delay, and power consumption for communication.

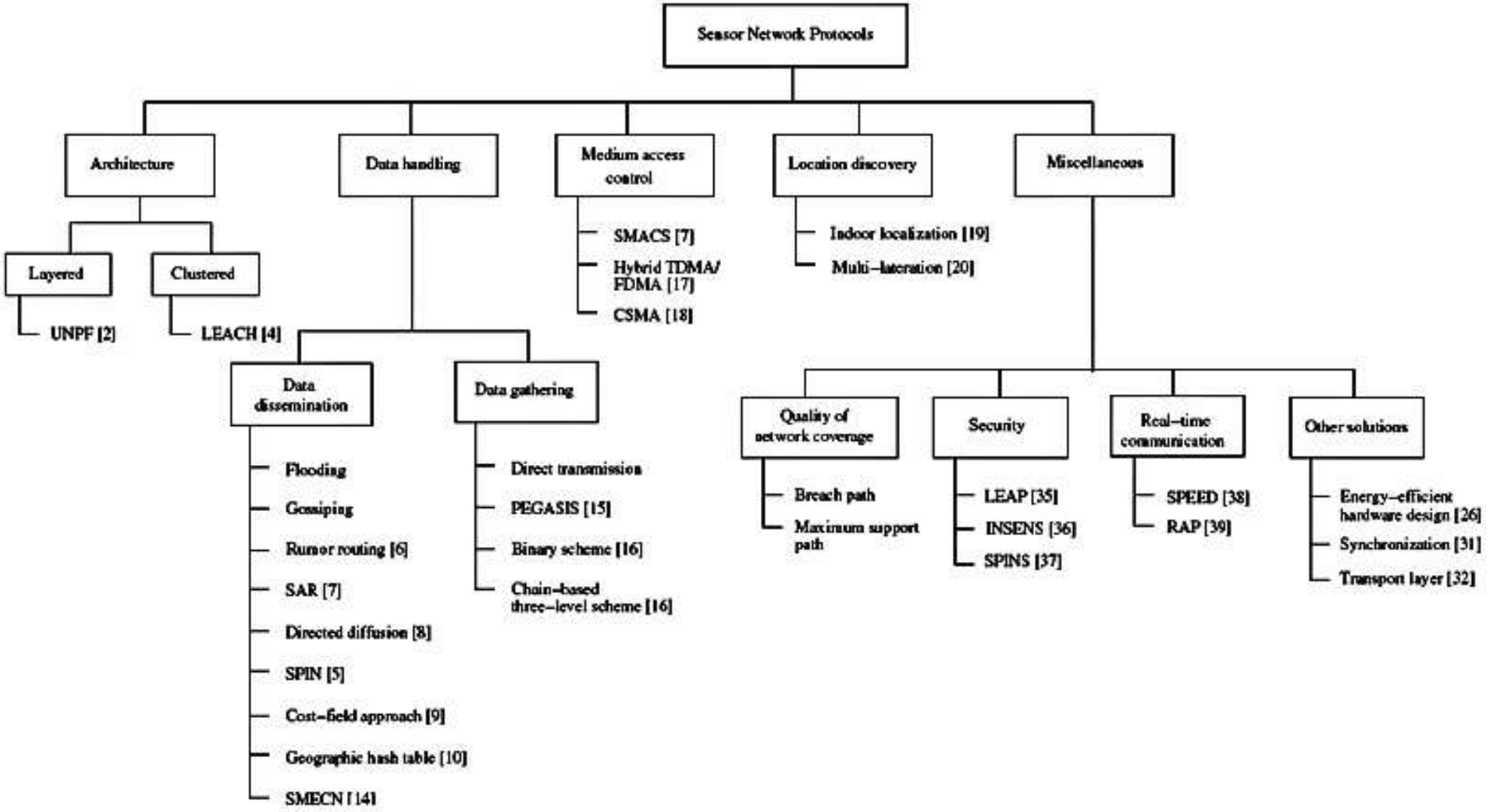
Issues and Challenges in Designing a Sensor Network

- Sensor nodes are randomly deployed and hence do not fit into any regular topology.
- Once deployed, they usually do not require any human intervention.
- Hence, the setup and maintenance of the network should be entirely autonomous.
- Sensor networks are infrastructure-less.
- Therefore, all routing and maintenance algorithms need to be distributed.
- Energy problem
- Hardware and software should be designed to conserve power
- Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed.

Issues and Challenges in Designing a Sensor Network

- A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up.
- The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.
- Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.
- Provision must be made for secure communication over sensor networks, especially for military applications which carry sensitive data.

Classification of Sensor Network Protocols



Sensor Network Architecture

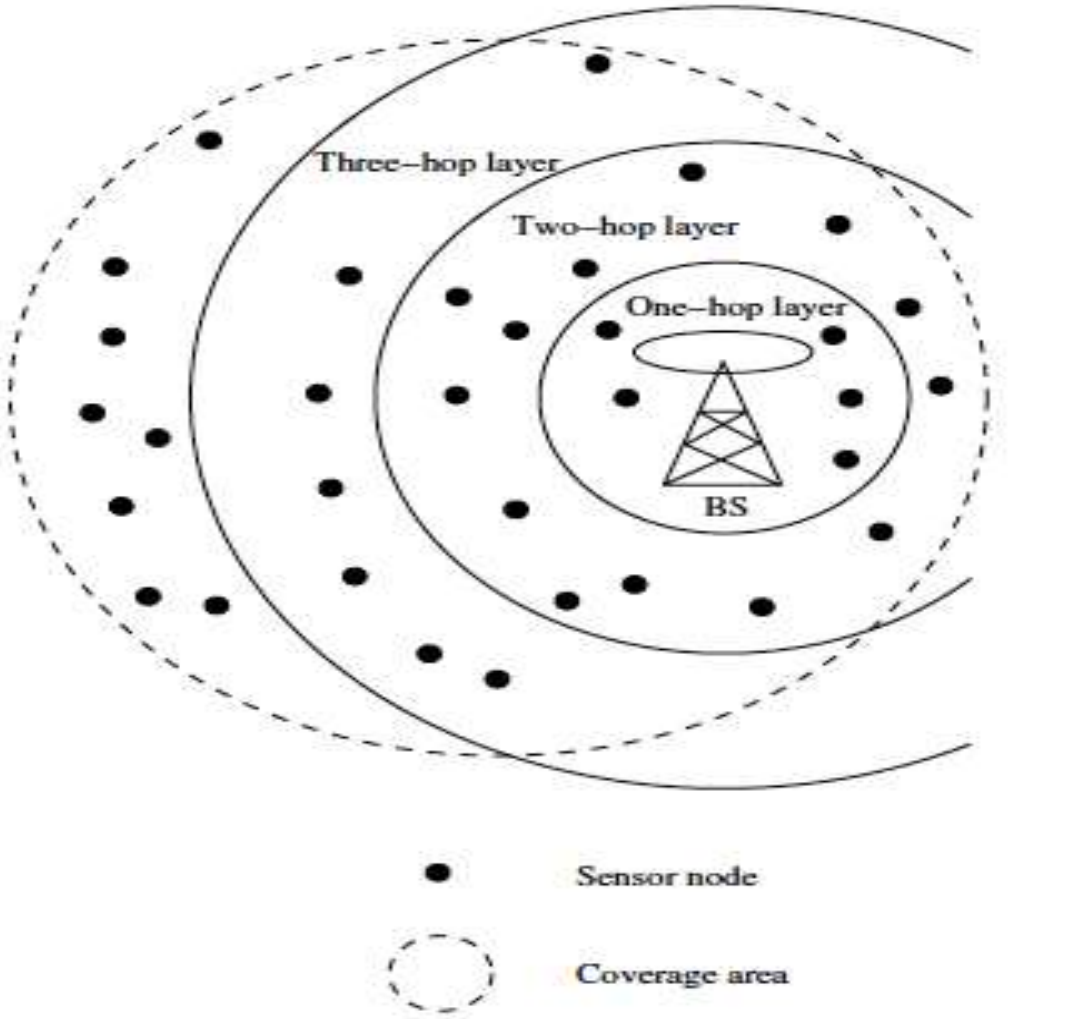
The design of sensor networks is influenced by factors such as scalability, fault tolerance, and power consumption.

The two basic kinds of sensor network architecture are

1. Layered Architecture and
2. Clustered Architecture

Layered Architecture

- It has a single powerful base station, and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS.
- Used with in-building wireless backbones, and in military sensor-based infrastructure, such as MINA
- In the in-building scenario, the BS acts an access point to a wired network, and small nodes form a wireless backbone to provide wireless connectivity.
- The users of the network have hand-held devices such as PDAs which communicate via the small nodes to the BS.
- **Advantage:** as each node is involved only in short-distance, low-power transmissions to nodes of the neighboring layers.



Unified Network Protocol Framework (UNPF)

- It is a set of protocols for complete implementation of a layered architecture for sensor networks

- UNPF integrates three operations in its protocol structure:
  1. Network initialization and maintenance
  2. MAC protocols
  3. Routing protocols

Network Initialization and Maintenance Protocol

- Organizes the sensor nodes into different layers, using the broadcast capability of the BS.
- The BS can reach all nodes in a one-hop communication over a common control channel.
- The BS broadcasts its ID using a known CDMA code on the common control channel.
- All nodes which hear this broadcast then record the BS ID.
- They send a beacon signal with their own IDs at their low default power levels.
- Those nodes which the BS can hear form layer one since they are at a single-hop distance from BS
- The BS now broadcasts a control packet with all layer one node IDs.
- All nodes send a beacon signal again.
- The layer one nodes record the IDs which they hear and these form layer two.
- In the next round of beacons, the layer one nodes inform the BS of the layer two nodes, which is then broadcast to the entire network.
- In this way, the layered structure is built by successive rounds of beacons and BS broadcasts.
- Periodic beaconing updates neighbor information and alters the layer structure if nodes die out or move out of range.

MAC Protocol

- Network initialization is carried out on a common control channel.
- During the data transmission phase, the distributed TDMA receiver oriented channel (DTROC) assignment MAC protocol is used.
- Two steps of DTROC :

1. Channel allocation: (The assignment of reception channels to the nodes)

– Each node is assigned a reception channel by the BS, and channel reuse is such that collisions are avoided.

2. Channel scheduling: (The sharing of the reception channel among neighbors)

– The node schedules transmission slots for all its neighbors and broadcasts the schedule.

– This enables collision-free transmission and saves energy, as nodes can turn off when they are not involved on a send/receive operation.

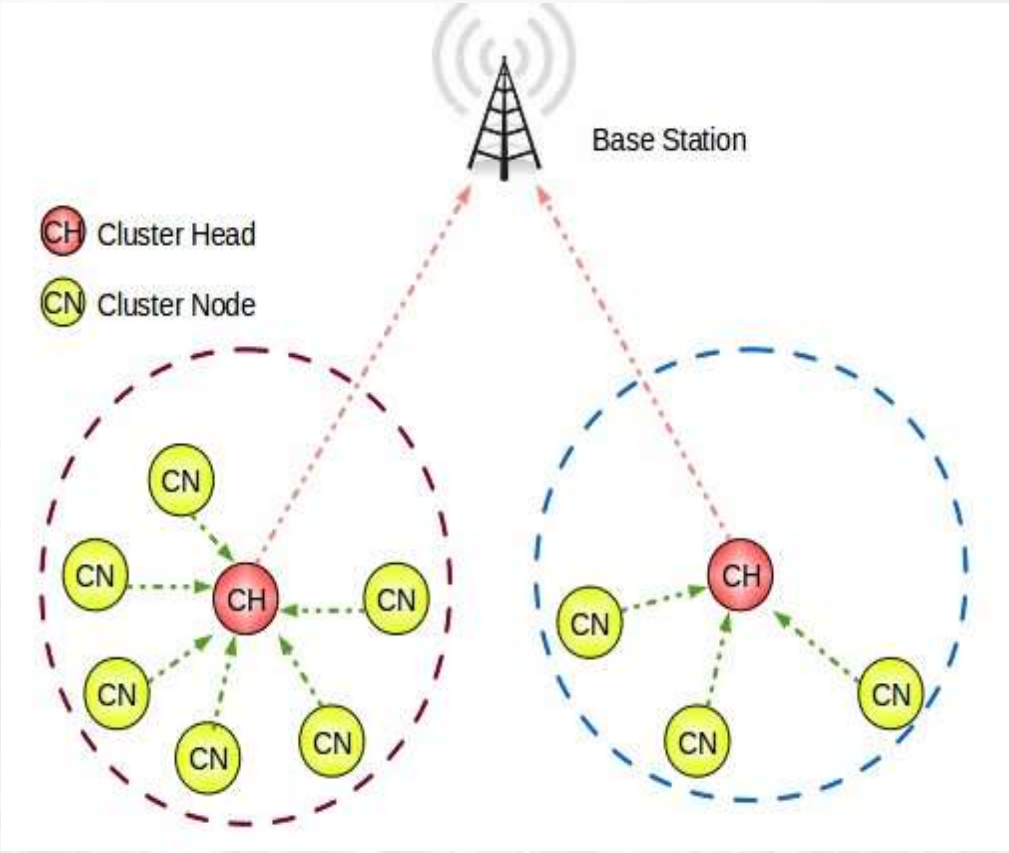
DTROC avoids hidden terminal and exposed terminal problems by suitable channel allocation algorithms.

Routing Protocol

- Downlink from the BS is by direct broadcast on the control channel.
- The layered architecture enables multi-hop data forwarding from the sensor nodes to the BS.
- Uplink from the sensor nodes to BS is by multi-hop data forwarding.
- The node to which a packet is to be forwarded is selected considering the remaining energy of the nodes.
- This achieves a higher network lifetime.
- Existing ad hoc routing protocols can be simplified for the layered architecture,
- Since only nodes of the next layer need to be maintained in the routing table.

Clustered Architecture

- Organizes the sensor nodes into clusters, each governed by a cluster-head.
- The nodes in each cluster are involved in message exchanges with their cluster-heads, and these heads send message to a BS.
- It is useful for sensor networks because of its inherent suitability for data fusion.
- The data gathered by all member of the cluster can be fused at the cluster-head, and only the resulting information needs to be communicated to the BS.
- Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process.
- This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy (LEACH)



A clustered architecture where any message can reach the BS in at most two hops

Low-Energy Adaptive Clustering Hierarchy (LEACH)

- LEACH is a clustering-based protocol that minimizes energy dissipation in sensor networks.
- LEACH randomly selects nodes as cluster-heads and performs periodic reelection, so that the high-energy dissipation experienced by the cluster-heads in communicating with the BS is spread across all nodes of the network.
- Each iteration of selection of cluster-heads is called a round.
- The operation of LEACH is split into two phases: **set-up** and **steady**.
  - **During the set-up phase**, each sensor node chooses a random number between 0 and 1.
  - If this is lower than the threshold for node n, T(n), the sensor node becomes a cluster-head.
- **The steady phase** is of longer duration in order to minimize the overhead of cluster formation.
- **During the steady phase**, data transmission takes place based on the TDMA schedule, and the cluster-heads perform data aggregation/fusion through local computation.
- The BS receives only aggregated data from cluster heads, leading to energy conservation.
- After a certain period of time in the steady phase, cluster-heads are selected again through the set-up phase.

Data Dissemination

- It is the process by which queries or data are routed in the sensor network.
- The data collected by sensor nodes has to be communicated to the node who interested in the data or collector of data.
- The node that generates data is call *Source Node* and the information to be reported is called *an event*.
- A node which interested in an event is called *Sink Node*.
- Data dissemination consist of a two-step process :

Interest propagation: An interest is a descriptor for a particular kind of data or event that a node is interested in, such as temperature, intrusion, or presence of bio-agents.

- For every event that a sink is interested in, it broadcasts its interest to its neighbors and periodically refreshes its interest.
- The interest is propagated across the network, and every node maintains an interest cache of all events to be reported.
- This is similar to a multicast tree formation, rooted at the sink.
- When an event is detected, it is reported to the interested nodes after referring to the interest cache.
- Intermediate nodes maintain a data cache and can aggregate the data or modify the rate of reporting data.

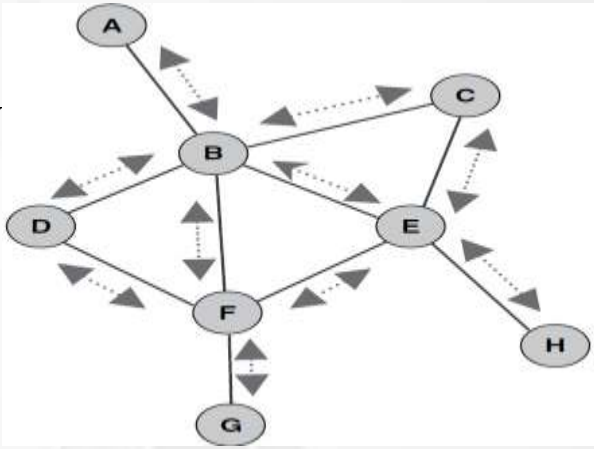
Data Dissemination

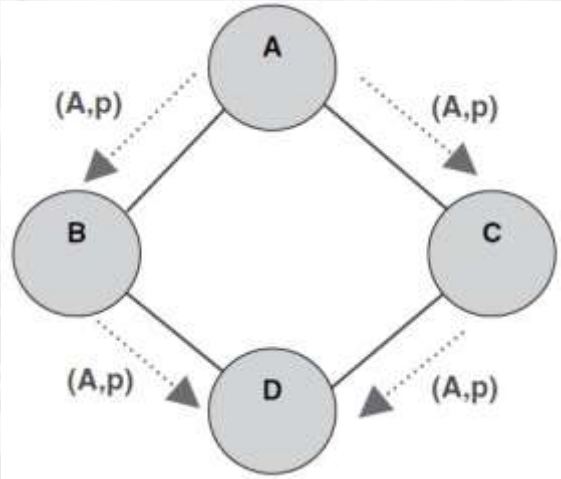
Data propagation:

- When an event is detected, it is reported to the interested nodes (sink node).
- The paths used for data propagation are modified by preferring the shortest paths and deselecting the weaker or longer paths.
- The basic idea of diffusion is made efficient and intelligent by different algorithms for interest and data routing.

1. Flooding

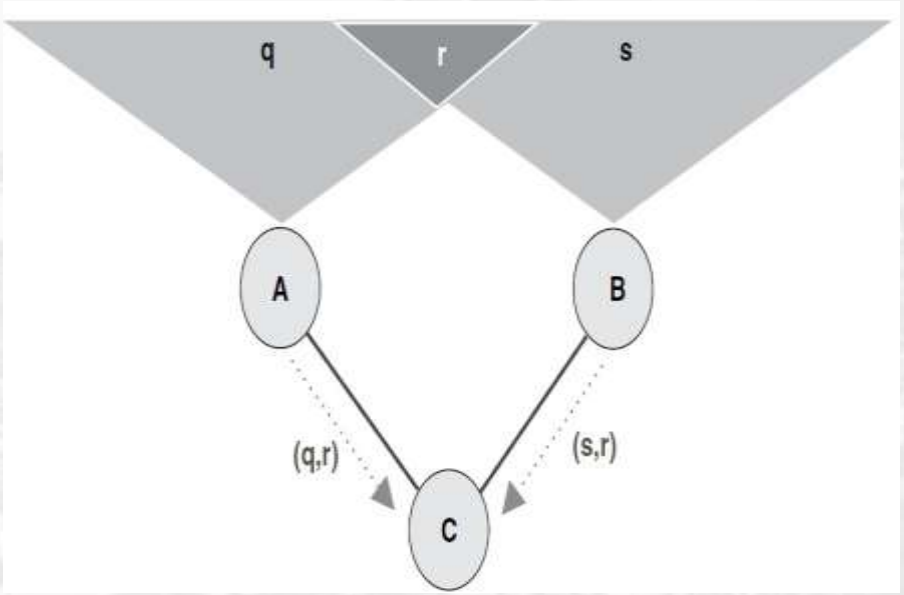
- Every sensor node (re-) broadcasts sensor data to all of its neighbors
- In flooding, each node which receives a packet broadcasts it if the maximum hop-count of the packet is not reached and the node itself is not the destination of the packet.
- This technique does not require complex topology maintenance or route discovery algorithms.
- Simple and reliable technique
- Incurs large traffic overhead (maximum-hop counts and sequence numbers can be used to limit broadcasts and eliminate duplicates)
- However, flooding faces three more challenges:
  - Traffic Implosion: This is the situation when duplicate messages are sent to the same node. This occurs when a node receives copies of the same message from many of its neighbors.
  - Overlap: The same event may be sensed by more than one node due to
  - overlapping regions of coverage. This results in their neighbors receiving duplicate reports of the same event.
  - Resource blindness: The flooding protocol does not consider the available energy at the nodes and results in many redundant transmissions. Hence, it reduces the network lifetime.





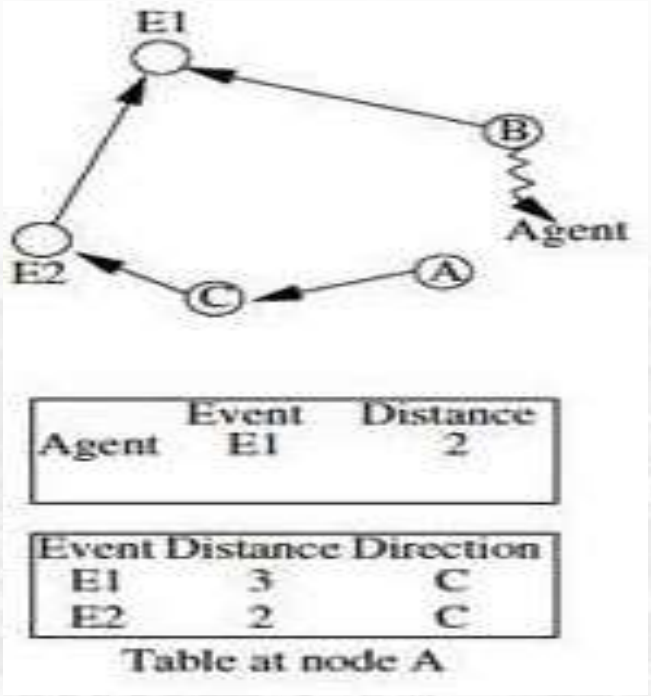
2. Gossiping

- Modified version of flooding i.e. **Gossiping**
- The nodes do not broadcast a packet, but send it to a randomly selected neighbor
- Avoid the problem of implosion by limiting the number of packets that each node sends to its neighbor to one copy
- It takes a long time for message to propagate throughout the network
- It does not guarantee that all nodes of network will receive the message



3. Rumor Routing

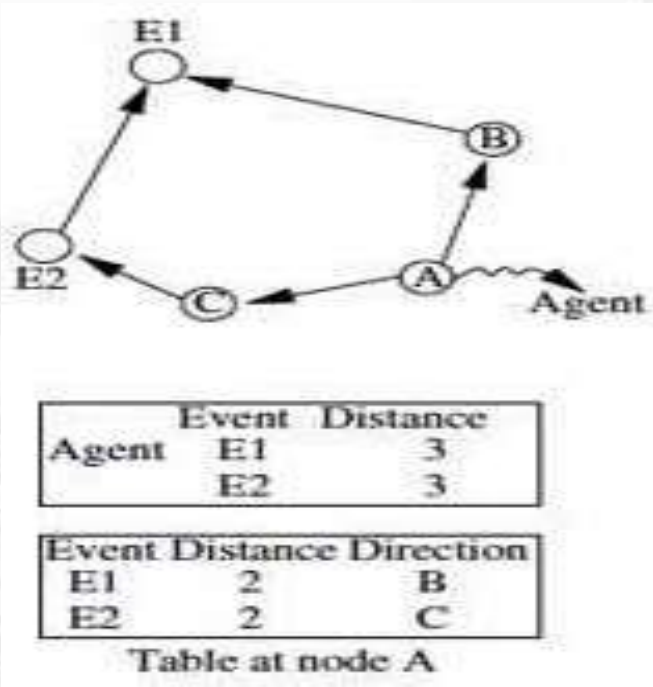
- Agent-based path creation algorithm
- Agent is a long-lived packet created at random by nodes
- It circulated in the network to establish shortest paths to events that they encounter.
- When an agent finds a node whose path to an event is longer than its own, it updates the node's routing table.



Agent	Event	Distance
	E1	2

Event	Distance	Direction
E1	3	C
E2	2	C

Table at node A

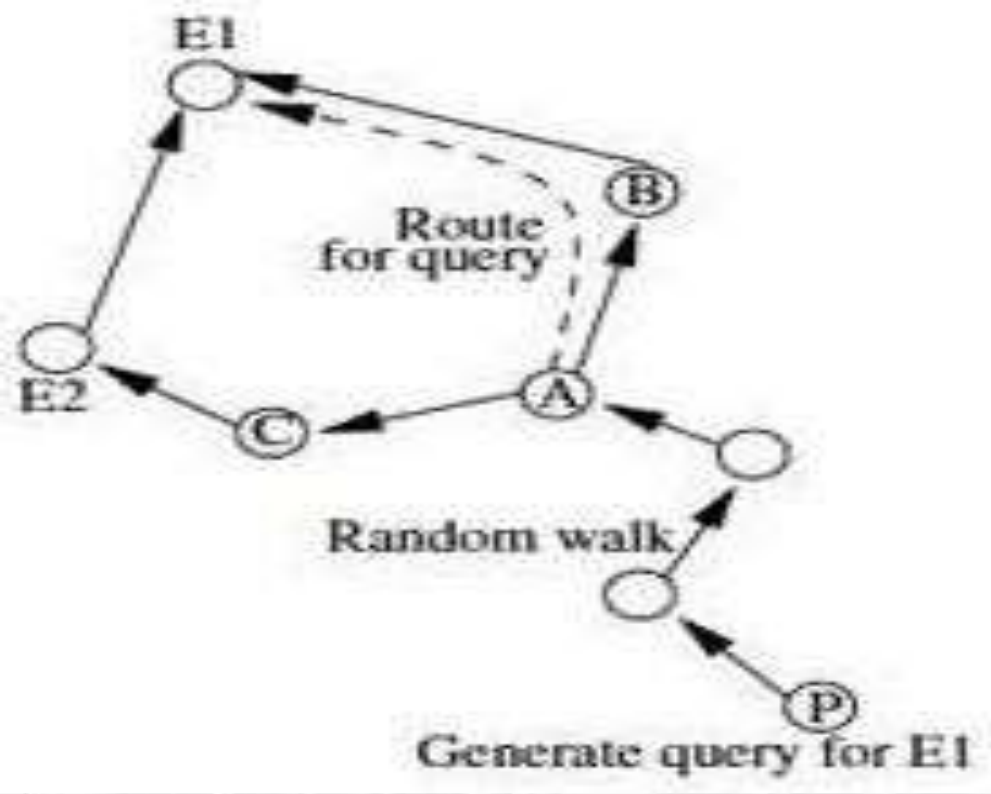


Agent	Event	Distance
	E1	3
	E2	3

Event	Distance	Direction
E1	2	B
E2	2	C

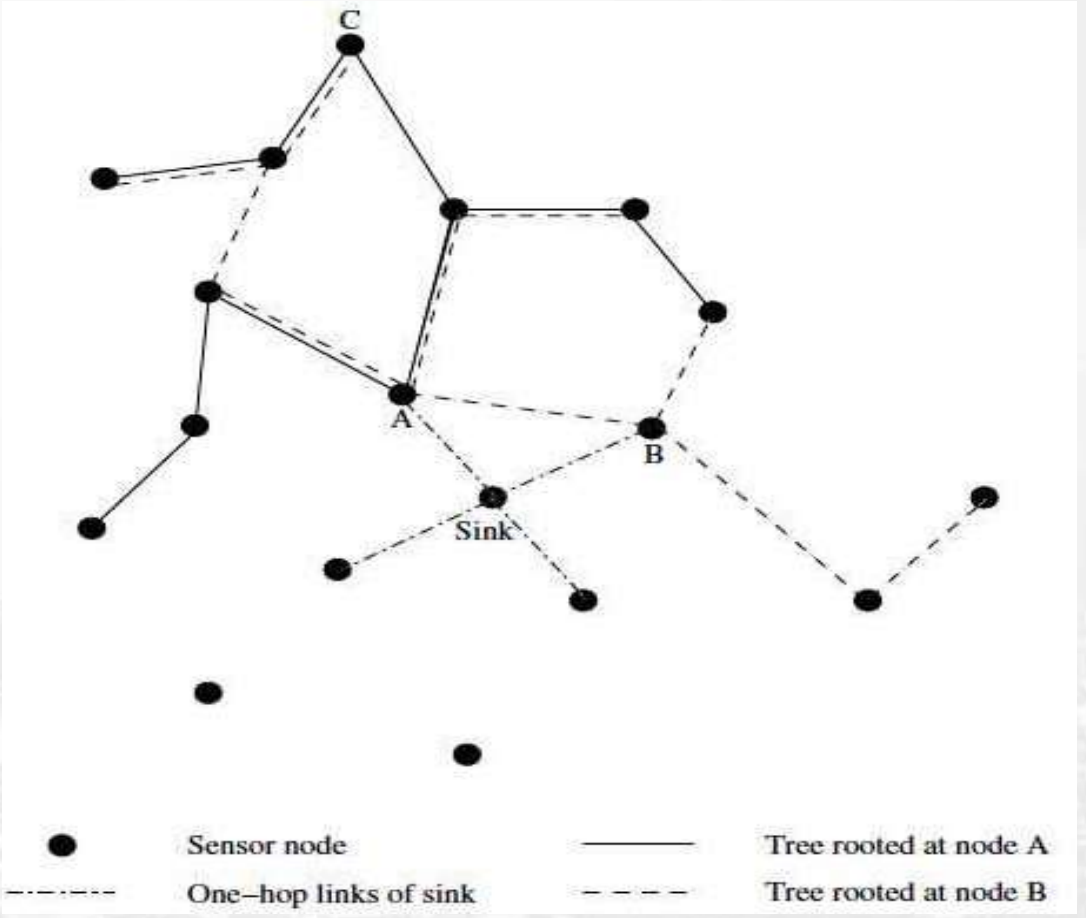
Table at node A

- When a query is generated at a sink, it is sent on a random walk with the hope that it will find a path leading to the required event.
- If a query does not find an event path, the sink times out and uses flooding as a last resort to propagate the query.



4. Sequential Assignment Routing (SAR)

- It creates multiple trees, where the root of each tree is a one-hop neighbor of the sink.
- To avoid nodes with low throughput or high delay.
- Each sensor node records two parameters: available energy resources on the path and an additive QoS metric such as delay.
  - Higher priority packets take lower delay paths, and lower priority packets have to use the paths of greater delay, so that the priority x delay QoS metric is maintained.
- SAR minimizes the average weighted QoS metric over the lifetime of the network.



5. Directed Diffusion

- Useful in scenarios where the sensor nodes themselves generate requests/queries for data sensed by other nodes.
- Each sensor node names its data with one or more attributes.
- Each sensor node express their interest depending on these attributes.
- Each path is associated with a interest gradient, while positive gradient make the data flow along the path, negative gradient inhibit the distribution data along a particular path.
  - Example : two path formed with gradient 0.4 and 0.8, the source may twice as much data along the higher one
  - Suppose the sink wants more frequent update from the sensor which have detected an event => send a higher data-rate requirement for increasing the gradient of that path.

- Query
  - Type = vehicle /* detect vehicle location
    interval = 1 s /* report every 1 second
    rect = [0,0,600,800] /* query addressed to sensors within the rectangle
    timestamp = 02:30:00 /* when the interest was originated
    expiresAt = 03:00:00 /* till when the sink retain interest in this data

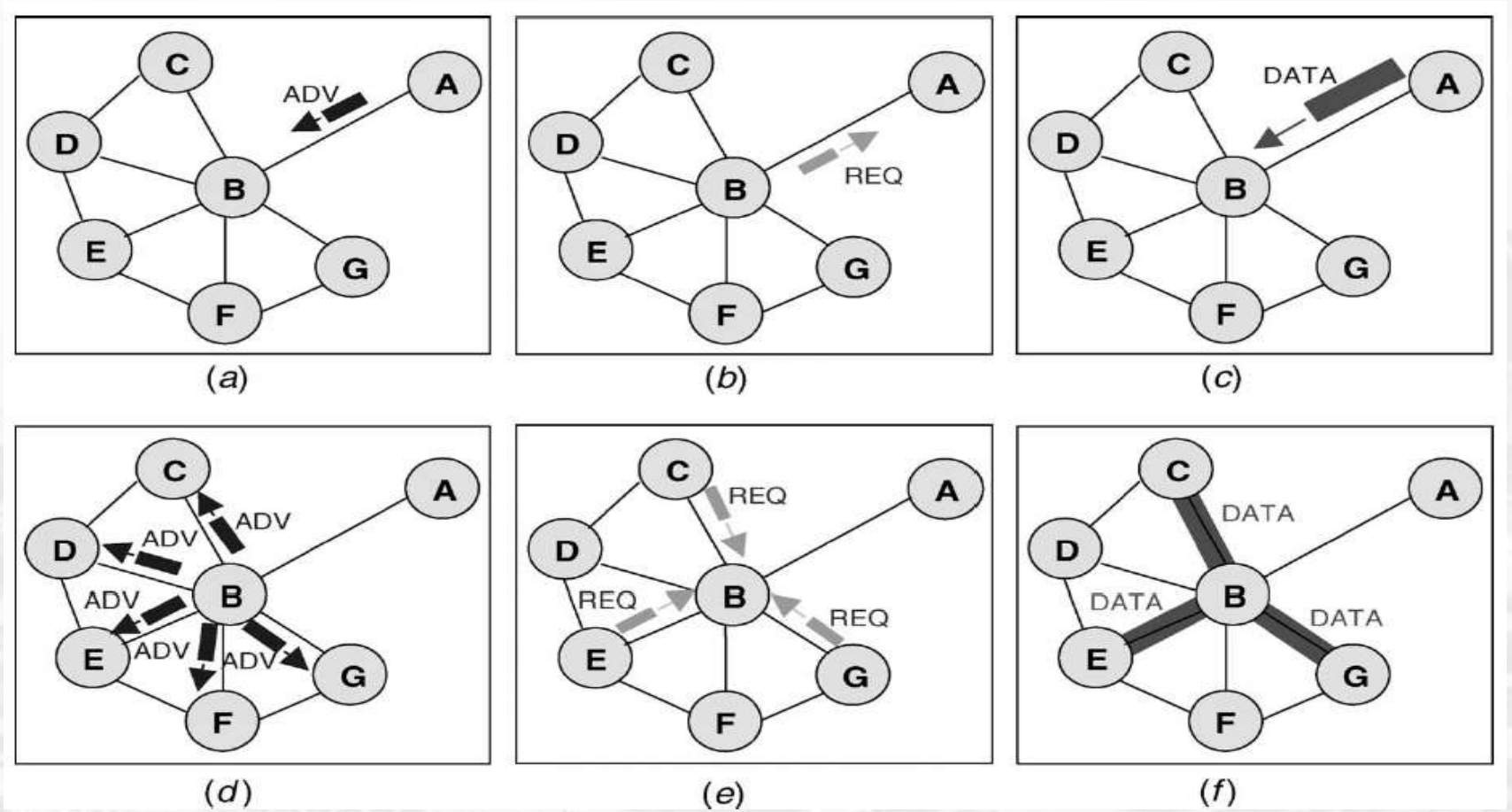
- Report
  - Type = vehicle /* type of intrusion seen
    instance = car /* particular instance of the type
    location = [200,250] /* location of node
    confidence = 0.80 /* confidence of match
    timestamp = 02:45:20 /* time of detection

6. Sensor Protocols for Information via Negotiation (SPIN)

- Example of data-centric routing
- Objective of SPIN are Data Negotiation and Resource Adaptation
- Uses negotiations to address all problems of flooding
  - **implosion:** nodes negotiate before data transmission
  - **overlap:** nodes negotiate before data transmission
  - **resource blindness:** resource manager keeps track of actual resource consumption and adapts routing and communication behavior

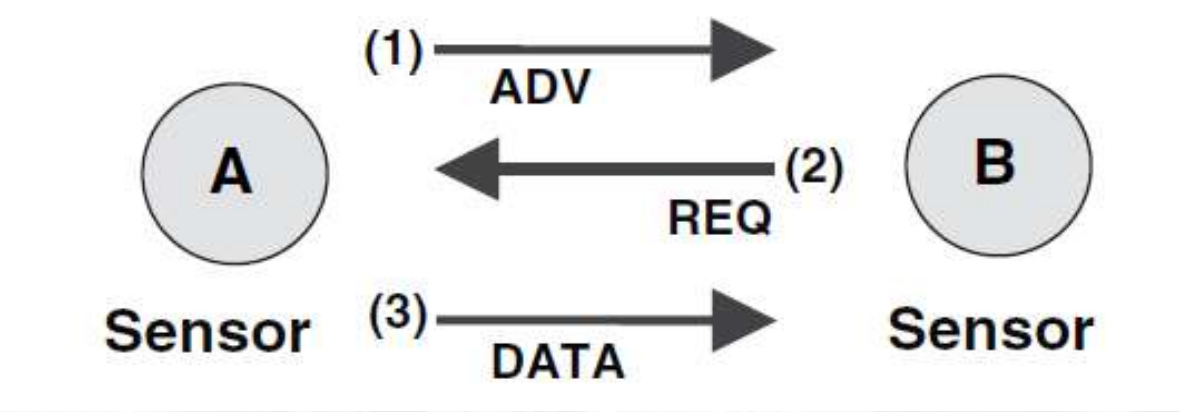
- SPIN uses meta-data instead of raw data.

- To carry out negotiation and data transmission, nodes running SPIN use three types of messages: ADV, REQ, DATA



SPIN-PP

- Optimized for networks using point-to-point transmission media (two nodes communicate exclusively with each other without interference)
- Three step handshake protocol used
- SPIN-PP uses negotiation to overcome the implosion and overlap problems of the traditional flooding and gossiping protocols

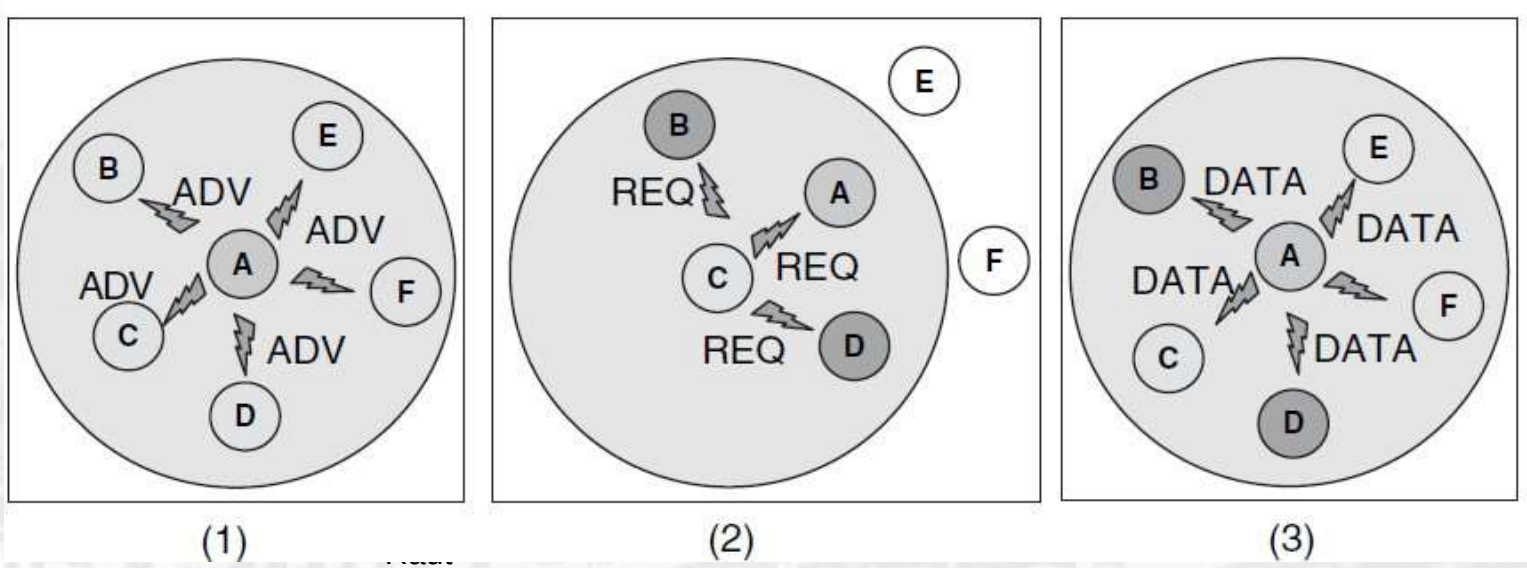


SPIN-EC

- Adds simple heuristic to protocol to add energy conservation
- As long as energy sufficient, node participates in 3-way handshake
- Nodes does not participate if it believes that this will reduce its energy below a certain low-energy threshold
  - Node replies to ADV only if sufficient energy for transmitting REQ and receiving DATA
  - Node initiates handshake only if it has sufficient energy to send DATA to all neighbors

SPIN-BC

- Uses one-to-many communications (broadcast)
- Receiver node waits for a random time interval before issuing REQ; if other node's REQ overheard, the receiver node cancels timer and does not send its own REQ
- Advertiser broadcasts DATA only once (ignore duplicate REQs)
- In broadcast environments, SPIN-BC has the potential to reduce energy consumption by eliminating redundant exchange of data requests and replies.



SPIN-RL

❖ Reliable version of SPIN-BC

- Nodes keep track of overheard REQ messages
- If DATA message does not arrive within certain timeout interval, it assumes that either REQ or DATA did not arrive
- Node broadcasts REQ to re-request data
  - in message header, node specifies identity of randomly selected node among nodes that previously sent ADV for missing DATA
- SPIN-RL limits frequency with which DATA messages are sent
  - once a node sends a DATA message, it will wait for certain amount of time before responding to other requests for the same data

Data Gathering

- The objective of the data gathering problem is to transmit the sensed data from each sensor node to a BS.
- One round is defined as the BS collecting data from all the sensor nodes once.
- The goal of algorithm which implement data gathering is
  - maximize the lifetime of network
  - Minimum energy should be consumed
  - The transmission occur with minimum delay
- The energy × delay metric is used to compare algorithms

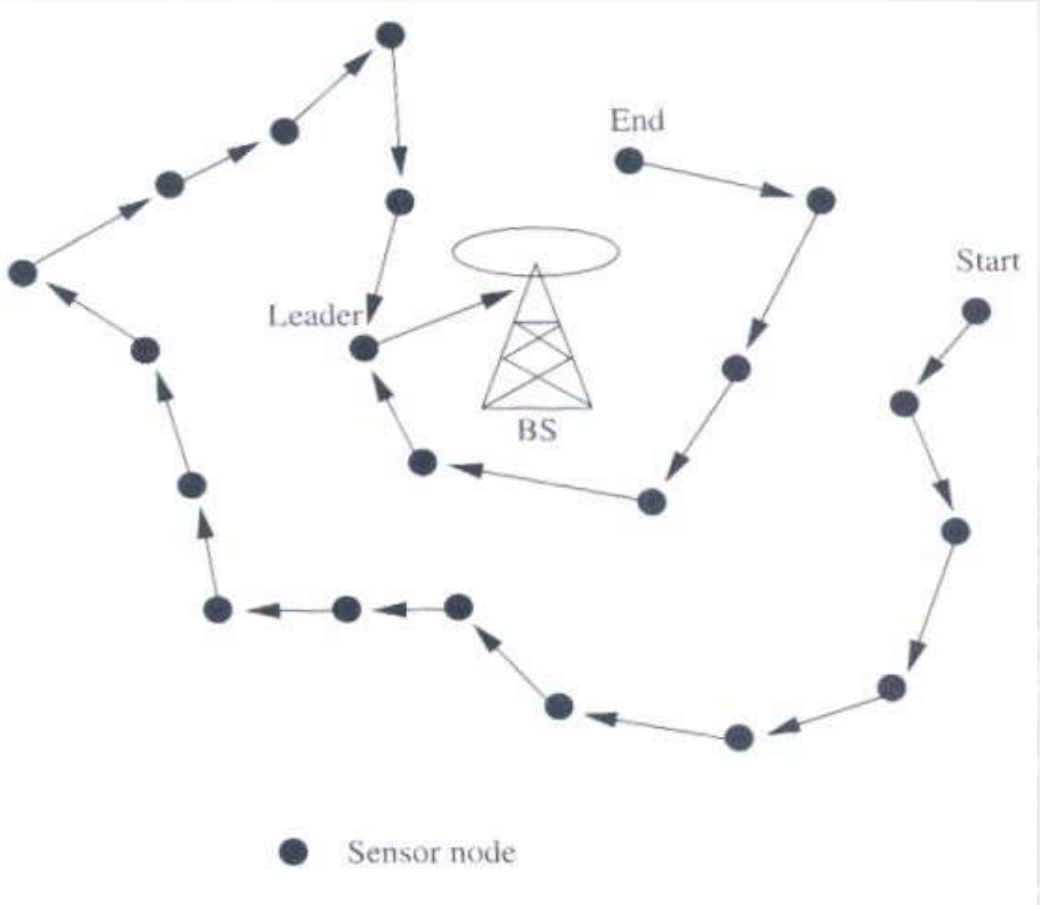
Algorithms that implement Data Gathering
1. Direct Transmission

- All sensor nodes transmit their data directly to the BS.
- It is cost expensive when the sensor nodes are very far from the BS.
- Nodes must take turns while transmitting to the BS to avoid collision, so the media access delay is also large.
- Hence, this scheme performs poorly with respect to the energy × delay metric.

2. Power-Efficient Gathering for Sensor Information Systems (PEGASIS)

- PEGASIS based on the assumption that all sensor nodes know the location of every other node.
- The topology information is available to all nodes.
- Any node has the required transmission range to reach the BS in one hop, when it is selected as a leader.
- The goal of PEGASIS are as following
  - Minimize the distance over which each node transmit
  - Minimize the broadcasting overhead
  - Minimize the number of messages that need to be sent to the BS
  - Distribute the energy consumption equally across all nodes
- A **Greedy Algorithm** is used to construct a chain of sensor nodes, starting from the node farthest from the BS.
- At each step, the nearest neighbor which has not been visited is added to the chain.
- The chain is constructed a priori, before data transmission begins, and is reconstructed when nodes die out.

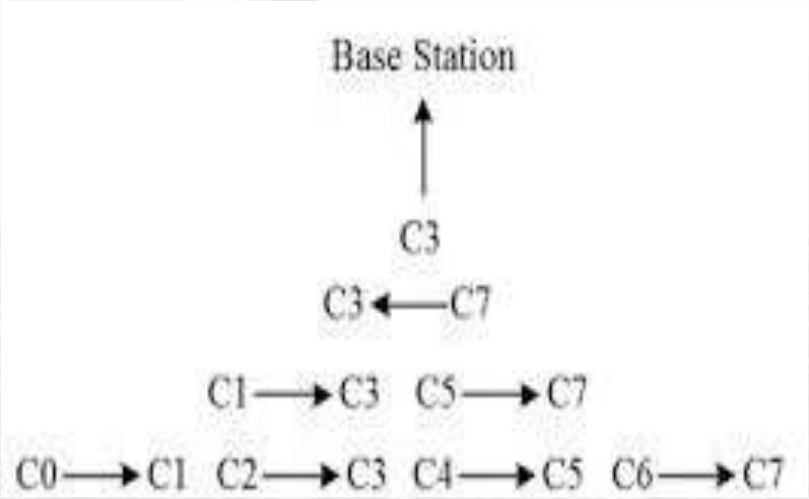
Data gathering with PEGASIS

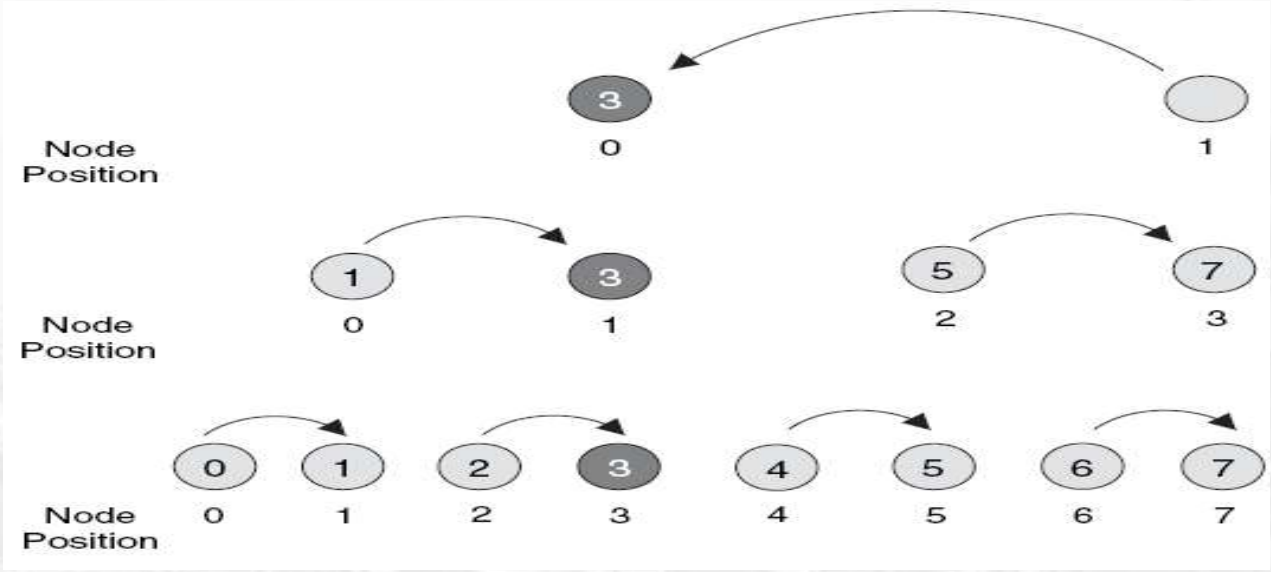


- At every node, data fusion or aggregation is carried out, so that only one message is passed on from one node to the next.
- A node which is designated as the leader finally transmits one message to the BS.
- Leadership is transferred in sequential order, and a token is passed so that the nodes know in which direction to pass messages in order to reach the leader.
- The delay involved in messages reaching the BS is O(N), where *N* is the total number of nodes in the network.

3. Binary Scheme

- This is a chain-based scheme like PEGASIS, which classifies nodes into different levels.
- This scheme is possible when nodes communicate using CDMA, so that transmissions of each level can take place simultaneously.
- The delay is O(logN)

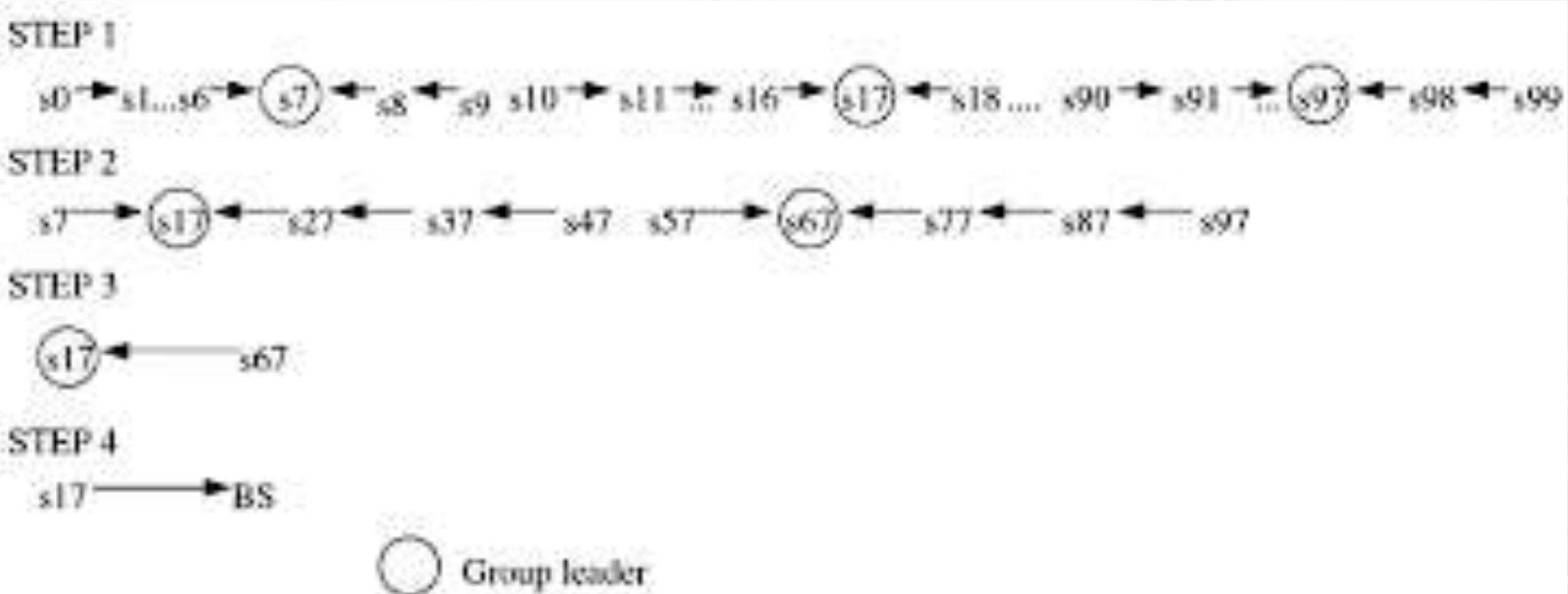




4. Chain-Based Three-Level Scheme

- For non-CDMA sensor nodes
- The chain is divided into a number of groups to space out simultaneous transmissions in order to minimize interference.
- Within a group, nodes transmit data to the group leader, and the leader fusion the data, and become the member to the next level.

- In the second level, all nodes are divided into two groups.
- In the third level, consists of a message exchange between one node from each group of the second level.
- Finally, the leader transmit a single message to the BS.



Overview of Positioning, Localization and Synchronization

Location Discovery

- During aggregation of sensed data, the location information of sensors must be considered.
- Each nodes couple its location information with the data in the messages it sends.
- GPS is not always feasible because it cannot reach nodes in dense foliage or indoor, and it consumes high power
- We need a low-power, inexpensive, and reasonably accurate mechanism.

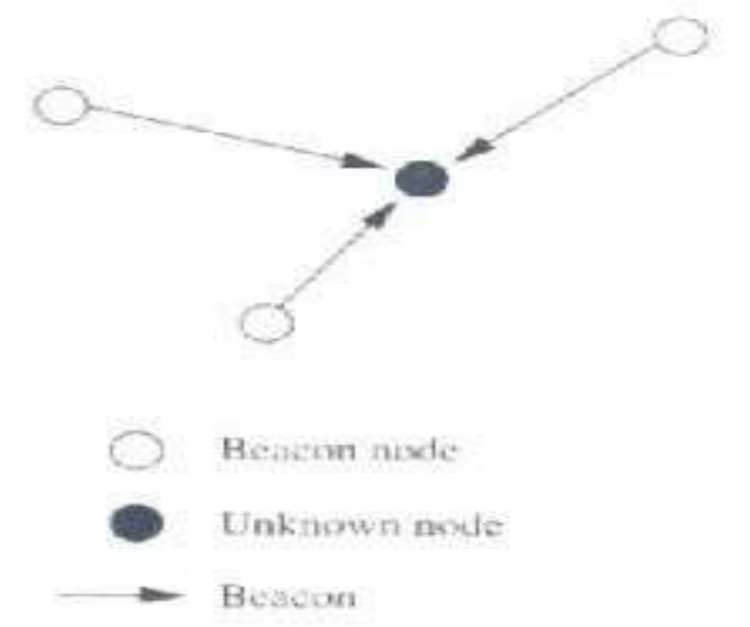
1. Indoor Localization

- Fixed beacon nodes are placed in the field of observation, such as within building.
- The randomly distributed sensors receive beacon signals from the beacon nodes and measure the signal strength, angle of arrival, time difference between the arrival of different beacon signals.
- The nodes estimate distances by looking up the database instead of performing computations.
- Only the BS may carry the database.

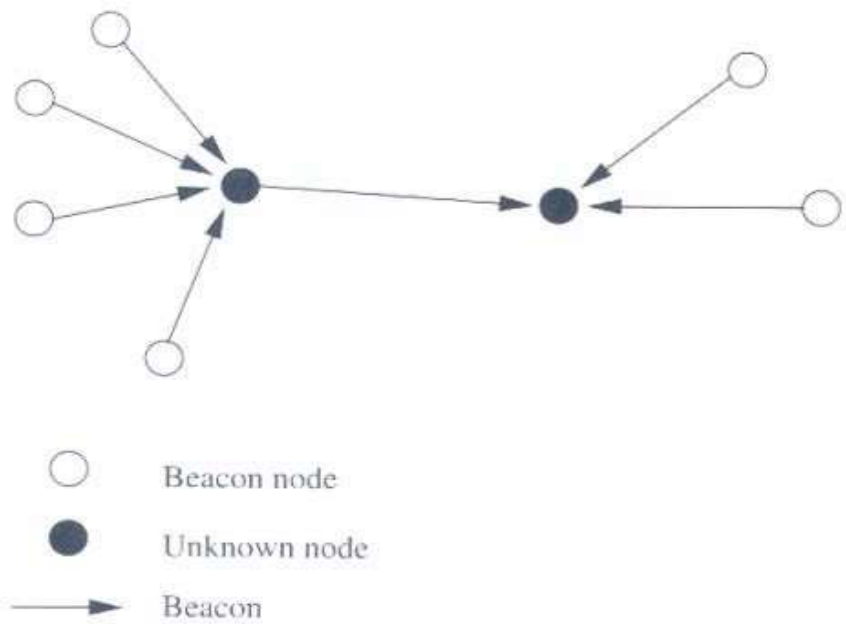
2. Sensor Network Localization

- In situations where there is no fixed infrastructure available, some of the sensor nodes themselves act as beacons.
- Using GPS, the beacon nodes have their location information, and send periodic beacons signal to other nodes.
- In the case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate the distance.
- The time difference between beacon arrivals from different nodes can be used to estimate location.
- Multi-lateration (ML) techniques
  - Atomic ML
  - Iterative ML
  - Collaborative ML

- Atomic ML



- Iterative ML



Synchronization in Sensor networks

Time synchronization is highly critical in sensor networks for purposes such as:

- Data Diffusion
- Coordinated Actuation
- Object Tracking

To Synchronize all the nodes in the sensor network using a method that:

- Eliminates error efficiently
- Energy conservative
- Provides tight synchronization

Clocks and the Synchronization Problem

Common time scale among sensor nodes is important for a variety of reasons,
identify causal relationships between events in the physical world support the elimination of redundant data facilitate sensor network operation and protocols.
Typical clocks consist of quartz-stabilized oscillator and a counter that is decremented with every oscillation of the quartz crystal When counter reaches 0, it is reset to original value and interrupt is generated Each interrupt (clock tick) increments software clock (another counter)Software clock can be read by applications using API Software clock provides local time with C(t) being the clock reading at real time t Time resolution is the distance between two increments (ticks) of software clock

Clock Parameters

Clock offset: difference between the local times of two nodes Synchronization is required to adjust clock readings such that they match Clock rate: frequency at which a clock progresses Clock skew: difference in frequencies of two clocks Clock rate dC/dt depends on temperature, humidity, supply voltage, age of quartz, etc., resulting in drift rate (dC/dt-1)

C(t) must be piecewise continuous (strictly monotone function of time)clock adjustments should occur gradually, e.g., using a linear compensation function that changes the slope of the local time simply jumping forward/backward in time can have unintended consequences time-triggered events may be repeated or skipped

Maximum drift rate ρ given by manufacturer (typical 1ppm to 100ppm)Guarantees that: Drift rate causes clocks to differ even after synchronization Two synchronized identical clocks can drift from each other at rate of at most 2ρ max To limit relative offset to δ seconds, the resynchronization interval τsync must meet the requirement:

Time Synchronization External synchronization

clocks are synchronized with external source of time (reference clock)reference clock is accurate real-time standard (e.g., UTC)Internal synchronization clocks are synchronized with each other (no support of reference clock) goal is to obtain consistent view of time across all nodes in network network-wide time may differ from external real-time standards External synchronization also provides internal synchronization Accuracy: maximum offset of a clock with respect to reference clock Precision: maximum offset between any two clocks If two nodes synchronized externally with accuracy of Δ, also synchronized internally with precision 2Δ

Why Time Synchronization in WSNs?

Sensors in WSNs monitor objects and events in the physical world,
Accurate temporal correlation is crucial to answer questions such as *how many moving objects have been detected? what is the direction of the moving object ? what is the speed of the moving object ?*
If real-time ordering of events is t1<t2<t3, then sensor times should reflect this ordering: C1(t1)<C2(t2)<C3(t3)

Time difference between sensor time stamps should correspond to real-time differences: Δ=C2(t2)-C1(t1)=t2-t1
important for data fusion (aggregation of data from multiple sensors) Synchronization needed by variety of applications and algorithms communication protocols (at-most-once message delivery) security (limit use of keys, detect replay attacks) data consistency (caches, replicated data) concurrency control (atomicity and mutual exclusion) medium access control (accurate timing of channel access) duty cycling (know when to sleep or wake up) localization (based on techniques such as time-of-flight measurements)

Challenges for Time Synchronization

Traditional protocols (e.g., NTP, GPS) are designed for wired networks WSNs pose a variety of additional challenges Environmental effects sensors often placed in harsh environments fluctuations in temperature, pressure, humidity Energy constraints finite power sources (batteries)time synchronization solutions should be energy-efficient Wireless medium and mobility throughput variations, error rates, radio interferences, asymmetric links topology changes, density changes node failure (battery depletion) Other challenges limited processor speeds or memory (lightweight algorithms)cost and size of synchronization hardware (GPS)

Synchronization Messages

Pairwise synchronization: two nodes synchronize using at least one message
Network-wide synchronization: repeat pairwise synchronization throughout network

One-way message exchange: single message containing a time stamp difference can be obtained from $(t2-t1)=D+\delta$ (D=propagation delay)

Two-way message exchange : receiver node responds with message containing three time stamps assumption: propagation delay is identical in both directions and clock drift does not change between measurements

Sender-Receiver Synchronization

Receiver-Receiver Synchronization

Receiver-receiver: multiple receivers of broadcast messages exchange their message arrival times to compute offsets among them

Example: 2 receivers; 3 messages (1 broadcast, 2 exchange messages) No time stamp in broadcast message required

Timing-sync Protocol for Sensor Networks

TPSN is another sender-receiver technique Uses a tree to organize network Uses two phases for synchronization
discovery phase
synchronization phase

Level discovery phase establish hierarchical topology root resides at level 0 root initiates phase by broadcasting level_discovery message (*contains level and identity of sender*) receiver can determine own level (*level of sender plus one*) receiver re-broadcasts message with its own identity and level receiver discards multiple received broadcasts if node does not know its level (*corrupted messages, etc.),* it can issue level_request message to neighbors (*which reply with their levels*) node's level is then one greater than the smallest level received node failures can be handled similarly (i.e., if all neighbors at level i-1 disappear, node issues level_request message if root node dies, nodes in level 1 execute leader election algorithm

Synchronization phase pairwise synchronization along the edges of hierarchical structure each node on level i synchronizes with nodes on level i-1 approach similar to LTS: node j issues synchronization pulse at t1 (containing level and time stamp) node k receives message at t2 and responds with an ACK at t3 (containing t1, t2, t3, and level) node j receives ACK at t4 node j calculates drift and propagation delay

Synchronization phase (contd.) phase initiate by root node issuing time_sync packet after waiting for random interval (to reduce contention), nodes in level 1 initiate two-way message exchange with root node nodes on level 2 will overhear synchronization pulse and initiate two-way message exchange with level 1 nodes after random delay process continues throughout network Synchronization error of TPSN depth of hierarchical structure end-to-end latencies

Flooding Time Synchronization Protocol

Goals of FTSP include: network-wide synchronization with errors in microsecond range scalability up to hundreds of nodes robustness to topology changes. FTSP uses single broadcast message to establish synchronization points Decomposes end-to-end delay into different components

t1: wireless radio informs CPU that it is ready for next message d1: interrupt handling time (few microseconds) t2: CPU generates time stamp d2: encoding time (transform message into electromagnetic waves; deterministic, low hundreds of microseconds) d3: propagation delay (from t3 on node i to t4 on node j; typically very small and deterministic) d4: decoding time (deterministic, low hundreds of microseconds) d5: byte alignment time (delay caused by different byte alignments (bit offsets), i.e., receiving radio has to determine the offset from a known synchronization byte and then shift incoming message accordingly); can reach several hundreds of microseconds t7: interrupt, CPU obtains time stamp

Time-stamping in FTSP sender sends single broadcast containing time stamp (estimated global time) receiver extracts time stamp from message and time-stamps arrival (leads to global-local time pair, providing a synchronization point) synchronization message begins with preamble followed by SYNC bytes, data field, and CRC preamble bytes are used to synchronize receiver radio to carrier frequency SYNC bytes are used to calculate bit offset

Time-stamping in FTSP (contd.)multiple time stamps are used at both sender and receiver to reduce jitter of interrupt handling and encoding / decoding times time stamps are recorded at each byte boundary after the SYNC bytes as they are transmitted or received time stamps are normalized by subtracting appropriate integer multiple of nominal byte transmission time (e.g., approx. 417μs on Mica2) jitter in interrupt handling can be reduced by taking the minimum of normalized time stamps jitter in encoding/decoding can be reduced by averaging these corrected normalized time stamps final (error-corrected) time stamp is added into data part of message at receiver side, time stamp must further be corrected by the byte alignment time (can be determined from transmission speed and bit offset)

Multi-hop synchronization root node is elected based on unique node IDs root node maintains global time and all other nodes synchronize to root synchronization is triggered by broadcast message by the root node.

Whenever node does not receive synchronization message for certain amount of time, it declares itself to be the new root whenever root receives a message from node with lower node ID, it gives up root status all receiver nodes within range establish synchronization points other nodes establish synchronization points from broadcasts of synchronized nodes that are closer to the root .

a new node joining the network with lowest node ID will first collect synchronization messages to adjust its own clock before claiming root status.

Multi-hop scenarios possible by establishing multiple reference beacons, each with its own broadcast domain. Domains can overlap and nodes within overlapping regions serve as bridges to allow synchronization across domains, RBS uses large amount of message exchanges,

However, RBS is a good candidate for post-facto synchronization nodes synchronize after event of interest has occurred to reconcile their clocks

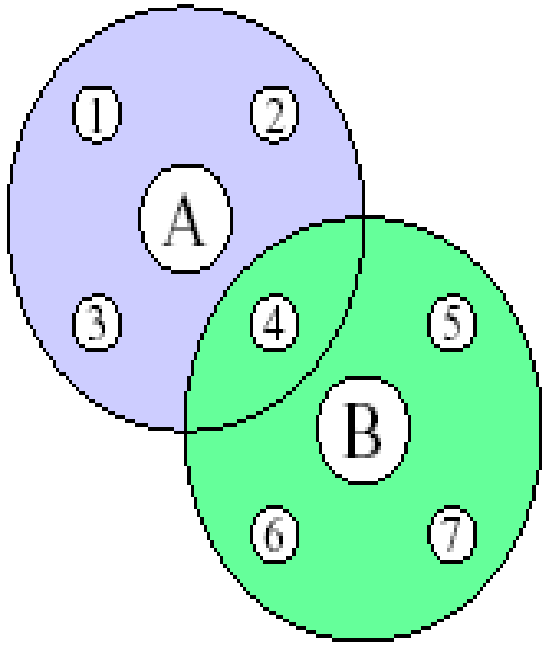


Illustration of Multi-Hop Synchronization

Concept of TTS- Traditional Time Synchronization

The sender periodically sends a message with its current clock as a timestamp to the receiver

Receiver then synchronizes with the sender by changing its clock to the timestamp of the message it has received from the sender (if the latency is small compared to the desired accuracy)

Sender calculates the phase error by measuring the total round trip-time by sending and receiving the respective response from the receiver (if the latency is large compared to the desired accuracy)

Types of errors that TTS should detect and eliminate

- Send Time Latency
  -time spent at the sender to construct the message
- Access Time Latency
  -time spent at the sender to wait for access to transmit the message
- Prorogation Time Latency
  -time spent by the message in traveling from the sender to the receiver
- Receive Time Latency
  -time spent at the receiver to receive the message from the channel and to notify the host
- Phase error
  -due to nodes' clock that contains different times
- Clock skew
  -due to nodes' clock that run at different rate

Therefore, We go for RBS!!!

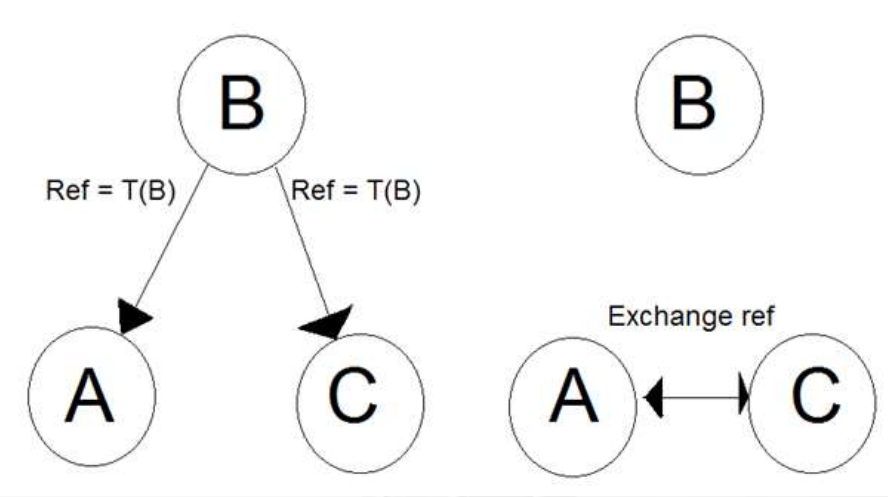
Illustration of TTS

(a) latency is small compared to desired accuracy

(b) latency is large compared to desired accuracy

Concept of RBS – Reference-Broadcast Synchronization

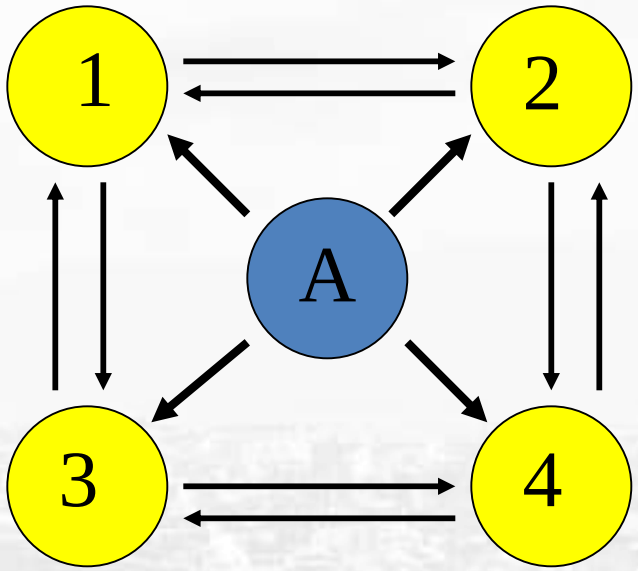
Basic idea to estimate phase offset:



-Transmitter broadcasts a reference packet to two receivers
-Each receiver records the time that the reference was received, according to its local clock
-The receivers exchange their observations

- Reference broadcasts do not have an explicit timestamp
- Receivers use reference broadcast's arrival time as a point of reference for comparing nodes' clocks
- Receivers synchronizes with one another using the message's timestamp (which is different from one receiver to another)

Reference-Broadcast Synchronization



Key idea of RBS: in the wireless medium, broadcast messages will arrive at receivers at approximately the same time, set of receivers synchronize with each other using a broadcast message variability in message delay dominated by propagation delay and time needed to receive and process incoming message (*send delay and access delay are identical*) RBS critical path is short than critical path of traditional techniques

Advantages of RBS

- Can be used without external timescales
- Energy conservative
- Does not require tight coupling between sender and its network interface
- Covers much wider area
- Applicable in both wired and wireless networks
- Largest resources of latency (that exists in TTS) is removed from critical path
- Allows tighter synchronization

How RBS is energy conservative?

- Nodes stay in sleep mode until an event of interest occurs – post-facto synchronization

RBS vs TTS

RBS - Synchronizes a set of receivers with one another

Traditional - Senders synchronizes with receivers

RBS – Supports both single hop and multi hop networks

Traditional – mostly supports only single hop networks

Limitations of RBS

Works only with broadband communication
Does not support point to point communication
(as time synchronization is done among a set of receivers.
In point-to-point – only one receiver exists)

Applications

Acoustic Motes: Acoustic Ranging implemented in Berkeley Motes
Collaborative Signal Detection

LoRa WANs, RFID Technologies

IOT Technologies: LoRa

LoRa (Long Range)
Low Power Wide Area Networks (LP-WAN)

IoT Definition

The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction using IP connectivity.

"Everything that can be connected will be connected"

IoT-Definition

Interconnection of computing devices via internet.
For the objects (things), enabling them to send and receive the data.

Note: IoT is not owned by specific engineering branch,
Uses multiple domains and technologies.

What is IoT?

The **Internet of Things (IoT)** is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data

- IoT is a conceptual framework
- It's about enabling connectivity and embedded intelligence in devices
- Some of these devices are connected today, but **MANY** are not…
- Not strictly machine-to-machine (M2M) – also machine-to-people, people-to-machine, machine-to-objects, people-to-objects
- Creates the ability to collect data from a broad range of devices
- Data can be accessed via the cloud and analyzed using "big data" techniques

What is IoT?

- Internet of Things (IoT) comprises things that have unique identities and are connected to the Internet

- The focus on IoT is in the configuration, control and networking via the Internet of devices or “Things” that are traditionally not associated with the internet
  - Eg: pump, utility meter, car engine

- IoT is a new revolution in the capabilities of the endpoints that are connected to the internet

What is IoT?

- The Scope of IoT is not limited to just connecting things (device, appliances, machines) to the Internet
- IoT allows these things to communicate and exchange data (control& information)
- Processing on these data will provide us various applications towards a common user or machine goal

Internet of Things

What are ‘THINGS’ in IoT?

Humans

Smart Devices

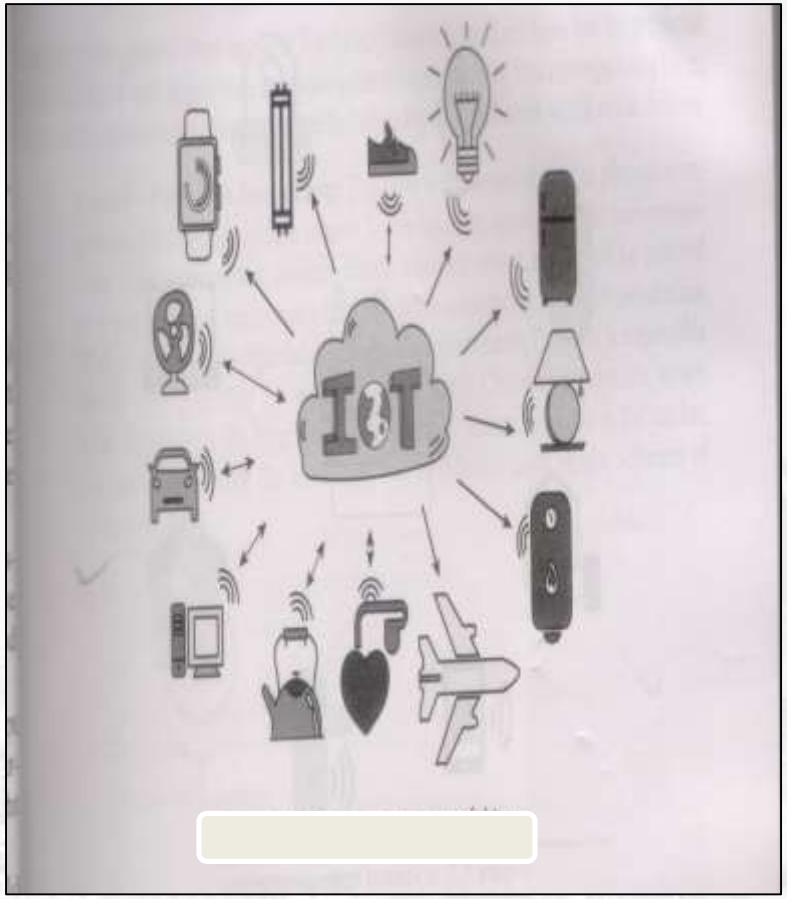
Computers

Animals

Automobiles

Buildings

Any natural or man-made Objects…

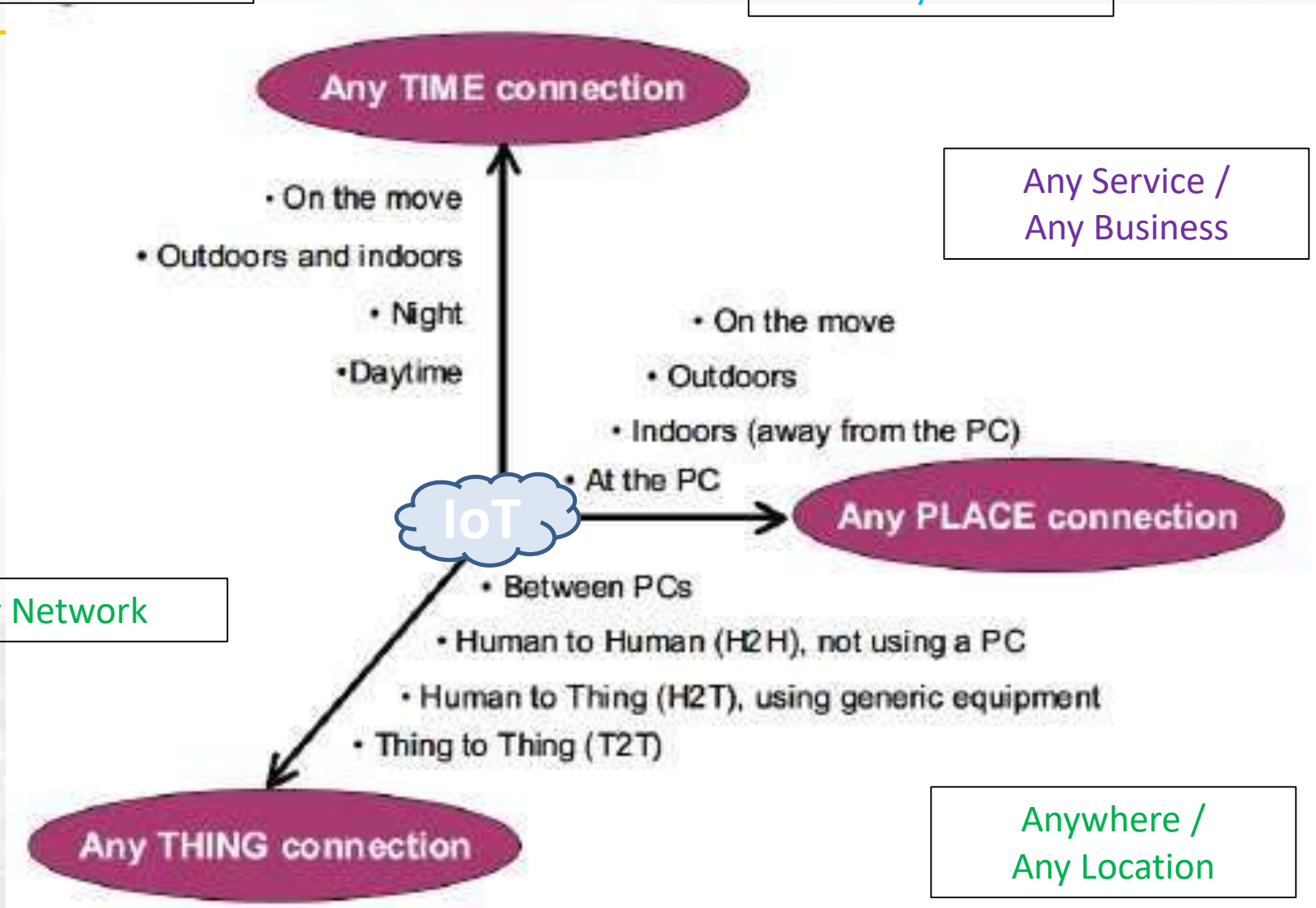


Things = Hardware + Software + Service

Design Goals

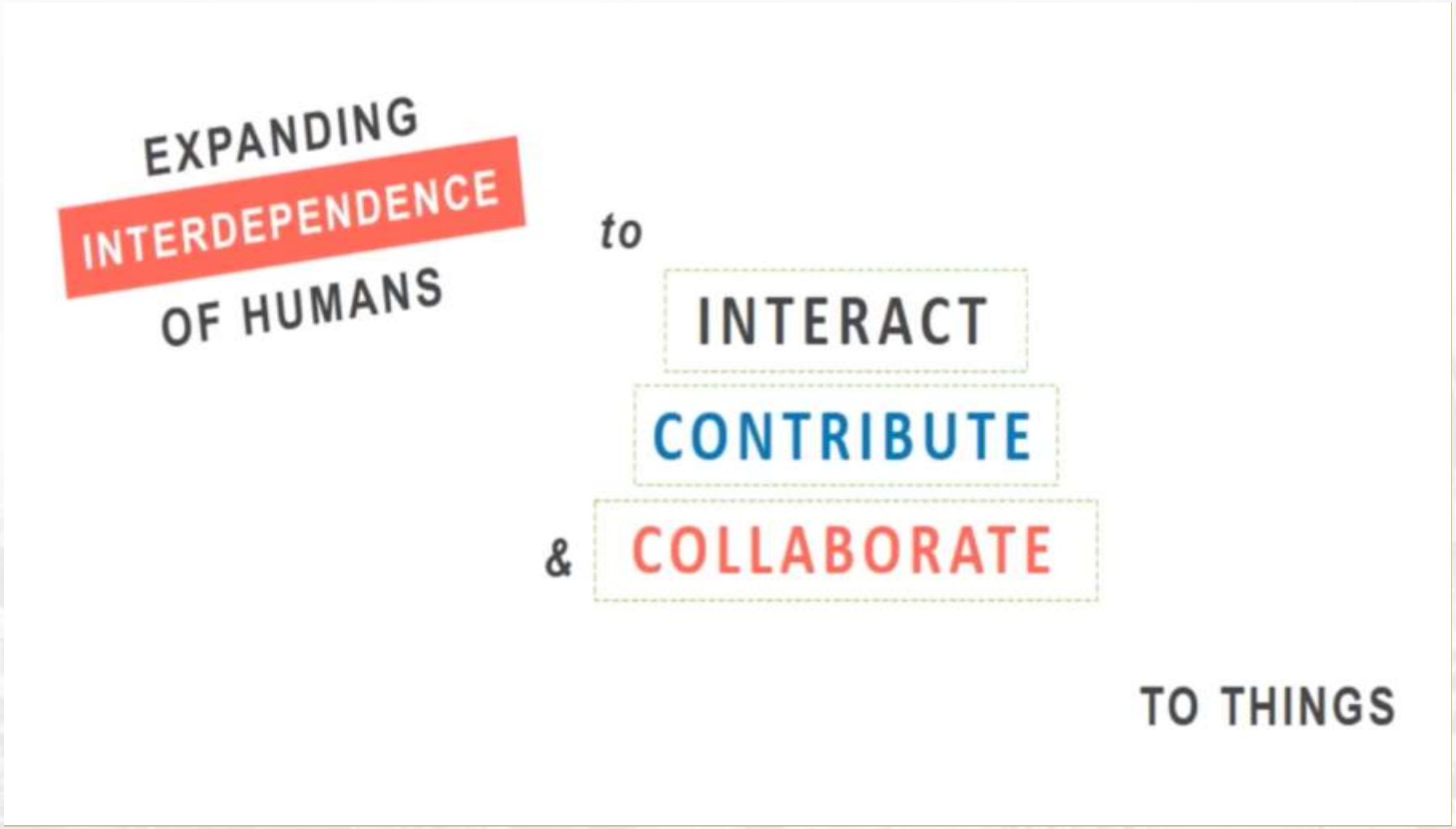
Anytime-Any Device

Anyone



Source: ITU adapted from Nomura Research Institute

Why do we need IoT?

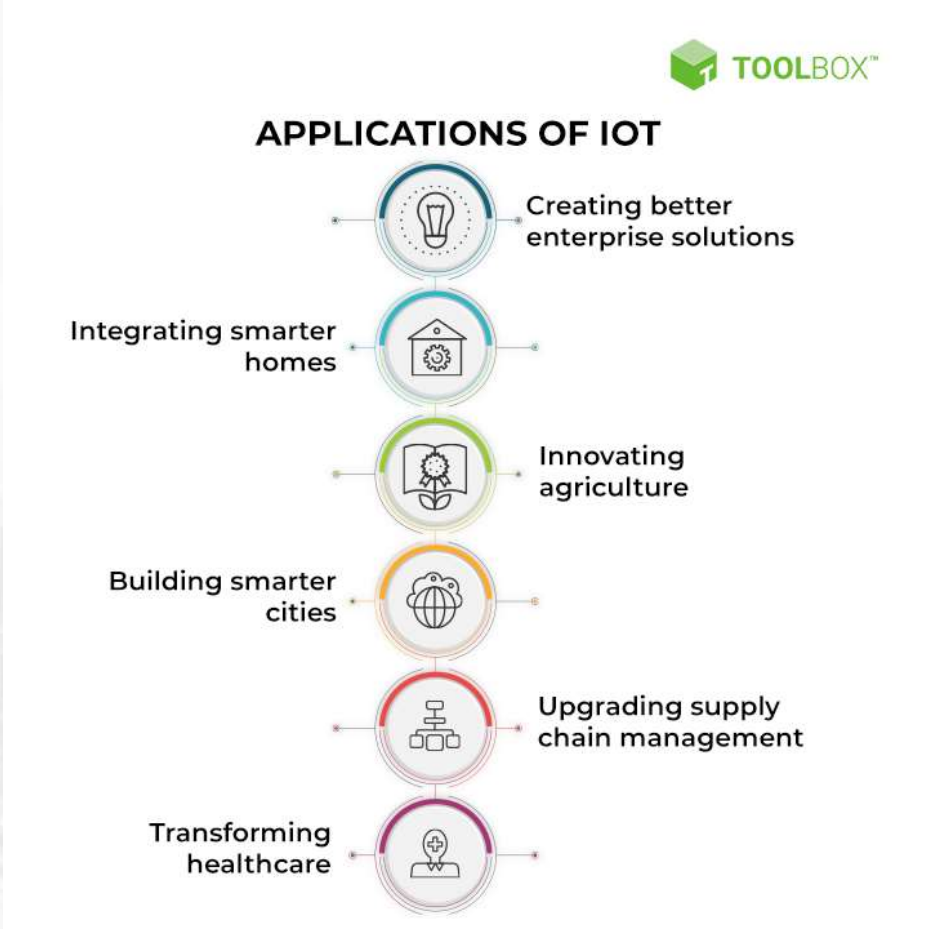


Benefits of IoT

- Efficient resource Utilization.
- Minimizing Human efforts
- Save Time.
- Development of AI through IoT.
- Improved Security …….

Applications of IoT

Connectivity
Intelligence and Identity
Scalability
Dynamic and Self Adapting
Architecture
Safety



IoT technologies

Wired	WPAN	W-Mesh	WLAN	WWAN
• Ethernet, Coax, Fiber, etc. considered as a single category	• ANT+ • *Bluetooth* ® – Classic & Smart Ready • *Bluetooth* ® Smart	• ZigBee PRO • ZigBee RF4CE • ZigBee Multi-Protocol • EnOcean • ISA100.11a • WirelessHART • Z-Wave • Other 802.15.4	• 802.11a/b/g • 802.11n • 802.11ac • 802.11ad • Other 802.11 • DECT ULE • Other 2.4GHz • Other Sub-GHz	• 2G Cellular • 3G Cellular • 4G Cellular

IOT Networking

- Range
- Data rate
- Traffic pattern
- Power
- Mobility
- Number of devices
- Price
- Security
- Coverage
- Spectrum

Block diagram of an IoT Device

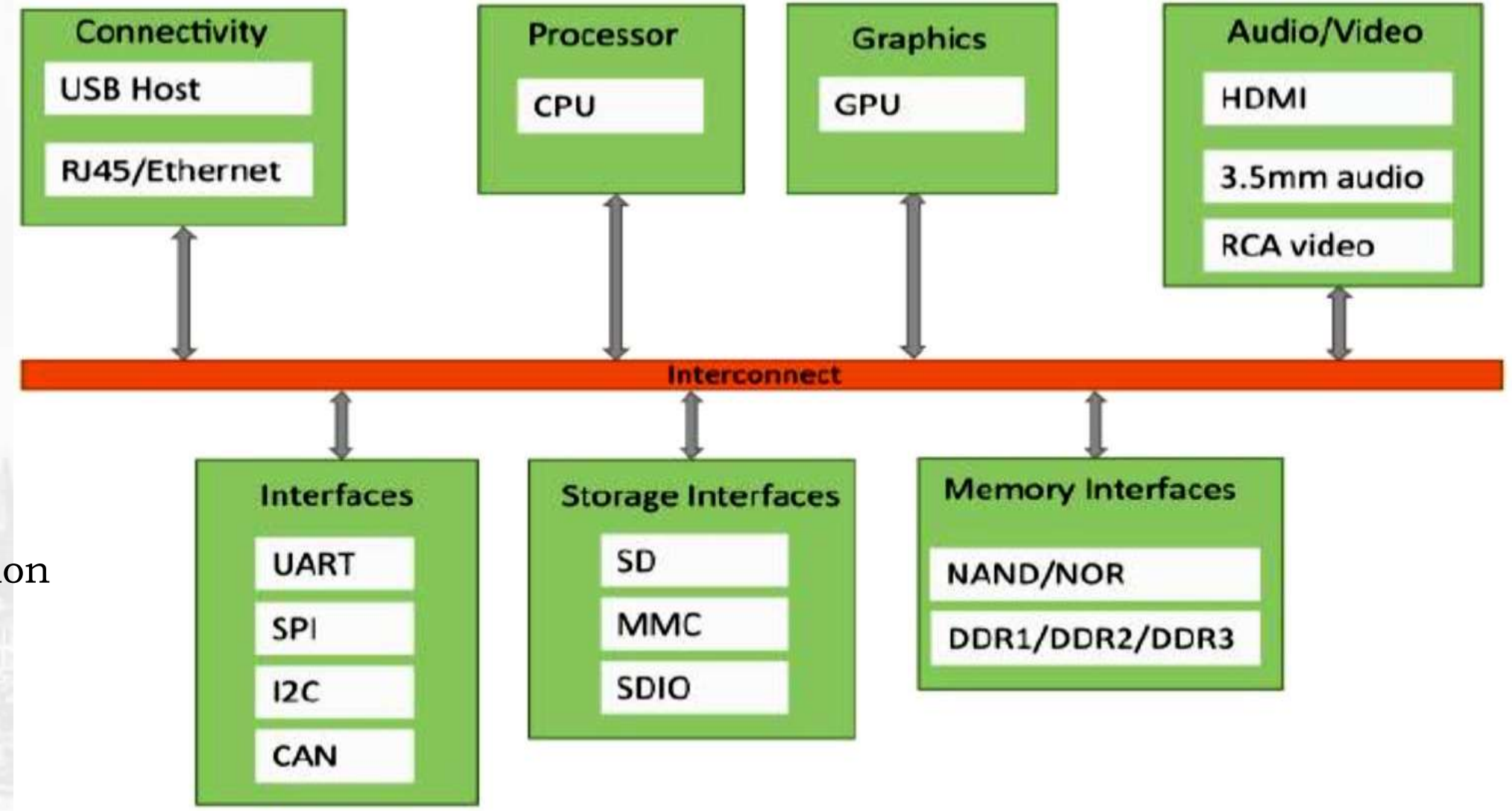
Functional attributes

Sensing

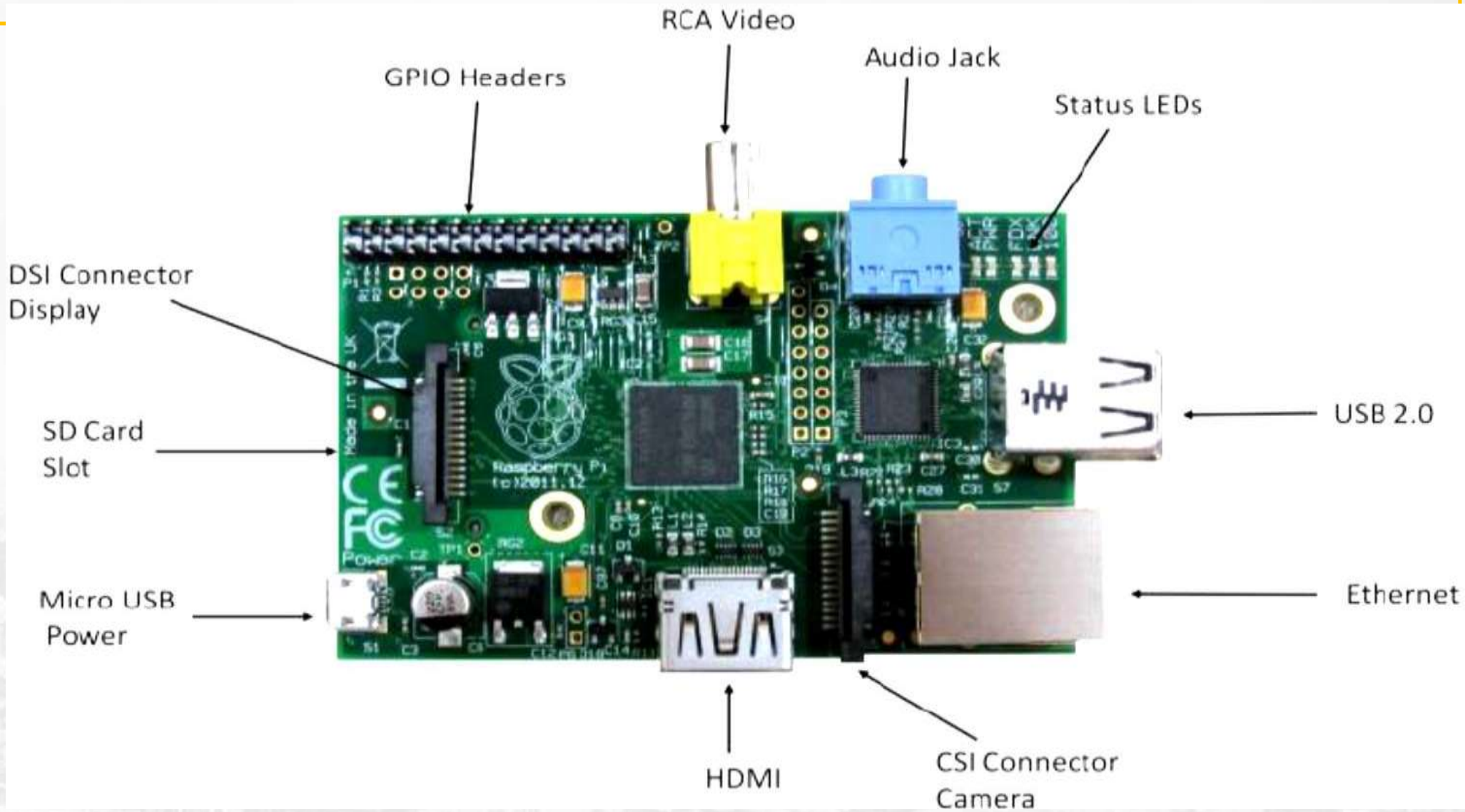
Actuation

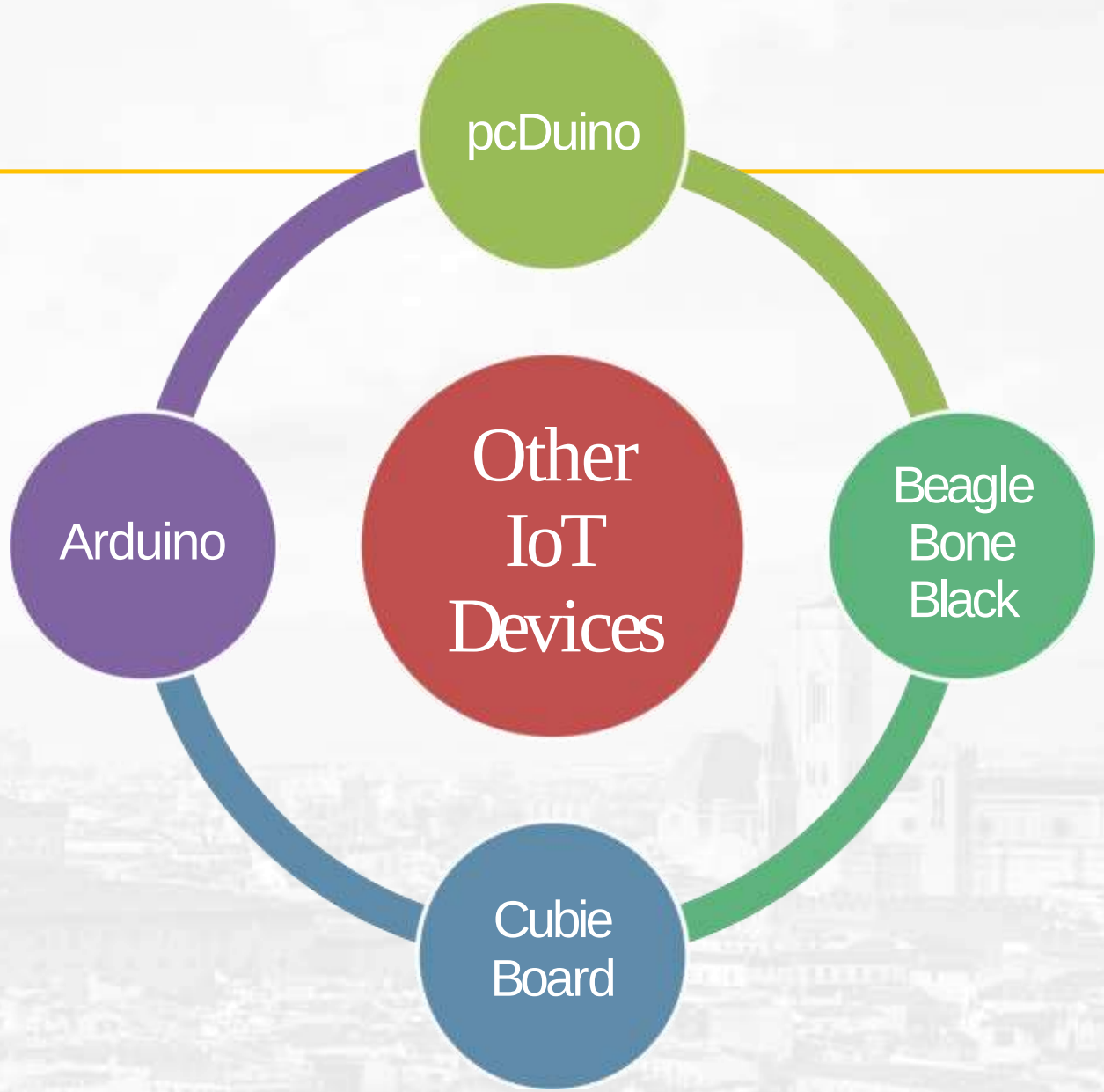
Analysis & Processing

Communication



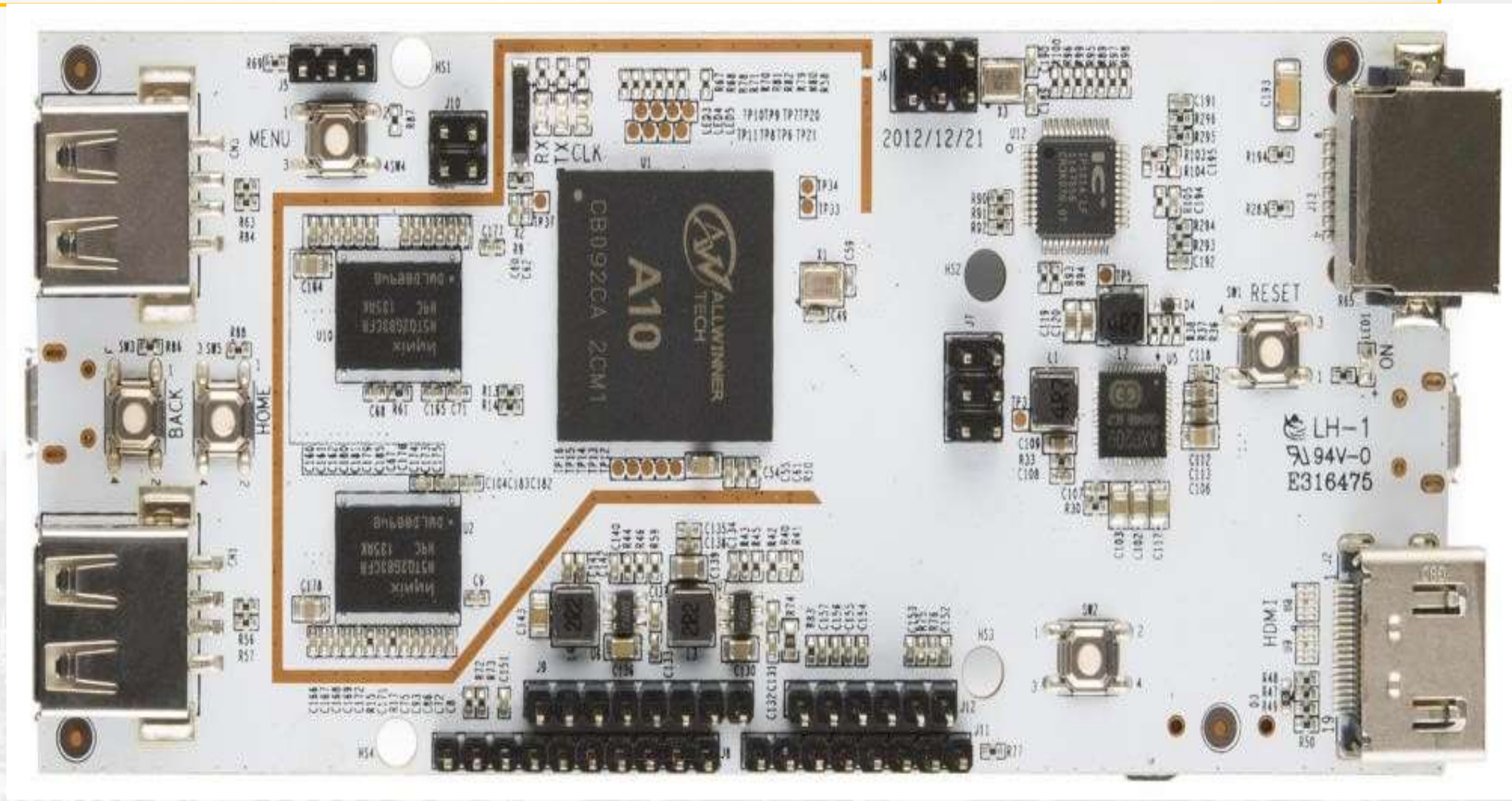
Raspberry Pi




pcDuino
Beagle Bone Black
Cubie Board
Arduino
Other IoT Devices

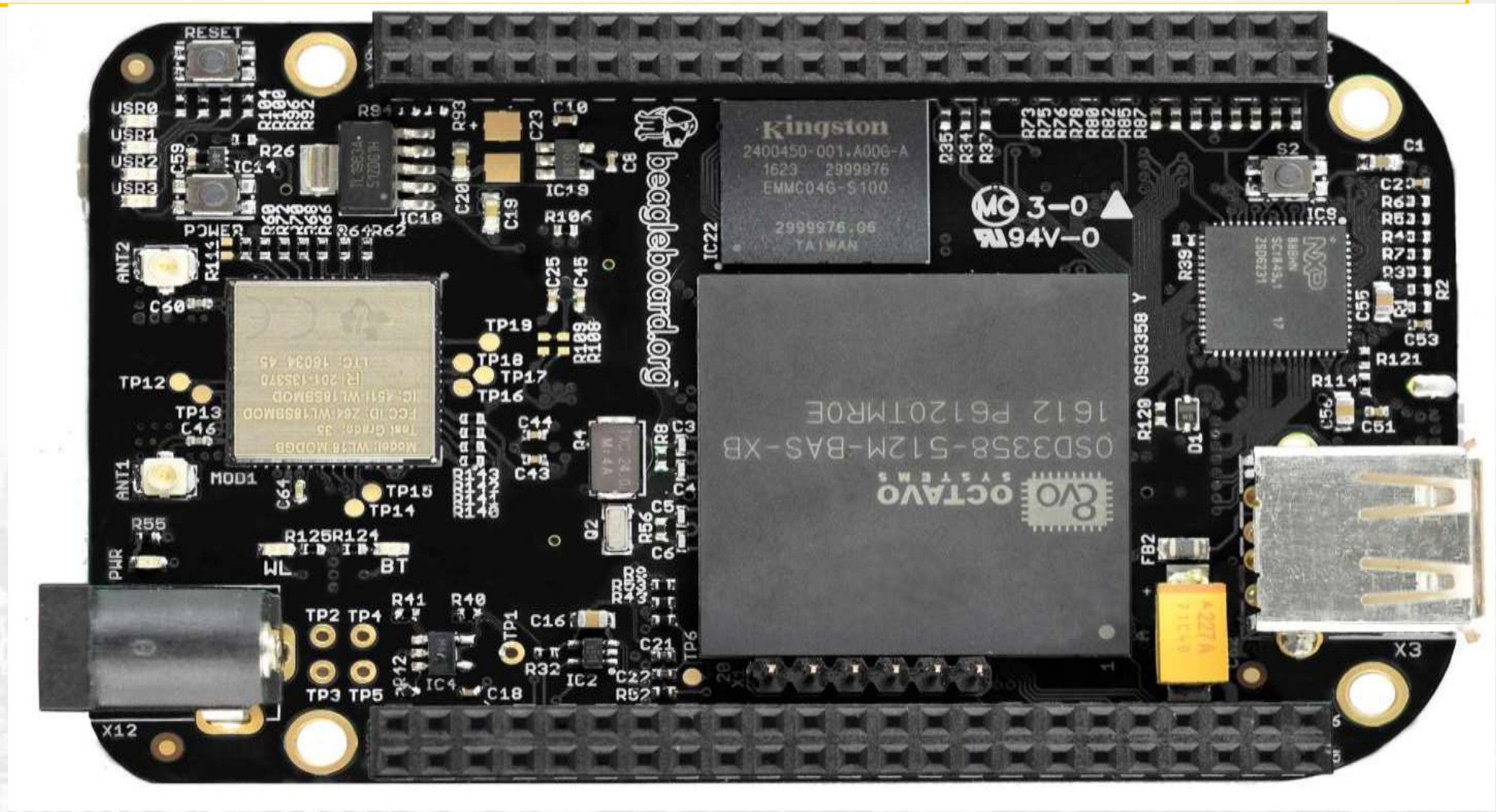
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

pcDuino



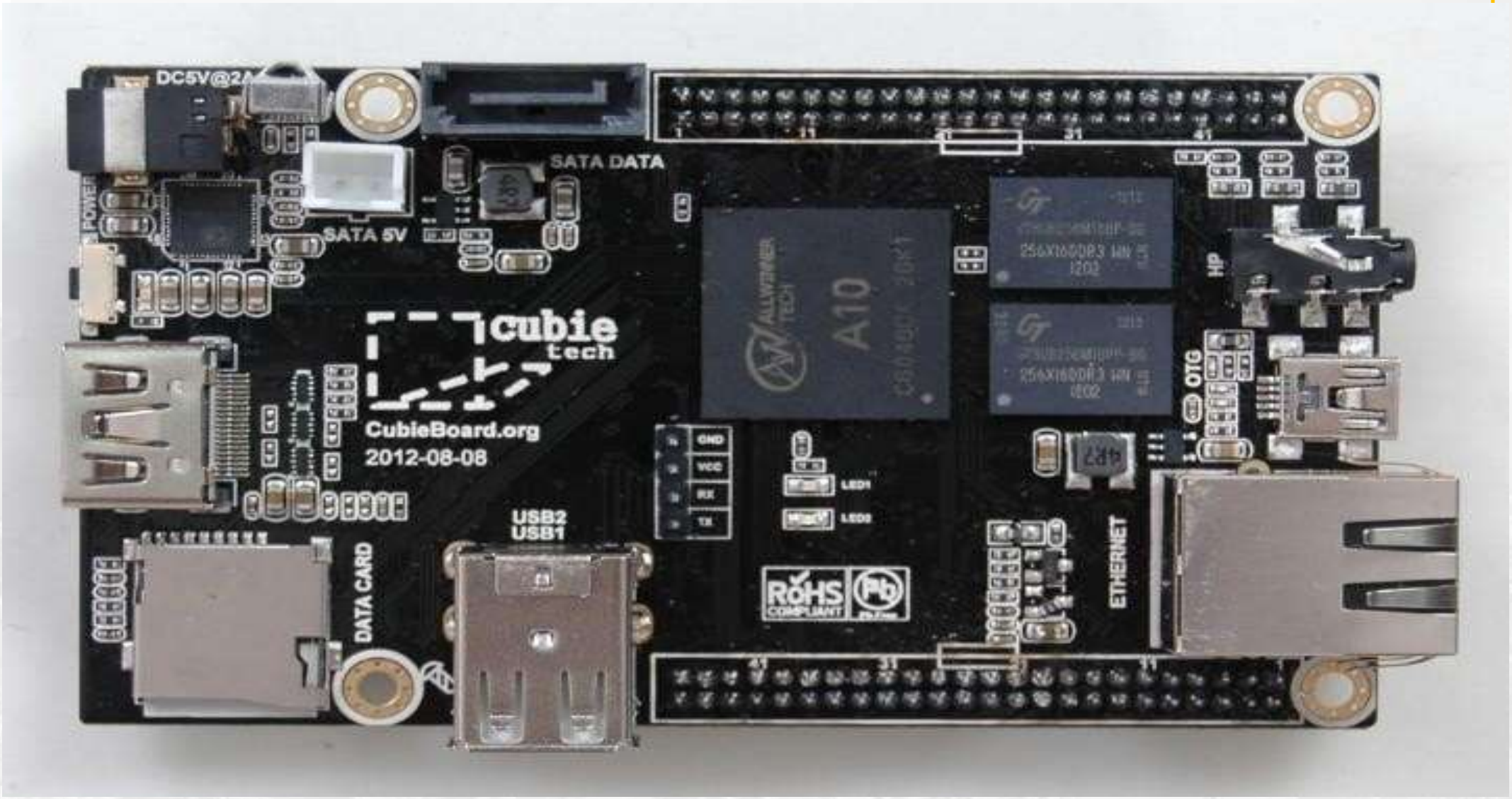
MIT-WPU
॥ विश्वशान्तिर्युवं ध्रुवा ॥

Beagle Bone Black



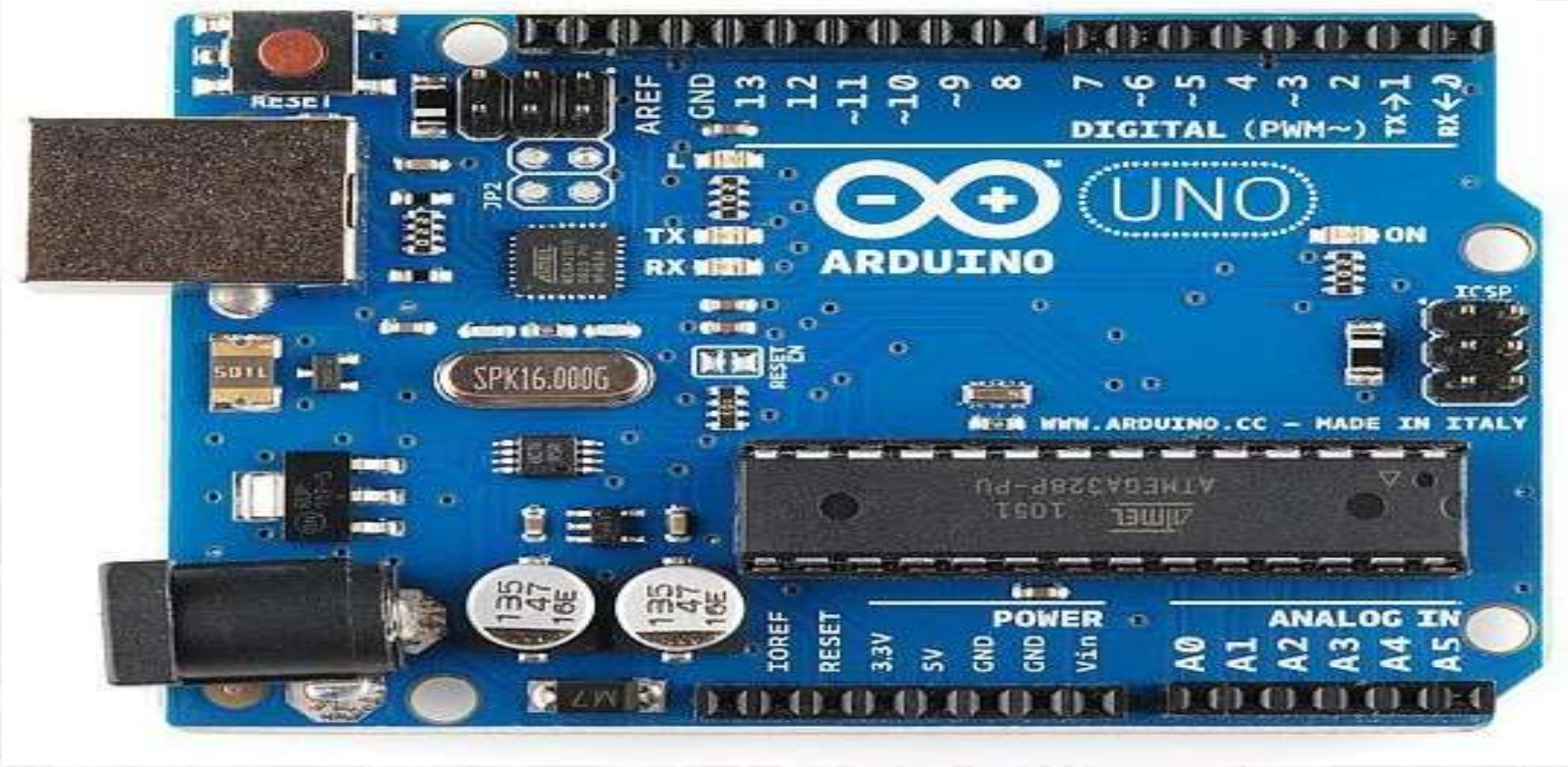
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Cubie Board

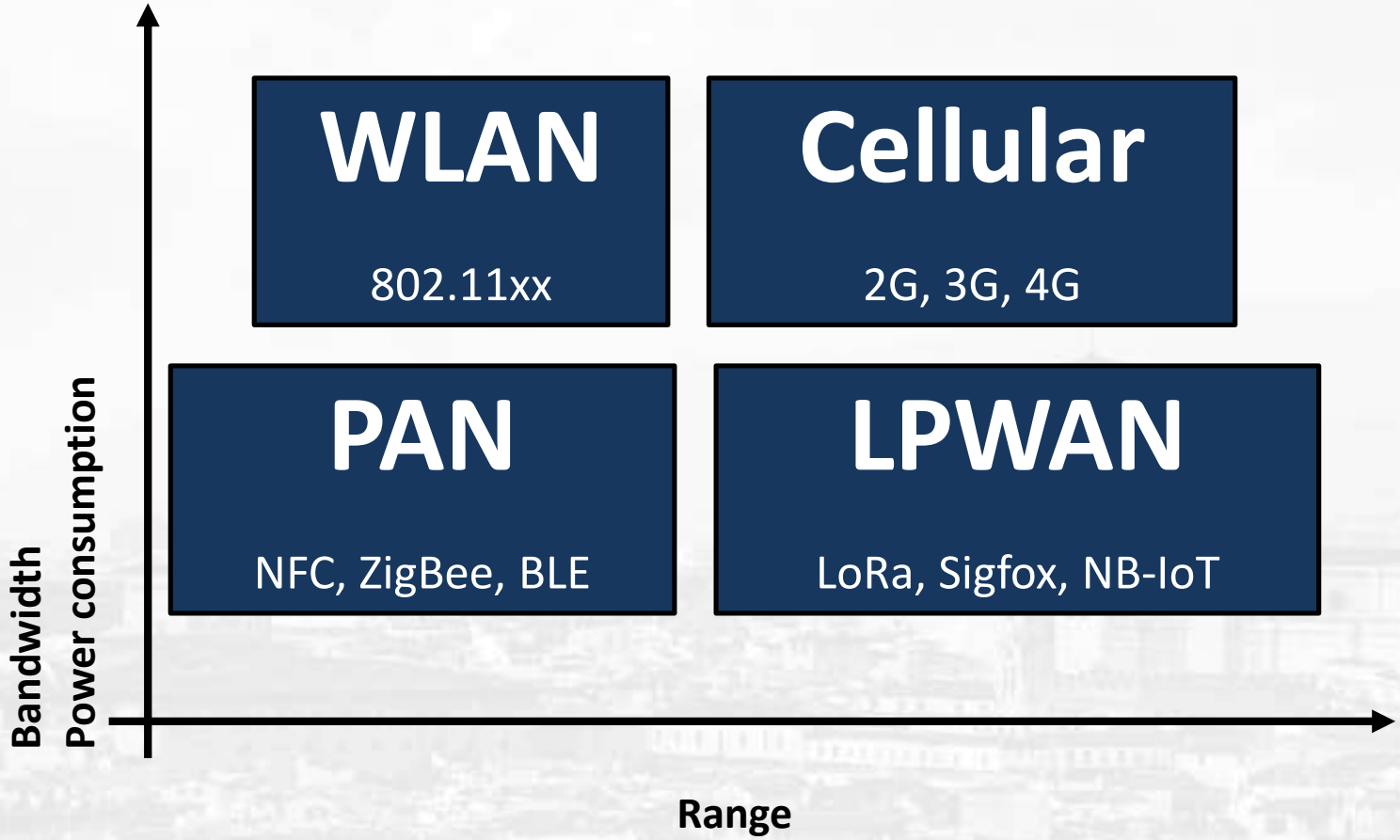


MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

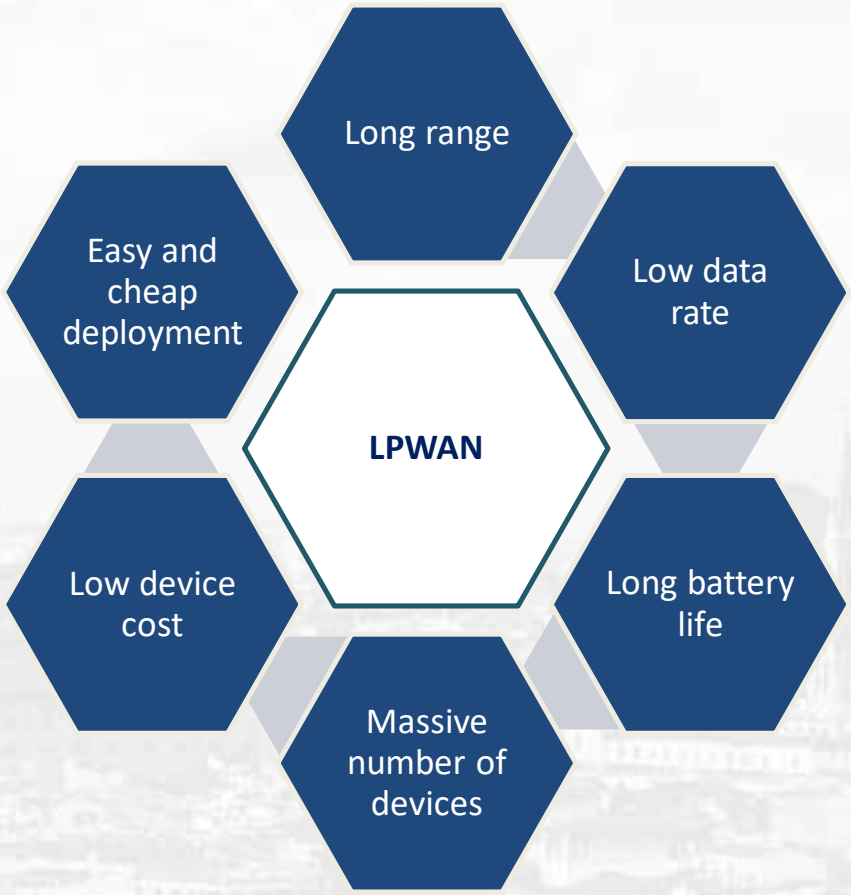
Arduino



IoT Networking



LPWAN


Long range
Low data rate
Long battery life
Massive number of devices
Low device cost
Easy and cheap deployment
LPWAN

Low Power Wide Area Networks: Fundamentals

Centralized Control
+
Minimal Signaling
Simple Devices
Energy Efficient
PHYALOHA-Based Medium Access
Reachability
Low Data Rate
Low Receiver Sensitivity
Reliability
Simple FEC Optional Retransmissions
Any Complexity at Basestation
Data Link Layer
Physical Layer

LoRaWAN

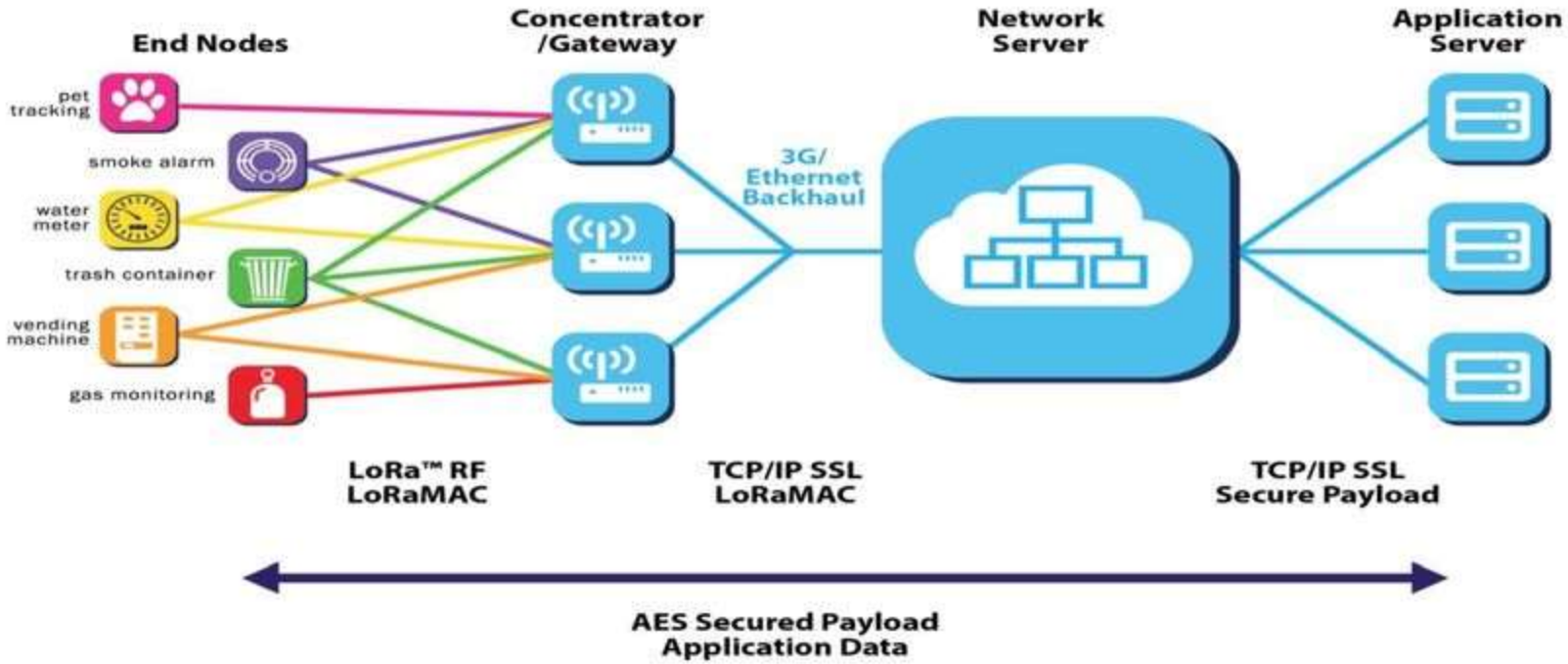
- Media access control (MAC) protocol for wide area networks
- Designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections
- Can be mapped to the second and third layer of the OSI model

LoRa is one of the most popular LPWANs

MIT-WPU
॥ विश्वशान्तिर्पुयं ध्रुवा ॥

LoRa

LoRa Network Protocol: Topology



LoRAWAN

- LoRa Alliance (Semtech, Orange, IBM, Cisco… up to 500)
- Mature: several national-wide and private networks deployed
- Unlicensed spectrum: independent of national operators (and borders)
- High sensitivity (-137dBm): indoor coverage
- Datarate between 0.3 and 50 kbps
- Symmetric encryption and authentication using AES
- Downlink capabilities (although primarily uplink)

LoRa Physical layer

- Enables long-range link
- Proprietary modulation technology from Semtech

LoRaWAN Medium Access Control

- Open standard developed by the LoRa Alliance

MIT-WPU
॥ विश्वशान्तिर्भुवं ध्रुवा ॥

LoRa

LoRa Use Cases

LoRa WAN Characteristics

- Long Range
- Greater than cellular
- Deep indoor coverage
- Simple star topology
- Max. Lifetime
- Low power optimized
- Battery lifetime of 10 years
- >10x vs cellular M2M

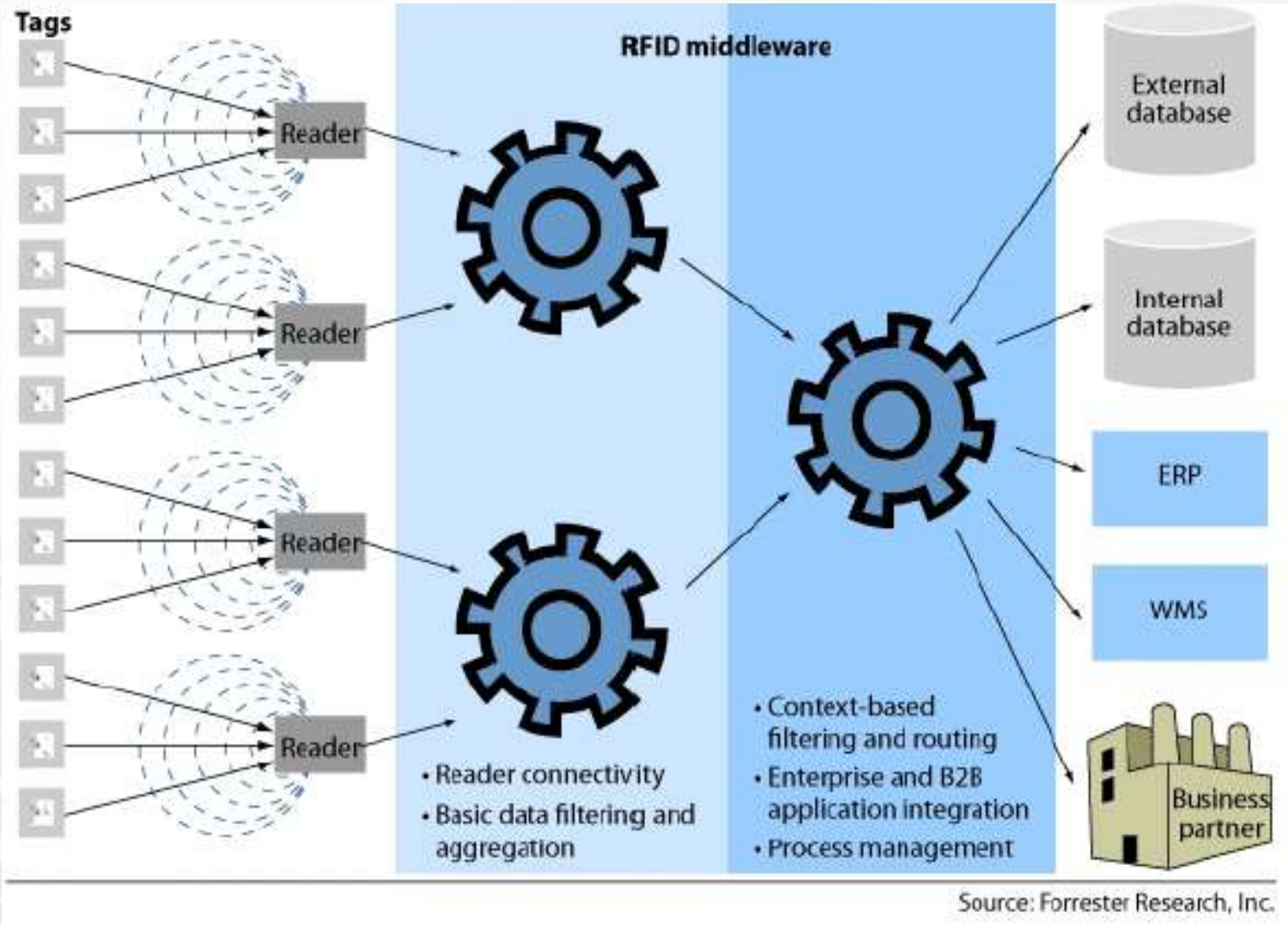
- Low Cost
- Minimal Infrastructure
- Low Cost End Node
- Open SW
- Multi-Usage
- High Capacity
- Multi-tenant
- Public Network

RFID: The Internet of Objects

IoT first used by Kevin Ashton (Co-founder and executive director of the Auto-ID Center, when he was doing research at Massachusetts Institute in 1999

Auto-ID Lab: a research federation in the field of networked RFID and emerging sensing technologies

Typical RFID System



RFID Tag…

- RFID tag is a simplified, low cost, disposable contactless smartcard
- Includes a chip to store a static number (ID) and attributes of the tagged objet and an antenna
- RFID Tags can be active, passive or semi passive
- It tags on an “unintelligent” object like pallet or and animal

Unique Identification of Objects

- Radio Frequency Identification (RFID)

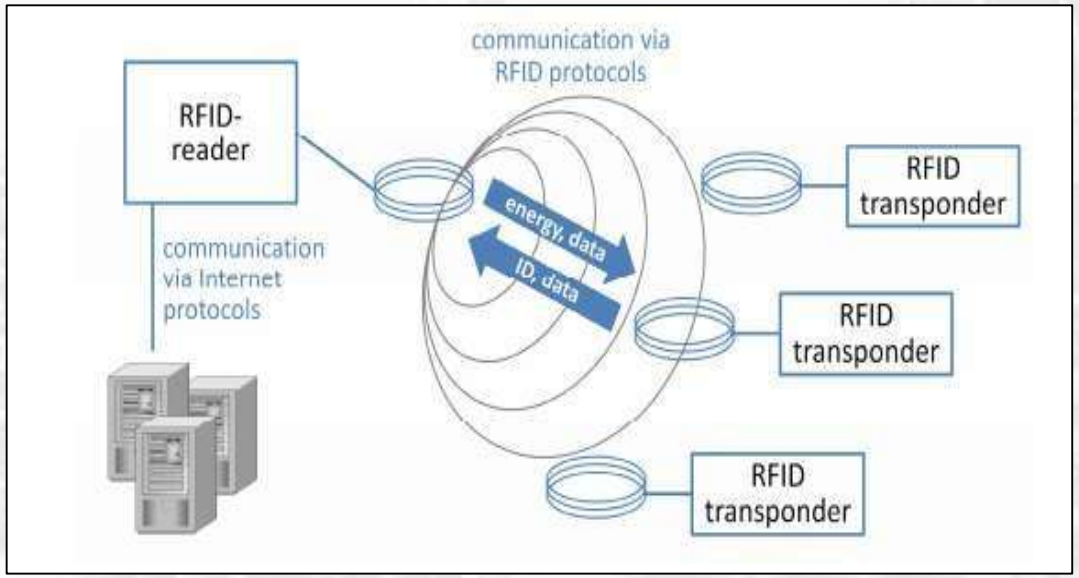
RFID

Passive RFID tags

- No Battery
- Use power of reader's interrogation signal to communicate the ID to reader

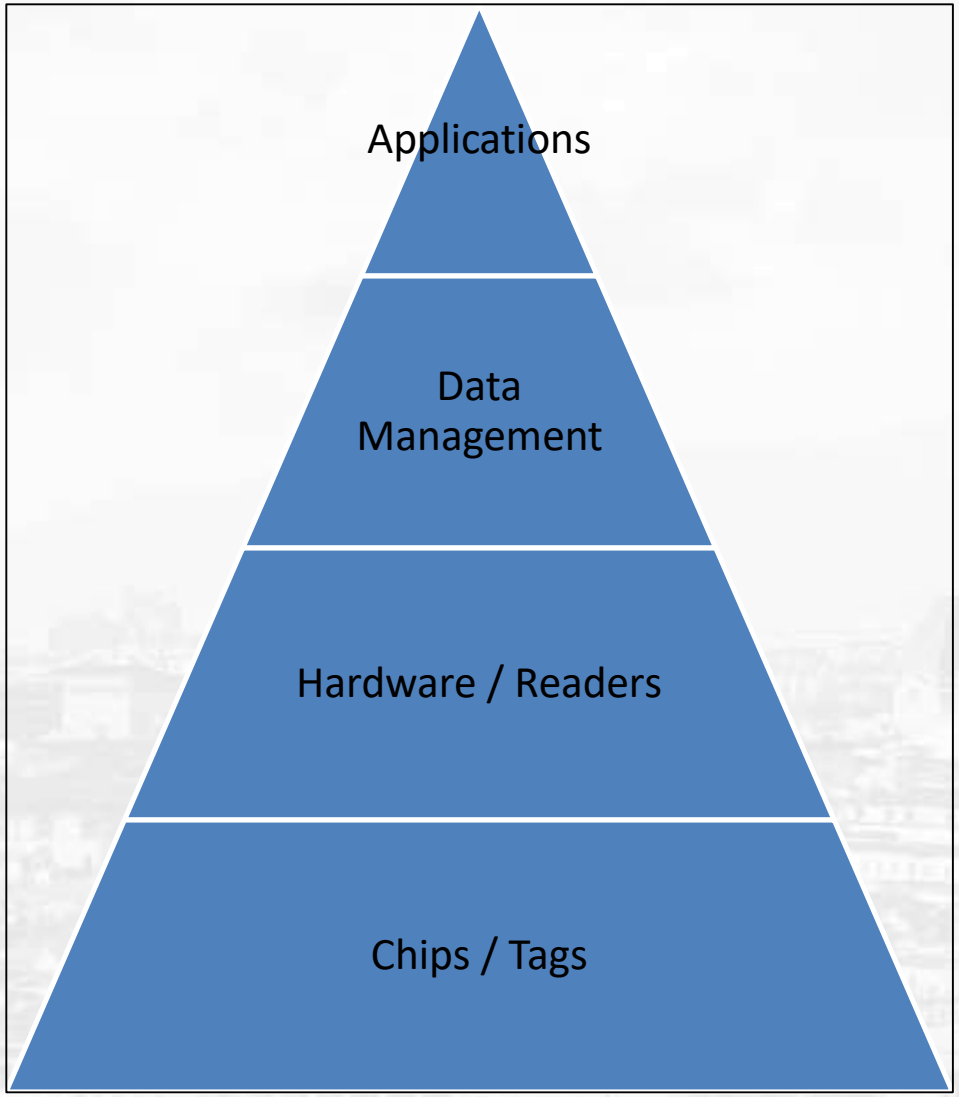
Active RFID tags

- Battery powered tags
- Can instantiate Communication



- Tracking/Identification
  - Library Books
  - Children
  - Pets
  - Auto Parts
- Inventory management in a Supply
- Chain Contactless Smart Cards

RFID value chain & Vendors



Manugistics	
Manhattan Associates	
RedPrairie	
SAP	Microsoft
Oracle	Tibco
ConnecTerra	
DataBrokers	
GlobeRanger	
OAT Systems	
IBM	Savi Technology
Sun	Symbol Tech.
RF Code	SAMSys
Intermec	ThingMagic
Tyco Int.	Philips
Alien Tech.	Semiconductor
Matrics	Texas Instruments
Zebra Tech.	AveryDennison

Thank You!!!

Learning Resources

Text books

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, PHI, ISBN - 9788131706885, 2007.
2. Nekoley Elenkov, “Android Security internals”, No Starch Press, ISBN-10: 1-59327-581-1 ISBN-13: 978-1-59327-581

Reference Books

1. KiaMakki, Peter Reiher, “Mobile and Wireless Network Security and Privacy “, Springer, ISBN 978-0-387-71057-0, 2007.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius , “Wiress and Mobile Networks Security”, Wiley publication, ISBN 978-1-84821-117-9
3. Noureddine Boudriga, “Security of Mobile Communications”, ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010
6. Tim Speed, Darla Nykamp,Mari Heiser,Joseph Anderson,Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover Your Devices", Copyright © 2013 Packt Publishing, ISBN 978-1-84969-360-8

Learning Resources

Web Resources:

i. http://whatis.techtarget.com/definition/mobile-security

ii. http://techgenix.com/security/mobile-wireless-security/

Weblinks

i. https://en.wikipedia.org/wiki/Mobile_security

MOOCs:

i. https://www.ntnu.edu/studies/courses/TTM4137#tab=omEmnet
ii. http://nptel.ac.in/courses/106105160/37
iii. https://www.eccouncil.org/
iv. https://www.csoonline.com/article/2122635/mobile-security/wireless-security--the-basics.html

MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

THANK YOU FOR LISTENING ANY QUESTION?