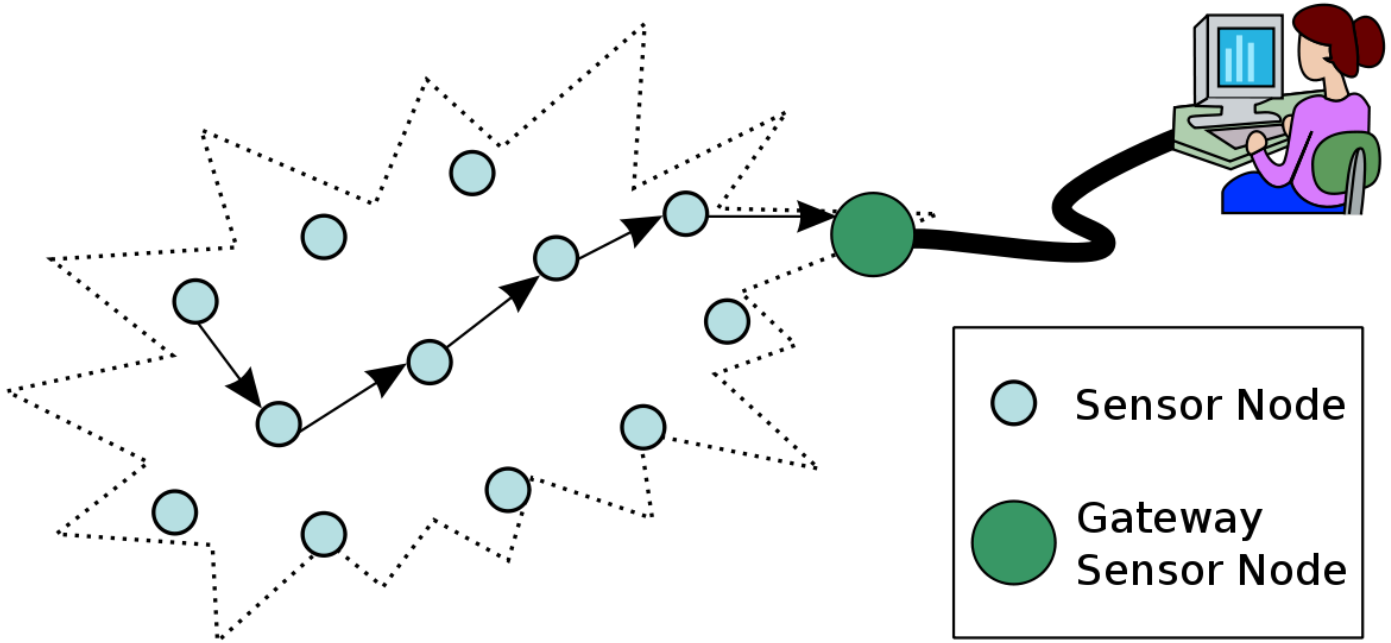
# Wireless Sensor Networks




By John A. Stankovic
University of Virginia

**Στασινός Αλκιβιάδης 9214**

# What are Wireless Sensor Networks (WSNs)

- A wireless sensor network is a collection of nodes organized into a cooperative network.

- Each node consists mainly of these parts:
  - One or more microcontrollers.
  - Multiple types of small memory units.
  - An RF transceiver.
  - A power source, usually with batteries and solar cells.
  - Various sensors and actuators.

- Networks can be comprised of many nodes, hundreds or even thousands.
- Nodes communicate wirelessly and self-organize after being deployed.

- WSNs have unlimited potential for numerous application areas (environmental, medical, military, …)

# A WSN is a distributed real-time system, but very little prior work on the subject can be applied.

**Past research on has assumed that distributed systems:**

- Have wired connections.
- Have unlimited power.
- Are mainly not real-time.
- Have user interfaces (screens, mice).
- Have fixed number of resources.
- Treat each node as very important.
- Are location independent.

**In contrast, for WSNs:**

- The systems are wireless.
- Have scarce power and resources.
- Are real-time.
- Utilize sensors and actuators as interfaces.
- Have dynamically changing set of resources.
- Location is critical.

# MAC protocols for Wireless Sensor Networks

- A **MAC** protocol coordinates actions over a shared channel.

- Traffic is generally from nodes to other nodes or to base stations.
- An effective MAC protocol for WSNs must:
  - consume little power and avoid collisions.
  - be implemented with a small code size and memory requirements.
  - be efficient for a single application.
  - be tolerant to changing radio frequency and networking conditions.

- One example of a good MAC protocol for WSNs is **B-MAC**.

# B-MAC protocol

- B-MAC is highly configurable and can be implemented with a small code and memory size.
- It allows choosing and implementing only the functionality needed by a particular application.
- It consists of four main parts:
  - **Clear Channel Assessment.**
  - **Packet Backoff Time**
  - **Packet-by-Packet link layer acknowledgment**
  - **Low-power listening**
- More complicated schemes add unnecessary overhead since packets in a WSN are only about 50 bytes.
- New work focuses on multichannel WSNs, adding a phase of channel assignment. Advantages include greater packet throughput and transmitting even in the presence of a crowded spectrum.

# Routing

- **Multihop routing** is a critical service required for WSNs.
- Classic routing techniques require reliable wired connections or symmetric links. This is not true for WSNs.
- Routing begins with neighbor discovery. Nodes send special packets and build local neighbor tables. These tables typically include only each neighbor's ID and location (or also remaining energy, delay via that node, link quality,…).
- Nodes must know their geographic location prior to neighbor discovery.
- Messages are directed from a source location to a destination address based on geographic coordinates, **not** IDs.
- Two typical routing algorithms that work like this are **geographic forwarding (GF)** and **directed diffusion.**

# Routing algorithms

- Geographic forwarding
  - A node is aware of its location.
  - The routed message contains the destination address.
  - Next hop is based on which neighbor node covers the most distance toward the destination.
  - Could also take into account delays, link reliability and remaining energy.
- Directed diffusion
  - A query requests data from remote nodes.
  - A node with that data responds with an attribute-value pair.
  - This pair reaches the requestor based on gradients, which are set up and updated during query transmission and response.
  - Data may travel over multiple paths increasing the robustness of routing.

# Beyond the basics of WSN routing, there are many additional key issues

- **Reliability**

  It is important to have a high reliability on each link. Reliability can be measured in various ways (e.g. signal strength). Packet delivery ratio is the best metric, but expensive to collect.

- **Integration with wake/sleep schedules to save power**
- **Unicast, multicast, and anycast**
  1. The message may include an ID with a specific node in this area as the target, or a node closest to the geographic destination. (unicast)
  2. All nodes within some area around the destination address should receive the message. (Multicast)
  3. It may only be necessary for any node, in the destination area to receive the message (anycast) The SPEED protocol supports these three types of semantics.

- **Real Time**

  Sometimes messages have arrival deadlines. Protocols like SPEED use a notion of **velocity** to prioritize packet transmissions. Velocity is a metric that combines the deadline and distance a message must travel.

- **Mobility**

  Routing is complicated if nodes are moving. Solutions include continuously updating local neighbor tables or identifying proxy nodes.

- **Voids**

  Voids can be created in the direction a message has to travel. Protocols like GPSR choose another node “not” in the correct direction in an effort to find a path around the void.

- **Security**

  Almost all WSN routing algorithms have ignored security and are vulnerable to various attacks. New protocols have begun to address secure routing issues.

- **Congestion**

  Congestion is a problem for more demanding WSNs.

# Node Localization

- Node localization is the problem of determining the geographical location of each node in the system.
- It is a function of many parameters and requirements (hardware cost, required accuracy, energy budget, …).
- If cost and form factors are not major concerns and accuracy of a few meters is acceptable, then for outdoor systems, equipping each node with GPS is a simple answer.
- Most other solutions for localization in WSN are either **range-based** or **range-free**.

## Range-based solutions:

- First determine distances between node (range) and then compute location using geometric principles.
- Extra hardware is usually employed, for example, to detect the time difference of arrival of sound and radio waves.
- This difference can then be converted to distance measurement.

## Range-free solutions:

- Distances are not determined directly, but hop counts are used.
- Once hop counts are determined, distances between nodes are estimated using an average distance per hop.
- Geometric principles are then used to compute location.
- Range-free solutions are not as accurate as range-based.

- Two recent solutions are **Spotlight** and **Radio Interferometric Geolocation (RIG)** . Spotlight uses a centralized laser device, and requires line of sight and clock synchronization. **RIG** relies on nodes emitting radio waves simultaneously at slightly different frequencies. Both provide high accuracy in the centimeter range.

# Clock Synchronization

- The clocks of each node in a WSN should read the same time within certain fault range and remain that way. Clocks drift over time and must be periodically resynchronized.
- When an event occurs in a WSN it is often necessary to know where and when it occurred.
- Clocks are also used for many system and application tasks. For example, sleep/wake-up schedules, some localization algorithms, and computing velocity often depend on clocks being synchronized.
- The network time protocol (NTP) used on synchronize clocks on the Internet is too heavyweight for WSN.
- Clock synchronization protocols that have been developed for WSNs are **RBS**, **TPSN** and **FTSP**.

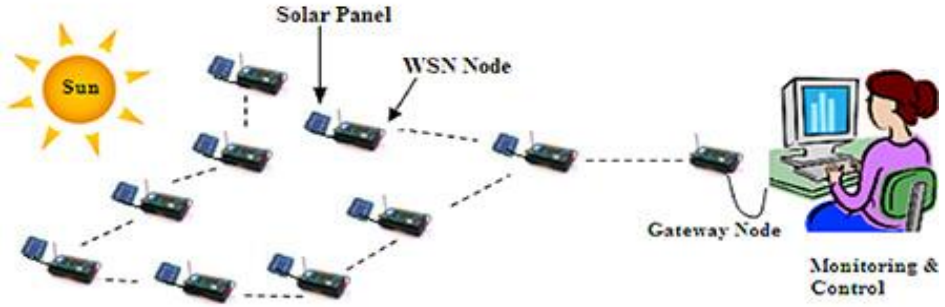
# Clock Synchronization Protocols for WSNs

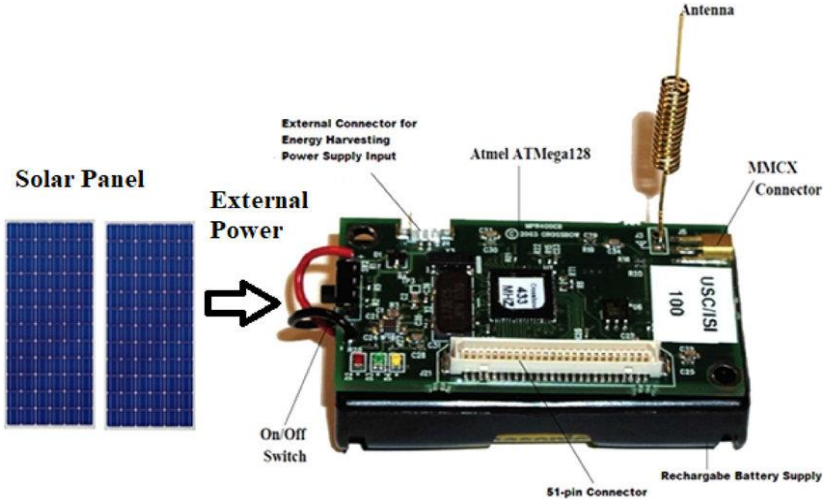
- In **RBS** a reference time message is broadcast to neighbors. Receivers record the time when the message is received and exchange their recorded times to synchronize their clocks. Accuracies are around 30µs for 1 hop.
- In **TPSN**, a spanning tree is created for the entire network. This solution assumes that all links in the tree are symmetric. Synchronization is performed along the edges of the tree starting at the root. Since there is no broadcasting as in RBS, TPSN is expensive. Accuracy is in the range of 17µs.
- In **FTSP**, transmission and reception of messages are timestamped and differences are used to compute and adjust clock offsets. Accuracy is within 1–2µs.

- Protocols should mainly consider the frequency of resynchronization and minimizing costs in energy and added network congestion.

# Power Management

- Many devices such as Mica2 and MicaZ used in WSN run on two AA batteries.
- With no power management schemes, node lifetime may be only a few days. Most systems require much longer lifetime. The main challenge is to increase lifetime while still meeting all functional requirements.
- At the hardware level, it is possible to add solar cells or scavenge energy from motion or wind. Batteries, low power circuits and microcontrollers are improving. If form factor is not a problem then we can add even more batteries. Most platforms allow multiple power-saving states (off, idle, on) for each device component.
- At the software level, solutions focus on minimizing communications since transmitting and listening for messages is energy expensive, and creating sleep/wake-up schedules for nodes.



- **Minimizing the number of messages**

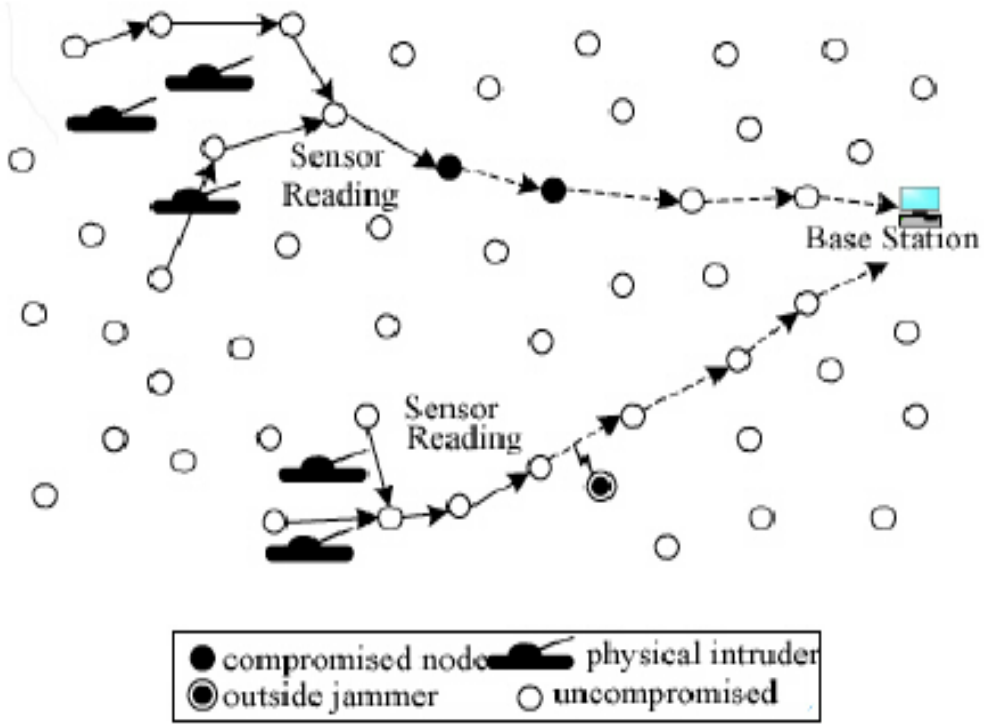
  Firstly, with a good MAC protocol there are fewer collisions and consequently **retries**. Good routing, short paths, efficient neighbor discovery, time synchronization, and localization can also minimize the number of messages thereby increasing lifetime.

- **Solutions to schedule sleep/wake-up patterns**
  - Many attempt to keep awake the **minimum number** of nodes, called sentries, to provide the required sensing coverage while all the others sleep. To balance energy consumption, a rotation of sleeping/awake nodes is performed periodically.
  - Another common technique is to **duty cycle** nodes. For example, a node may be awake for 200 ms out of each second for a 20% duty cycle. The duty cycle depends on application requirements, but the end result is usually very significant savings in energy. Duty cycle and sentry solutions can be combined.

# To demonstrate the capabilities of WSNs, we present two characteristic examples of applications and associated systems.

## Surveillance and tracking

- The **VigilNet** system is a real-time WSN for military **surveillance.**
- **VigilNet** is comprised of over 200 nodes with a sentry-based power management scheme, to achieve minimum 3–6 months lifetime.
- The general objective is to alert military units of events of interest in hostile regions.
- Examples include the presence of people, people with weapons, and large and small vehicles.
- Successful detection, tracking, and classification require obtaining the current position of an object with acceptable precision and confidence.
- When a node obtains the information, it is reported to a remote base station within an acceptable latency.



- VigilNet architecture can be divided in three main categories:

  - **Application components** that are specially designed for surveillance purposes. These include an **entity-based tracking service**, **target classification components, target velocity calculation**, and **false alarm filtering**

  - **Middleware components** designed to be application independent. These include **Time synchronization**, **localization,** and **routing**.

  - **TinyOS components**. Vigilnet was built on top of **TinyOS**, which is an event-driven computation model specifically for the nodes platform. TinyOS provides a set of essential components such as hardware drivers, a scheduler, and basic communication protocols.

- Power management and collaborative detection are two key services provided by VigilNet.
- When an event occurs the sentries awaken the other nodes in the region, which are dynamically organized into groups to collaboratively track.

.

# Assisted Living Facilities

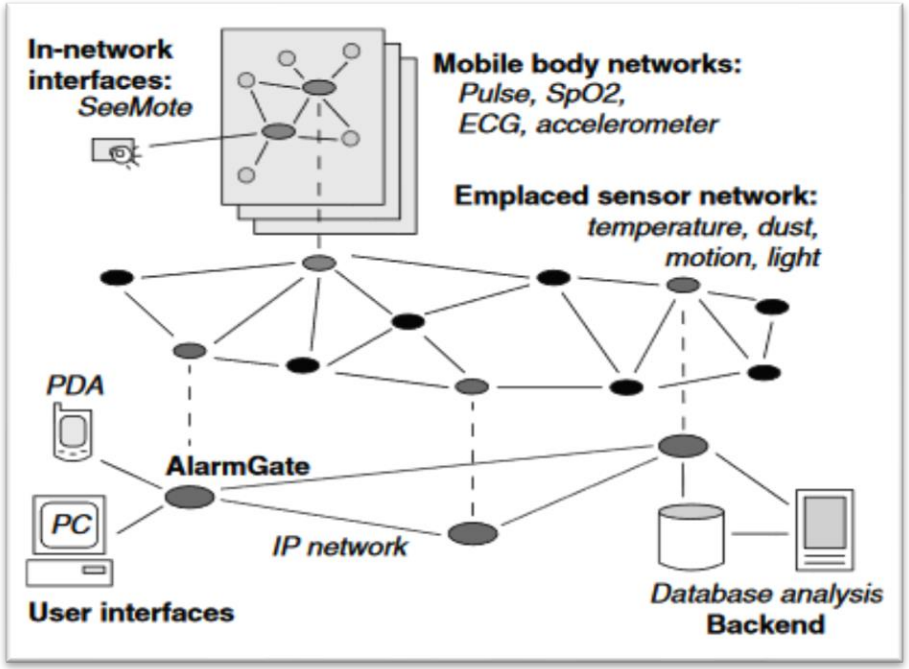
- **AlarmNet** is a sensor network system, integrating heterogeneous devices, some wearable and some placed inside the living space. Together they inform the healthcare provider about the health status of the resident.
- Data are collected using a variety of sensors and devices (activity, environmental, pressure, and pollution).
- Some nodes can use line power, but others depend on batteries.

- **AlarmNet** architecture is comprised of:
- **Body networks and Frontends.** The body network consists of tiny energy optimised portable devices with sensors (pulse, temperature, …) and performs biophysical monitoring. Actuators notify the wearer of important messages. Size and energy constraints limit processing and storage capabilities in this network.
- **Emplaced sensor network** includes sensors deployed in the living environment (rooms, hallways, …) to support sensing and monitoring. Devices are connected to a more resourceful backbone. Nodes here do not perform extensive calculation or store much data.

- **Backbone** network connects systems such as PDAs, PCs, and databases, to the emplaced sensor network. The backbone has significant storage and computation capability. Number of backbone devices is minimized to reduce cost.

- **In-network and backend databases.** One or more nodes connected to the backbone are dedicated in-network databases for real-time processing and caching. Databases are located at the medical center for long-term archiving, monitoring, and data mining.

- **Human interfaces**. Patients and health providers interface with the network. These are used for data management, querying, object location, and configuration depending on who is accessing the system. Caregivers use these to specify medical sensing tasks and to view important data.



# Conclusions and where to go from here

- Many important topics are not covered here. **Security** and **privacy** are **critical** services needed for these systems. **In-field autocalibration of sensors**, **signal processing** that runs on low-cost microcontrollers with minimum power and memory, **and low-cost techniques for self-organization**, and **parameter tuning** are critical areas of research.
- New tools (e.g. debugging, management tools) for WSNs are constantly appearing.
- Studies are also collecting empirical data on WSN performance.
- Such data are critical to improve models and solutions.
- All of this research is producing a **new** technology, which is already appearing in **many practical applications.** The future should see an accelerated pace of adoption of this technology.