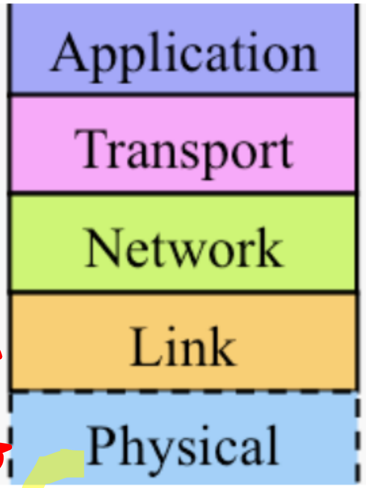
THE TRANSPORT LAYER

TRANSPORT LAYER



The success and efficiency of WSNs directly depend on reliable communication between the sensor nodes and the sink.

In a multi-hop, multi-sensor environment, to accomplish this a reliable transport mechanism is imperative in addition to robust modulation and media access, link error control, and fault-tolerant routing.

The main objectives of a transport layer protocol for WSNs are as follows:

Congestion control: Packet losses due to congestion can impair reliability at the sink even when enough information is sent out by the sources. Hence, congestion control is an important component of the transport layer to achieve the required reliability. Furthermore, congestion control not only increases the network efficiency, but also helps conserve scarce sensor resources.

Reliable transport: Based on the application requirements, the extracted event features should be reliably transferred to the sink. Similarly, the programming/retasking data for sensor operation, command, and queries should be reliably delivered to the target sensor nodes to assure the proper functioning of the WSNs.

(De)multiplexing: Different applications can be served on sensor nodes through the same network. The transport layer should bridge the application and network layers by using multiplexing and demultiplexing.

TRANSPORT LAYER

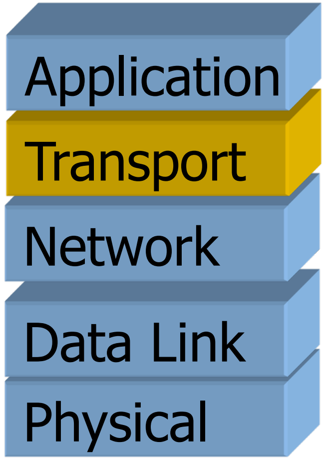
major tasks of the Transport Layer is:

(1) to guarantee the reliable transmission of network packets through end-to-end retransmissions or other strategies, and

(2) to reduce or avoid the network congestion due to too much traffic flowing in the routers or other relay points.

TCP schemes adopted in traditional wireless networks are not suitable for WSNs. In WSNs the concept of end-to-end reliability carries a different context due to the "sensor" nature of the network which, as a result, introduces issues such as:

- Multiple source(sensors), single destination, the sink, which creates a reverse multicast type of data flow

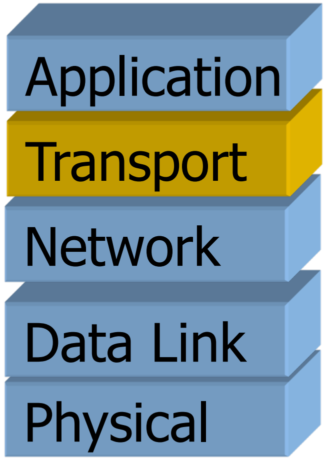


TRANSPORT LAYER

- For the same event there is high level of redundancy or correlation in the data collected by the sensors and thus there is no need for end-to-end reliability between individual sensors and the sink but instead between the event and the sink

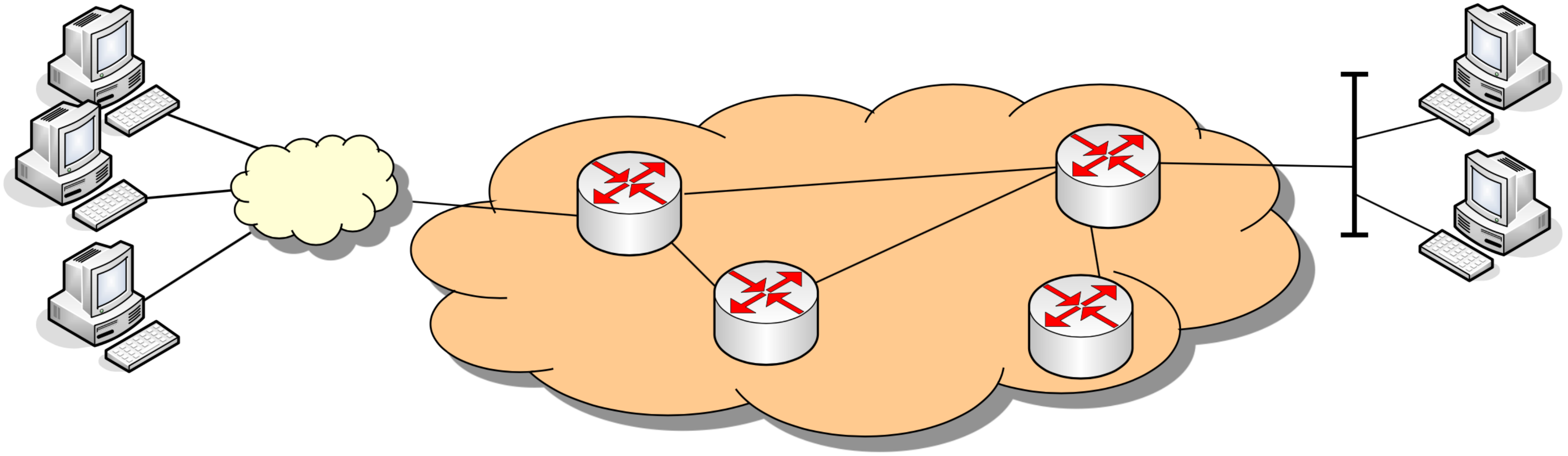
- On the other hand there is need for end-to-end reliability between the sink and individual nodes for situations such as re-tasking or reprogramming

- The protocols developed should be energy aware and simple enough to be implemented in the low-end type of hardware and software of many WSN applications



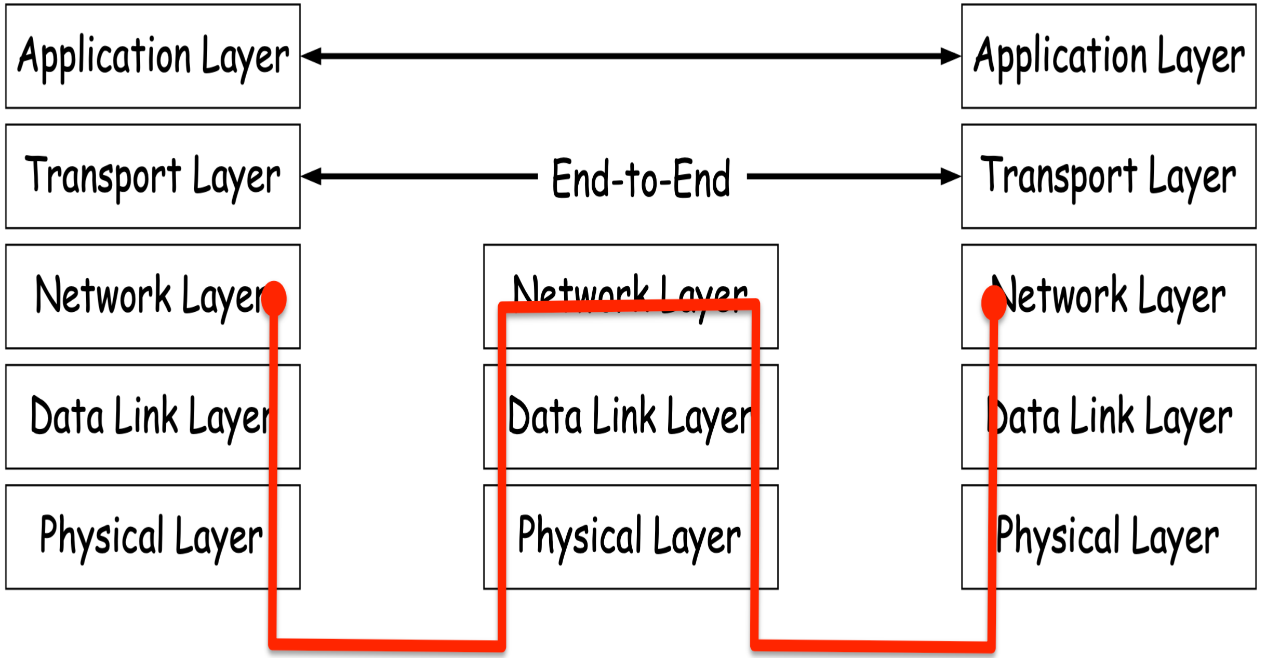
IN SUMMARY

- Transport protocols are used to …
  - orderly transmission
  - eliminate or mitigate congestion
  - reduce packet loss
  - provide fairness in bandwidth allocation
  - guarantee end-to-end reliability



SUMMARY

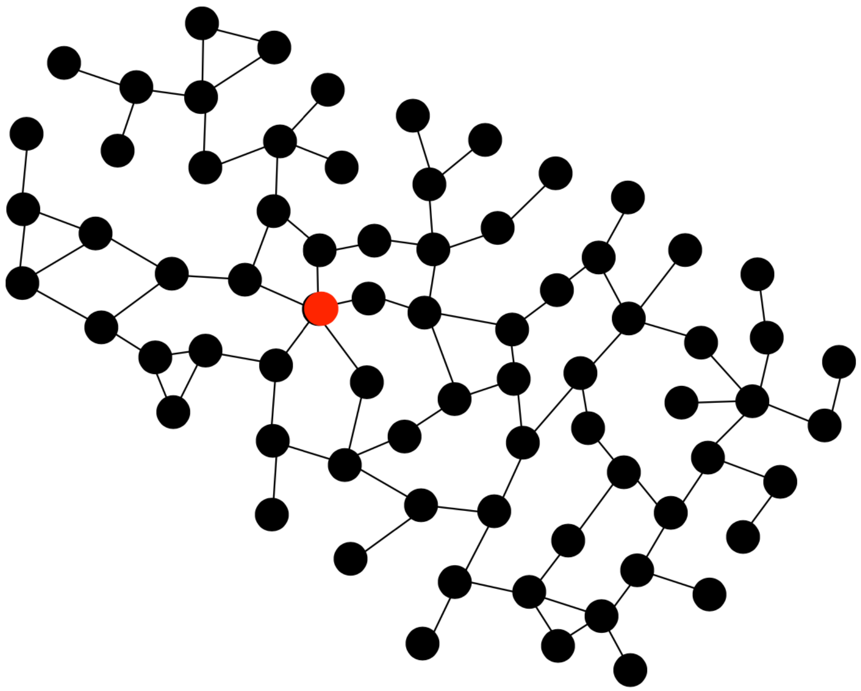
- Transport protocols are used to ...
  - orderly transmission
  - eliminate or mitigate congestion
  - reduce packet loss
  - provide fairness in bandwidth allocation
  - guarantee end-to-end reliability



DISTINCT FEATURES OF WSNS

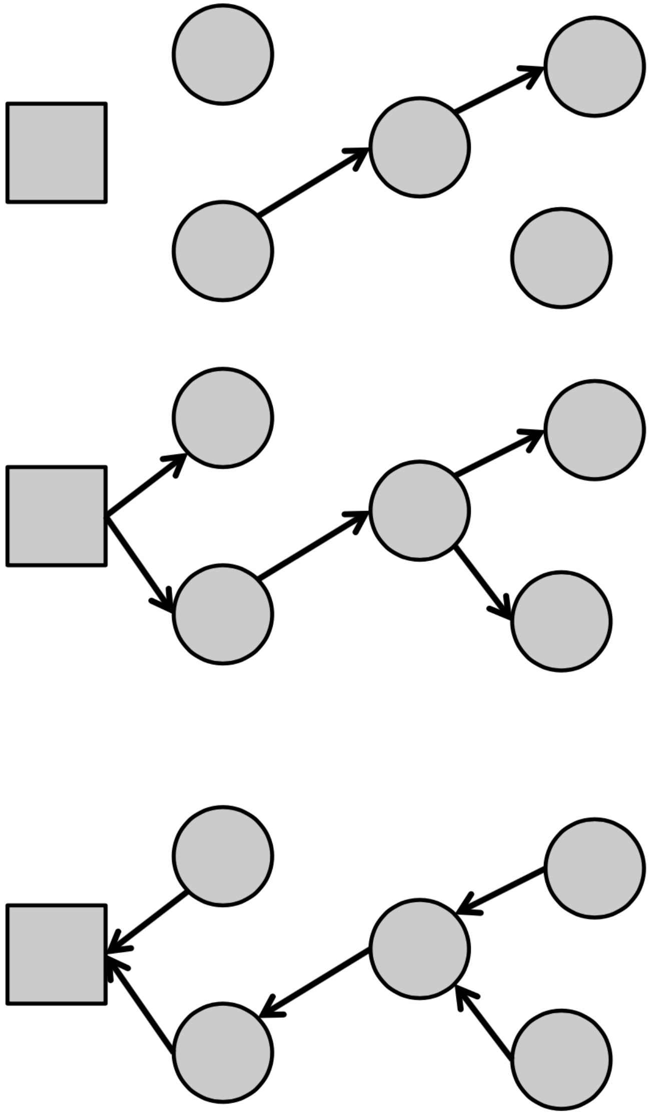
Topology

- multi-hop star topology
- Diverse applications
- event-driven
- continuous delivery
- query-driven delivery • hybrid delivery
- Traffic characteristic
- Mainly from sensors to sink -> MP2P
- Resource constraint
- Limited resources (CPU, Memory, Bandwidth, ...)
- Small message size
- No segmentation of messages



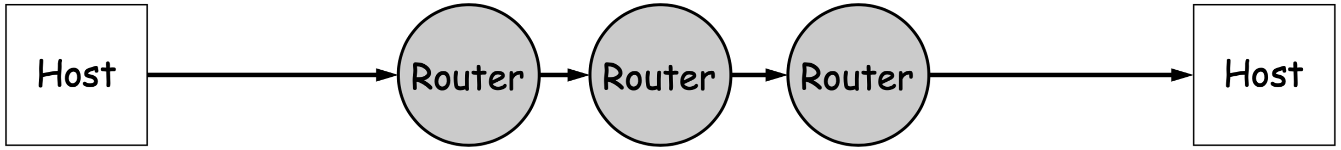
TYPICAL TRAFFIC STRUCTURE

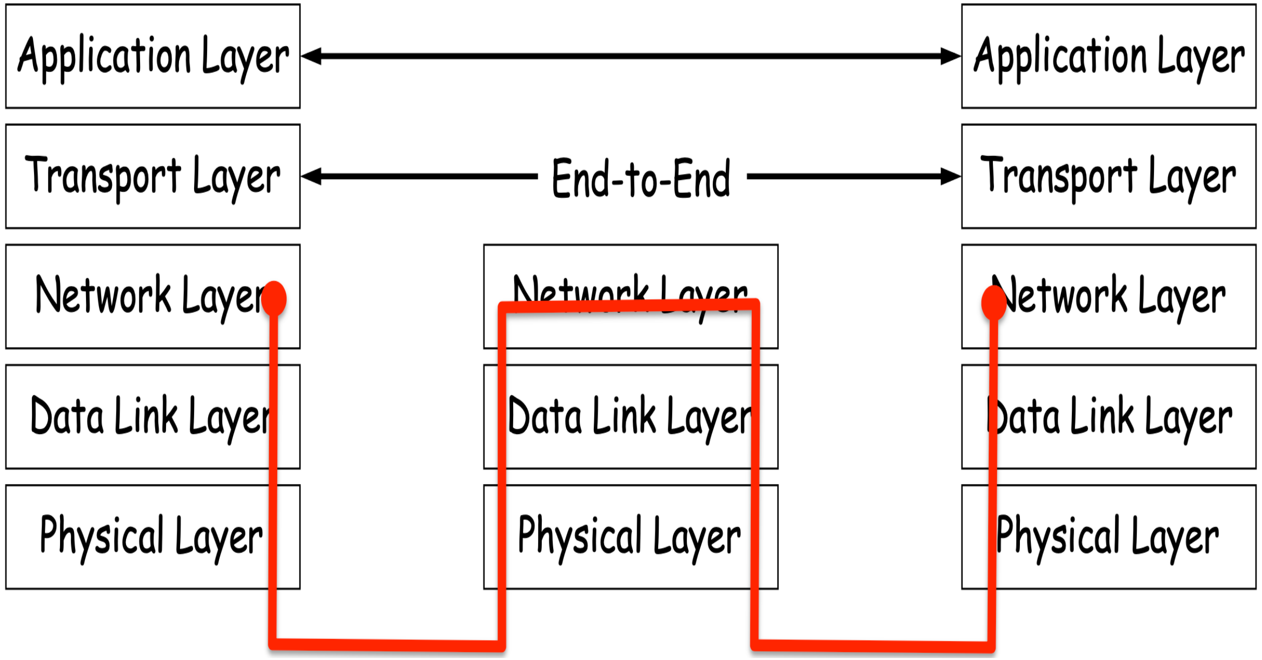
- Sensor -> Actor
  - Unicast
  - Challenge: Reliability
- Sink -> Sensor/Actor
  - Data
    - Control and signaling
    - Code update -> reprogramming
  - Multicast/Broadcast
  - Challenge: Reliability
- Sensor -> Sink
  - Data
    - Sensor measurements/events
  - Concast
  - Challenge: Reliability + Congestions



DESIGN CRITERIA FOR TRANSPORT PROTOCOLS

- Performance metrics
- Congestion control
- Loss recovery





PERFORMANCE METRICS

- Energy efficiency -> maximize system lifetime
- Reliability
  - Packet reliability -> consider every packet
  - Event reliability -> not all packets need reliability, but the event
- QoS metrics -> as in traditional networks
  - Bandwidth
  - Delay
  - Packet loss rate
- Fairness -> distance of the nodes to sink

CONGESTION CONTROL

- Two main causes for congestion
  - Packet arrival rate exceeding packet service rate • More likely at nodes close to the sink
  - Link level performance such as contention, interference and bit error
- Three methods involved
  - Congestion detection
  - Congestion notification
  - Rate adjustment

CONGESTION CONTROL

Congestion detection

- queue length
- packet service time
- ratio between packet service time and packet inter-arrival time at an intermediate node

- channel loading
- Congestion notification -> inform the nodes
  - explicit notification
  - implicit notification
- Rate adjustment
  - Nodes adjust their traffic sending rate
  - AIMD (Additive Increase Multiplicative Decrease) schemes

LOSS RECOVERY

- Loss detection and notification
  - Usual approach -> sequence numbers
  - End-to-end -> like in TCP
  - Hop-by-hop -> receiver based or sender based
- Retransmission-based loss recovery
  - End-to-end -> like in TCP, expensive
  - Hop-by-hop -> nodes need to cache
    - Energy efficient

TRANSPORT LAYER TECHNIQUES

Pump Slowly, Fetch Quickly (PFSQ) – introduced to distribute data from a source node by injecting packets into the network at relatively low speed (pump slowly). This allows nodes that experience data loss to aggressively recover missing data from their neighbors (fetch quickly). Goals of this protocols are:

- ❑Ensure that all data segments are delivered to the intended destinations with minimum especial requirements on the nature of the lower layers
- ❑Minimize number of transmissions to recover lost information
- ❑Operate correctly even in situations where the quality of the wireless links is very poor
- ❑Provide loose delay bounds for data delivery to all intended receivers

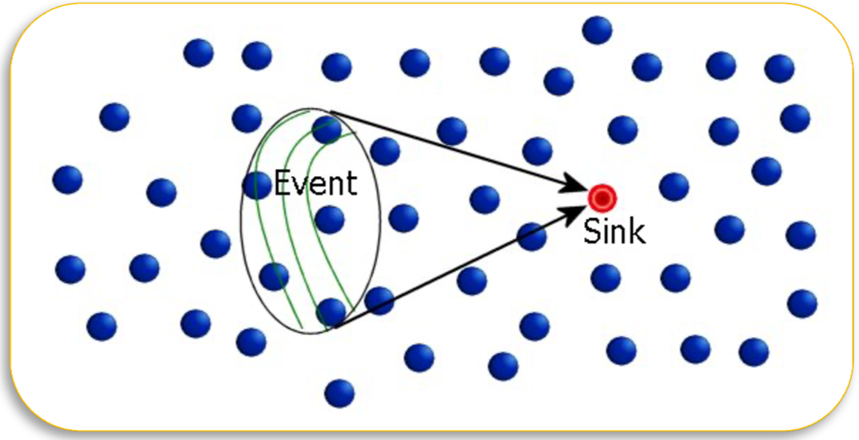
TRANSPORT LAYER TECHNIQUES

PFSQ aims to guarantee sensor-to-sensor delivery and to provide end-to-end reliability for control management distribution from the control node (sink) to the sensors. It does not address congestion control

TRANSPORT LAYER TECHNIQUES

Event-to-Sink Reliable Transport (ESRT) – aims to achieve reliable event detection (at the sink node) based on a protocol that is energy aware and which can control congestion. Important features include:

- Self-configuration – even in the case of a dynamic topology
- Energy awareness – sensor nodes are notified to decrease their frequency of reporting if the reliability level at the sink node are above the minimum



TRANSPORT LAYER TECHNIQUES

- Congestion control – takes advantage of the high level of correlation between the data flows corresponding to the same event
- Collective identification – sink only interested in the collective information from a group of sensors not in their individual reports
- Biased implementation – most of the complexity of the protocol falls on the sink node minimizing the requirements on the sensor nodes

Summary: TCP

- Why not TCP?
  - TCP is unable to distinguish between congestion losses and transmission losses -> poor performance
  - TCP is not suitable for wireless multi-hop
  - TCP provides 100% reliability -> not required by many applications
  - TCP is connection-oriented -> expensive and not necessary
  - TCP depends on network-wide unique addresses of nodes
  - Preprocessing or aggregation of data in intermediate nodes is desirable and often necessary
    - Packets can be combined or changed before they reach destination
  - TCP is not light-weight -> too much overhead

- Why not UDP?
  - No reliability at all

Challenges for the Transport Layer in WSNs

- Reliability
- Congestion Control
- Self-configuration
  - Adaptive to dynamic topologies caused by node mobility/failure/ temporary power-down, and random node deployment
- Energy Awareness
- Biased Implementation
  - Mainly run on the sink with minimum functionalities at sensor nodes
- Constrained Routing/Addressing
  - No assumption of the existence of an end-to-end global addressing