COEN 331 (Wireless & Mobile Networks)

Summer 2020

Sensor Networks

Sravya Maduri

SCU ID: W1597753

Audience

This paper gives an overview of wireless sensor networks. It additionally incorporates organizing parts of WSNs and spreads the most significant systems administration issues, including system engineering plan, medium access control. It also includes node localization, transport protocols, routing, network security and finally future trends in WSNs.

The peruser is relied upon to know the basic routing protocols, Network architectures, IEEE standards. This book is proposed for scholastic scientists, graduate studies, professionals in industry, and exploration engineers.

Table Of Contents

Table of Figures

Table of Tables

1
INTRODUCTION

A Sensor network generally consists of a group of small, battery-powered devices. They are normally used to display bodily or environmental situations like temperature, sound, and that they ship their facts via the network to a chief sink or base station in which the facts are analyzed and observed. Sensor networks are typically two types: Wired or Wireless. Wireless sensor networks (WSNs) use technologies such as Bluetooth, cellular, wifi or near field communication (NFC) to connect sensors. Wired sensor networks take the help of ethernet cables to connect sensors.WSNs are easier to deploy and maintain and offer better flexibility of devices. With the rapid development of sensors and wireless technologies, WSNs have become a key technology of the IoT. WSNs don't need the physical network infrastructure to be modified.

This paper is written as below sections:

Section 1: Introduction.
Section 2: This section includes an overview of WSNs, WSN structure and sensor node structure.
Section 3: Discusses about network architectures and protocol stack of WSN.
Section 4: This section introduces Medium Access Control and IEEE 802.15.4 Standard for WSNs.
Section 5: Talks about Routing Protocols and strategies.
Section 6: This section discusses Transport Control Protocols.
Section 7: Discusses different types of Node localization techniques.
Section 8: In this section, Network security and related attack defense mechanisms are explained.
Section 9: This section includes future trends in WSNs.

2
OVERVIEW OF WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) allow new programs and require non-traditional paradigms for protocol layout because of numerous constraints. Owing to the requirement for low tool complexity collectively with low power consumption (i.E. long network lifetime), the right stability among communication and signal/fact processing abilities should be found. A Base station or Sink behaves as a bridge among the customers and the network. Information may be retrieved from the network with the aid of using enforcing queries and gathering outcomes from the station.

The nodes in WSNs are in-built with sources that are constrained: they've constrained conversation bandwidth, processing speed, and garage capacity. This motivates a massive attempt in studies activities, standardization process, and time, the maximum of the studies on WSNs has focused on the layout of power- and computationally green algorithms and protocols, and the software area has been constrained to easy facts-orientated tracking and reporting programs. Most of the time, the studies on wireless sensor networks have taken into consideration homogeneous sensor nodes.

But in recent times researchers have centered on heterogeneous sensor networks in which the sensor nodes are in contrast to every difference in phases in their energy. New network architectures with heterogeneous gadgets and the current development of this generation dispose of the contemporary obstacles and amplify the spectrum of viable programs for WSNs significantly and these kinds of are converting very rapidly.

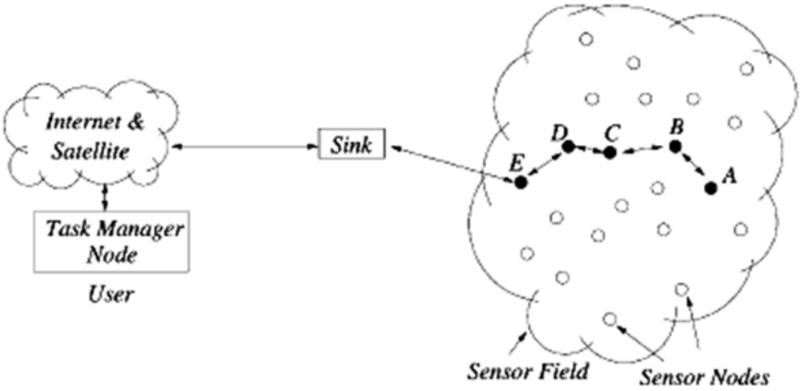


Figure 1: A typical wireless sensor network

2.1 Objectives of network design

The characteristics of sensor frameworks and the requirements of different applications definitively influence the framework plan focuses similar to framework limits and framework execution. The essential structure objectives for sensor frameworks consolidate the going with a couple of edges:

- **Small Node Size:** Reducing center point size is one of the basic network goals of sensor frameworks. Sensor center points are ordinarily sent in a remorseless or antagonistic condition in gigantic numbers. Reducing center point size can energize center association, and moreover diminish the cost and power use of sensor centers.
- **Low Node Cost:** Reducing center expenses is another basic network objective of sensor frameworks. Since sensor centers are typically sent in a ruthless or adversarial condition in colossal numbers and can't be reused, it is basic to diminish the cost of sensor center points so the cost of the whole framework is diminished.
- **Low Power Consumption:** Diminishing power use is the most noteworthy objects in the arrangement of a sensor sort out. Since

sensor center points are constrained by a battery and it is often amazingly problematic or even hard to change or stimulate their batteries, it is vital to lessen the power use of sensor center points with the objective that the lifetime of the sensor center points, similarly as the whole framework, is drawn out.

- **Self-Configurability:** In sensor frameworks, sensor center points are normally passed on in a district of eagerness without careful orchestrating and structuring. Once passed on, sensor center points should have the alternative to independently sift through themselves into a correspondence sort out and reconfigure their accessibility in the event of geology changes and center point frustrations.
- **Versatility:** In sensor sorts out, the amount of sensor center points may be on the solicitation for tens, hundreds, or thousands. Thusly, mastermind shows planned for sensor frameworks should be versatile to different framework sizes.
- **Adaptability:** In sensor composes, a center point may crash and burn, join, or move, which would achieve changes in center thickness and framework topography. In this manner, compose shows planned for sensor frameworks should be adaptable to such thickness and geology changes.
- **Steadfast quality:** For a few, sensor orchestrate applications, it is required that data be reliably passed on over boisterous, botch slanted, and time-fluctuating remote channels. To meet this need, orchestrate shows proposed for sensor frameworks must give botch control and alteration instruments to ensure strong data transport.
- **Fault tolerance:** Sensor centers are slanted to dissatisfactions on account of coldblooded association circumstances and unattended

undertakings. As such, sensor centers should be issue permissive and have the limits of self-testing, self-changing, self-fixing, and self-recovering.

- **Security:** In various military applications, sensor center points are sent in a hostile circumstance and as such are unprotected against adversaries. In such conditions, a sensor framework ought to familiarize convincing security instruments with hinder the data information in the framework or a sensor center point from unapproved get to or poisonous attacks.

- **Channel Utilization:** Sensor frameworks have obliged information transmission resources. Along these lines, correspondence shows planned for sensor frameworks should capably use the information move ability to improve channel utilization.

- **QoS Support:** In sensor frameworks, different applications may have assorted Quality of Service (QoS) essentials with respect to transport lethargy and bundle setback. For example, a couple of uses, for example, fire checking, are delay-delicate and thusly require helpful data transport. A couple of utilizations, for example, data collection for consistent examination, defer liberal yet can't stand bundle incident. Along these lines, sort out show setup should consider the QoS necessities of express applications. Most sensor frameworks are application-express and have assorted application necessities. It isn't fundamental and extremely ridiculous to execute all the arrangement focuses on a singular framework. Or maybe, simply bit of these goals should be considered in the architecture of a specific framework in order to meet its application essentials.

2.2 Structure of a wireless sensor network

Structure of a Wireless Sensor Network includes various topologies for radio communications networks and they are outlined as below:

- **Star network (single point-to-multipoint):**

A star network is a communications topology wherein a single base station can ship and/or get hold of a message to some of the faraway nodes. It additionally lets in low latency communications among the faraway node and sink station. The downside of this kind of network is that the sink station ought to be inside the radio transmission range of all of the individual nodes and isn't as sturdy as different networks because of its dependency on a single node to control the network.

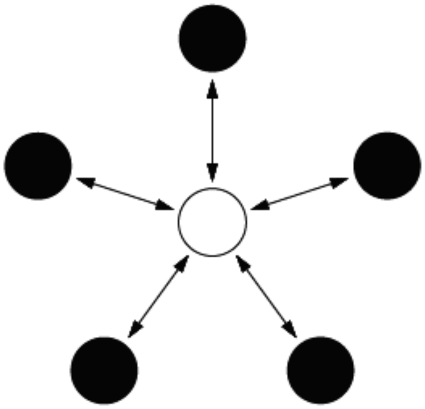


Figure 2: A star network topology

- **Mesh network:**

In this network if a single node fails, a remote node nonetheless can communicate to some other node in its range, which in turn, can deliver the message to the preferred location.

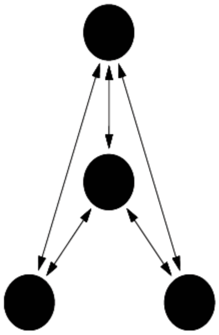


Figure 3: A mesh network topology

- **Hybrid star – Mesh network:**

A hybrid among the star and mesh network presents a strong and flexible communications network, whilst retaining the capacity to hold the wireless sensor nodes power intake to a minimum. This lets in for minimum power intake to be maintained. This is the topology carried out with the aid of using the up and coming mesh networking standard referred to as ZigBee.

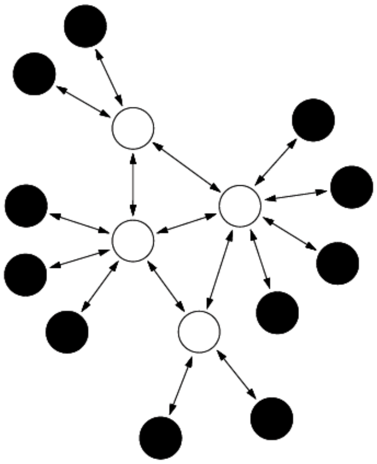


Figure 4: A Hybrid Star – Mesh network topology

2.3 Structure of a wireless sensor node

A sensing unit, a processing unit, a transceiver unit, and a power unit are basically the four fundamental components of a sensor node.

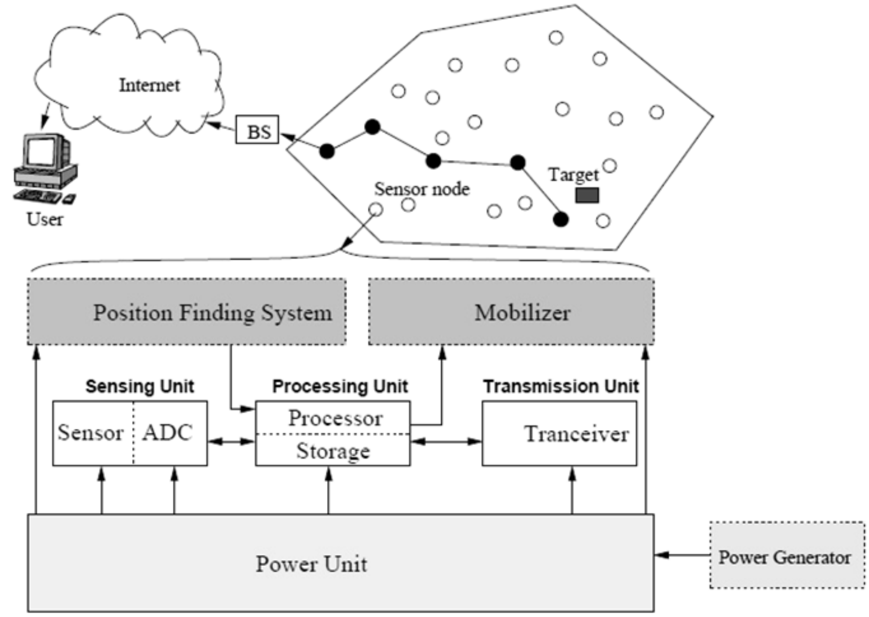


Figure 5: Components of a sensor node

It additionally has utility established extra additives consisting of an area locating system, a power generator, and a mobilizer. Sensing devices are commonly composed of subunits: sensors and analog to digital converters (ADCs). The analog signals produced via way of means of the sensors are transformed into virtual indicators via way of means of the ADC, after which fed into the processing unit. The processing unit is typically related to a small garage unit and it could manipulate the approaches that make the sensor node collaborate with the opposite nodes to perform the assigned sensing tasks. Node is connected to the network through a transceiver unit. One of the maximum crucial additives of a sensor node is the power unit.

3

NETWORK ARCHITECTURES AND PROTOCOL STACK

Network architectures and protocols are crucial factors with inside the layout of wireless sensor networks. Due to the excessive energy constraint of sensor nodes, network architectural layout has a large effect at the energy intake and as a result the operational life of the complete network. On the alternative hand, a sensor network includes a large number of sensor nodes that can be densely deployed in a sensing vicinity and collaborate to perform a sensing task. It requires a set of network protocols to enforce numerous network control and management functions, for example, synchronization, self-configuration, medium get entry to manage, routing, data aggregation, node localization, and network security.

3.1 Network Architectures

A sensor network normally includes a massive range of sensor nodes densely deployed in a location of interest, and one or greater information sinks or base stations which might be positioned near or in the sensing location. The sink(s) sends queries or instructions to the sensor nodes inside the sensing location whilst the sensor nodes collaborate to perform the sensing assignment and ship the sensed information to the sink(s). Meanwhile, the sink(s) additionally serves as a gateway to the outdoor networks, for example, the Internet. It collects facts from the sensor nodes, plays easy processing at the amassed facts, after which sends applicable information (or the processed facts) through the Internet to the customers who asked it or use the information. To deliver information to the sink, every sensor node can use single-hop long-distance transmission, which ends up in the single-hop network structure.

In maximum sensor networks, sensor nodes are densely deployed and neighbor nodes are near every other, which makes it possible to apply short-distance communication. In multi-hop communication, a sensor node transmits its sensed information towards the sink through one or greater intermediate nodes, that could lessen the energy intake for communication. The structure of a multi-hop network may be prepared into types: flat and hierarchical.

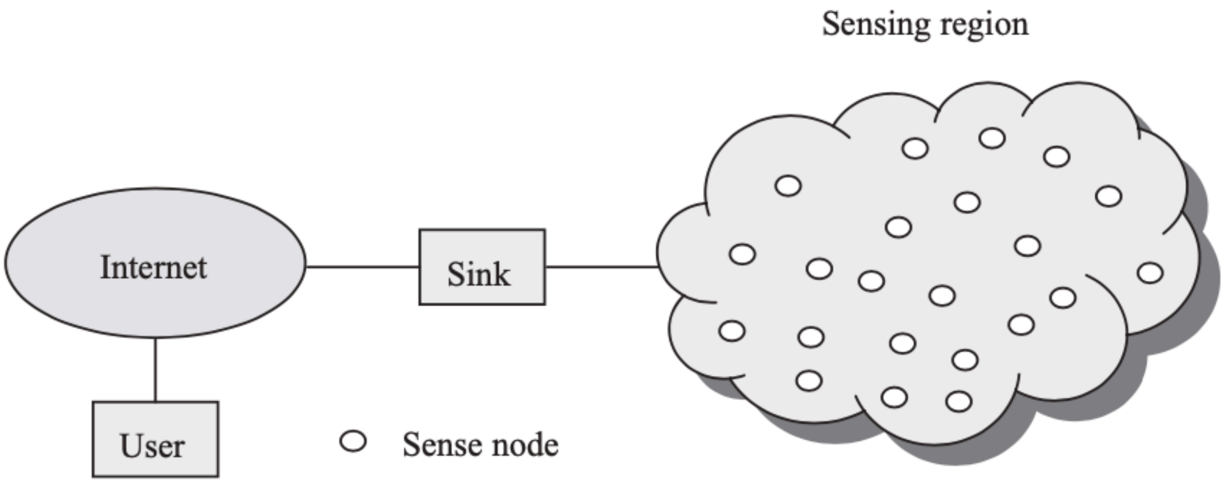


Figure 6: Sensor Network Architecture

3.1.1 Flat Architecture

In a flat network, every node performs an equal position in appearing a sensing venture and all sensor nodes are peers. Due to the huge wide variety of sensor nodes, it isn't always possible to assign a worldwide identifier to every node in a sensor network.

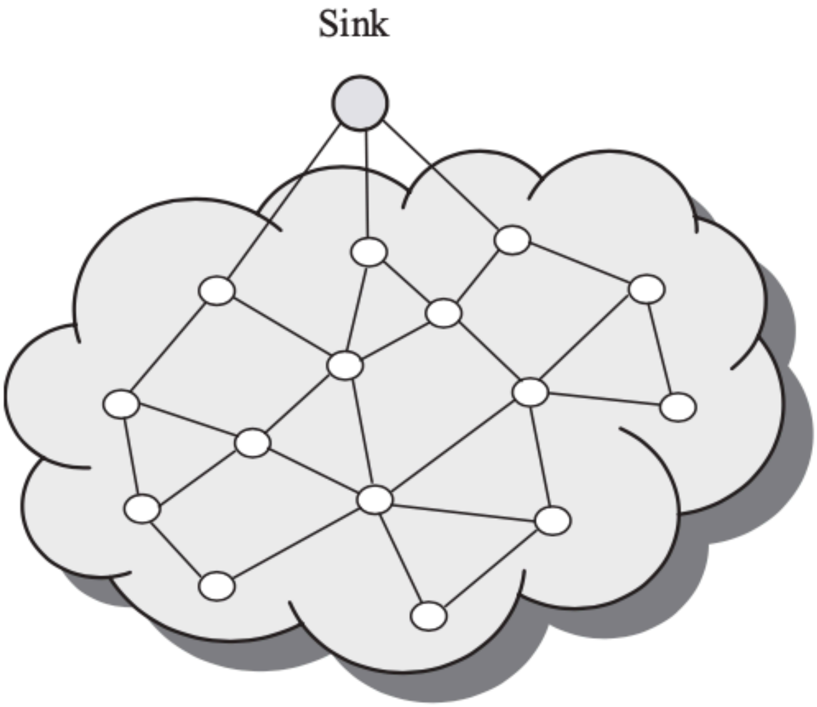


Figure 7: Flat Network Architecture

For this reason, information collecting is typically executed through the usage of data-centric routing, wherein the data sink transmits a query to all nodes inside the sensing area thru flooding and handiest the sensor nodes which have the statistics matching the question will reply to the sink. Each sensor node communicates with the sink thru a multi-hop direction and makes use of its peer nodes as relays.

3.1.2 Hierarchical Architecture

In a hierarchical network, sensor nodes are grouped into clusters, in which the cluster contributors deliver their records to the cluster heads at the same time as the cluster heads function relays for transmitting the records to the sink. A node with low energy capacity may be used to carry out the sensing work and ship the sensed records to its cluster head at a quick distance, at the same time as a node with high energy may be decided on as a cluster head to procedure the records from its cluster contributors and transmit the processed records to the sink. This procedure can't best lessen the energy intake for communication, however additionally stability site visitors load and enhance scalability whilst the network size grows.

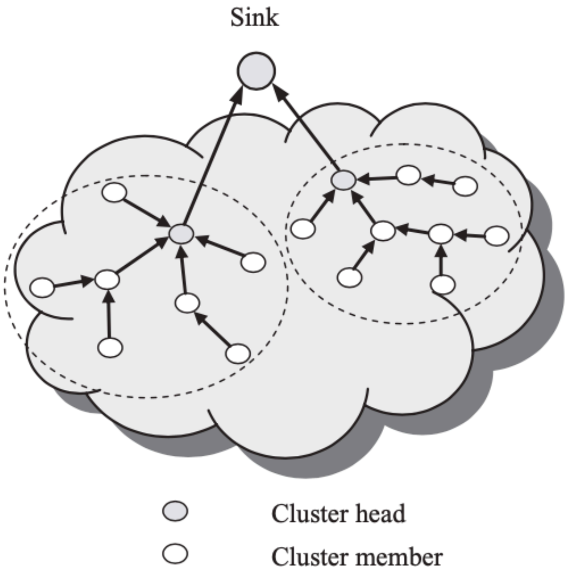


Figure 8: Multi-hop Clustering Architectures

Since all sensor nodes have equal transmission capability, the clustering needs to be periodically executed so as to stability the site visitors load amongst all sensor nodes. Moreover, data aggregation may be executed at cluster heads to lessen the quantity of records transmitted to the sink and enhance the power performance of the network. The fundamental trouble with clustering is the way to pick the cluster heads and the way to group the clusters. In this context, there are numerous clustering strategies. According to the gap among the cluster contributors and their cluster heads, a sensor network may be prepared right into a single-hop clustering structure or a multi-hop clustering structure. According to the range of ranges inside the clustering hierarchy, a sensor network may be prepared right into a single-tier clustering structure or a multi-tier clustering structure.

3.2 Classifications of wireless sensor networks

WSNs are application-specific. A sensor network is typically deployed for a particular application and thus has some different characteristics. in step with different criteria, WSNs will be classified into different categories.

- **Single-Hop and Multi-jump Network:** As indicated by the number of bounces between a sensor network and the information sink, a sensor system can be grouped into single-jump or multi-jump. In a single hop network, all sensor nodes transmit their detected information legitimately to the sink, which makes organize control more straightforward to actualize. Be that as it may, this requires long-run remote correspondence, which is exorbitant as far as both energy utilization and equipment usage. The farthest nodes from the information sink will bite the dust substantially more rapidly than those near the sink. Likewise, the general traffic load in the system may increment quickly with the expansion of the system size, which would cause more crashes, and in this way increment energy utilization and conveyance idleness. In a multi-hop network, sensor nodes transmit their detected information to the sink utilizing short-extend remote correspondence by means of at least one middle of the road nodes. Each middle of the road network must perform directing and forward the information along a multi-jump way. Besides, information collection can be performed at a middle of the road network to wipe out information repetition, which can decrease the aggregate sum of traffic in the system and in this way improve the energy effectiveness of the system.

- **Deterministic and Nondeterministic Network:** As indicated by the organization of sensor nodes, a sensor system is deterministic or nondeterministic. In a very deterministic sensor network, the places of sensor nodes are preplanned and are fixed once conveyed, this sort of system must be utilized in some restricted circumstances, where the preplanned arrangement is conceivable. As a rule, be that because it may, it's hard to send sensor nodes in a very preplanned way as a result of the unforgiving or unfriendly situations. Rather, sensor nodes are haphazardly conveyed without preplanning and designing. Clearly, non-deterministic systems are increasingly versatile and adaptable, yet require higher control unpredictability.

- **Static-Sink and Mobile-Sink Network:** An information sink in an exceedingly sensor system may be static or portable. In a static-sink network, the sink is static with a hard and fast position found near or inside a detecting locale. All sensor nodes send their detected information to the sink. Clearly, a static sink makes the system easier to regulate, however it'd cause the hotspot impact. The measure of traffic that sensor nodes are required to advance increments significantly because the separation to the data sink decreases. Therefore, sensor nodes nearest to the data sink will generally die early, hence bringing about system segment and in any event, disturbing typical system activity. In a very portable sink arrange, the sink moves around within the detecting region to assemble information from sensor nodes, which may adjust the traffic heap off sensor nodes and ease the hotspot impact within the system.

- **Homogeneous and Heterogeneous Network:** As indicated by whether sensor nodes have similar abilities, a sensor system can be homogeneous or heterogeneous. In a homogeneous system, all sensor nodes have similar abilities as far as energy, calculation, and capacity. Interestingly, a heterogeneous system has some modern sensor nodes that are outfitted with more handling and conveying capacities than typical sensor nodes. For this situation, the system can allot additionally handling and correspondence undertakings to those complex nodes so as to improve its energy efficient and along these lines delay the lifetime.

- **Single-Sink and Multi sink Network:** A sensor system can have a solitary sink or various sinks. In a solitary sink arrange, there is just one sink found near or inside the detecting locale. All sensor nodes send their detected information to this sink. In a multi sink arrange, there might be a few sinks situated in various positions near or inside the detecting locale. Sensor nodes can send their information to the nearest sink, which can adequately adjust the traffic heap of sensor nodes and lighten the hotspot impact in the system.

- **Self-Reconfigurable and Non-Self-Configurable Network:** As per the configurability of sensor nodes, a sensor system can act naturally configurable or non-self-configurable. In a non-self-configurable system, sensor nodes have no capacity to sort out themselves into a system. Rather, they need to depend on a focal controller to control every sensor network and gather data from them. Consequently, this kind of system is just appropriate for little scope systems. In most sensor systems, in any case, sensor nodes can self-sufficiently sort out and keep up their network without anyone else and cooperatively achieve a detecting task. A system with such self-configurability is reasonable for enormous scope systems to perform muddled detecting assignments.

- **Static and Mobile Network:** As per the portability of sensor nodes, a sensor system is static or versatile. during a static sensor organize, all sensor nodes are static without any movement, which is the situation for a lot of applications. Be that because it may, some sensor applications require portable nodes to realize a detecting task. Contrasted with static sensor systems, which are more straightforward to regulate and simpler to execute, the structure of portable sensor systems must consider the flexibility impact, which builds the intricacy of usage.

3.3 Protocol Stack for wireless sensor networks

The protocol stack for WSNs comprises five layers: data link layer, transport layer, application layer, the physical layer, and network layer.

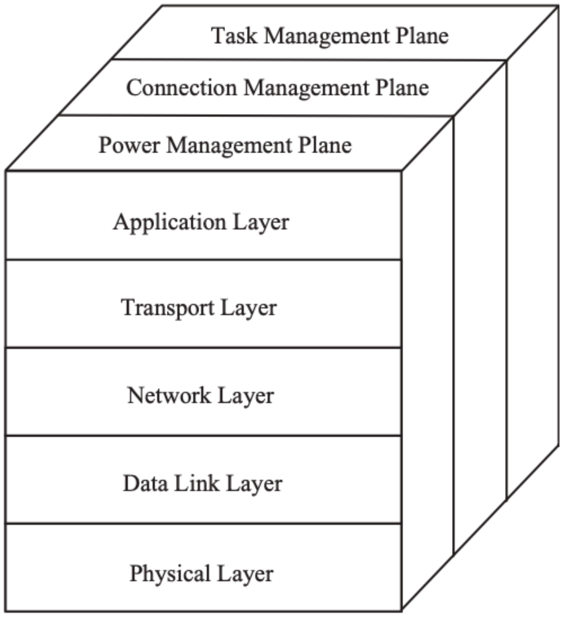


Figure 9: Protocol stack for Sensor Networks

Application Layer:

The application layer incorporates an assortment of application layer protocols that perform different sensor arrange applications, for example, inquiry dispersal, network restriction, time synchronization, and system security. For instance, the sensor management protocol (SMP) is an application-layer the executive's protocol that gives programming activities to play out an assortment of errands, for instance, trading area related information, synchronizing sensor networks, moving sensor networks, booking sensor networks, and questioning the status of sensor networks. Inquiries, reacting to questions, and gather reactions are provided by sensor query and data dissemination protocol (SQDDP). The sensor query and tasking language (SQTL) give a sensor programming language used to actualize middleware in WSNs. Even though numerous sensor arrange applications have been proposed, their comparing application-layer protocols despite everything should be created.

Transport Layer:

By and large, the transport layer is answerable for a dependable start to finish information conveyance between sensor networks and the sink. Because of the energy, calculation, and capacity limitations of sensor networks, transport protocols can't be applied straightforwardly to sensor systems without adjustment. For instance, the regular start to finish retransmission-based error control and the window-based blockage control systems utilized in the transport control protocol (TCP) can't be utilized for sensor organizes straightforwardly in light of the fact that they are not productive in asset usage. Then again, sensor systems are application-explicit. A sensor network is generally sent for a particular detecting application, for instance, environment observing, stock control, and combat zone observation. Various applications may have diverse dependability prerequisites, which hugely affect the plan of transport-layer protocols. Also, information conveyance in sensor arranges principally happens in two ways: upstream and downstream. In the upstream, the sensor networks transmit their detected information to the sink, while in the downstream the information began from the sink, for instance, questions, orders, and programming pairs are sent from the sink to the source sensor networks. The information stream in the two headings may have diverse unwavering quality necessities. For instance, the information stream the upstream way is misfortune lenient in light of the fact that the detected information is normally connected or repetitive to a limited degree. In the downstream, be that as it may, the information streams are questions, orders, and programming doubles sent to the sensor networks, which for the most part require 100% dependable conveyance.

Network Layer:

The network layer is answerable for directing the information detected by source sensor nodes to the information sink. In a sensor organization, sensor nodes are sent in a detecting area to watch a marvel of intrigue. The watched marvel or information should be transmitted to the information sink. When all is said in done, a source network can transmit the detected information to the sink either straightforwardly by means of single-bounce long-extend remote correspondence or through multi-hop short-go remote correspondence. Be that as it may, long-run remote correspondence is exorbitant as far as both energy utilization and usage multifaceted nature for sensor nodes. Interestingly, multi-hop short-extend correspondence can not just essentially decrease the energy utilization of sensor nodes, yet in addition, adequately diminish the sign proliferation and divert blurring impacts intrinsic in long-run remote correspondence, and is hence liked. It is conceivable to utilize multi-hop short-run correspondence in sensor systems as sensor nodes are thickly sent and neighbor nodes are near one another. For this situation, to send the detected information to the sink, a source network must utilize a directing protocol to choose an energy proficient multi-jump way from the network itself to the sink. Notwithstanding, steering protocols for customary remote systems are not reasonable for sensor systems since they don't consider energy efficiency as an essential concern. Likewise, information from the detecting district toward the sink shows an exceptional many-to-one traffic design in sensor systems. The blend of multi-hop and many-to-one interchanges brings about a critical increment in travel traffic power and in this manner bundle clog, crash, misfortune, postponement, and energy utilization as information push nearer toward the sink. The sensor nodes closer to the sink, normally inside few jumps, will lose a bigger number of parcels and devour significantly more energy than the nodes further away from the sink, consequently generally lessening the operational lifetime of the whole system. In this way, it is essential to consider the energy requirement of sensor nodes just as the one of a kind traffic design in the structure of the system layer and directing protocols.

Data Link Layer:

The data link layer is answerable for information stream multiplexing, information outline creation and discovery, medium access, and mistake control so as to give dependable highlight point and highlight multipoint transmissions. One of the most significant elements of the information connect layer is medium access control (MAC). The essential target of MAC is to decently and proficiently share the mutual correspondence assets or medium among different sensor networks so as to accomplish great system execution as far as energy utilization, organize throughput, and conveyance inactivity. Be that as it may, MAC protocols for customary remote systems can't be applied straightforwardly to sensor systems without alteration since they don't consider the one of a kind qualities of sensor systems, specifically, the energy imperative. For instance, the essential worry in a cell framework is to give quality of service (QoS) to clients.

Energy Efficiency is just an auxiliary significance on the grounds that there is no force limit with the base stations and the portable clients can renew the batteries in their handsets. Another significant capacity of the information interface layer is blunder control in information transmission. In numerous applications, a sensor organize is conveyed in an unforgiving environment where remote correspondence is blunder inclined. For this situation, blunder control gets basic and basic for accomplishing join unwavering quality or dependable information transmission. As a rule, there are two primary mistake control components: Forward Error Correction (FEC) and Automatic Repeat reQuest (ARQ). ARQ accomplishes dependable information transmission by retransmitting lost information parcels or edges. Obviously, this acquires critical retransmission overheads and extra energy consumption, and in this way isn't appropriate for sensor systems. FEC accomplishes connect unwavering quality by utilizing blunder control codes in information transmission, which presents extra encoding and translating complexities that require extra handling assets in sensor networks.

Be that as it may, FEC can altogether diminish the channel bit error rate for some random transmission power. Given the energy requirement of sensor networks, FEC is as yet the most proficient answer for mistake control in sensor systems. To structure an FEC instrument, the decision of the blunder control code is significant in light of the fact that an all-around picked mistake control code can acquire a decent coding gain and a few significant degrees decrease in BER. Then, the extra preparing power devoured for encoding and unraveling must likewise be thought of. In this way, an exchange off ought to be streamlined between the extra preparing power and the comparing coding gain so as to have an incredible, energy-efficient, and low-multifaceted nature FEC component.

Physical Layer:

The physical layer is liable for changing over bits streams from the information link layer to signals that are appropriate for transmission over the correspondence medium. For this reason, it must arrangement with different related issues, for instance, transmission medium and recurrence choice, bearer recurrence age, signal regulation and identification, and information encryption. What's more, it should likewise manage the structure of the fundamental equipment, and different electrical and mechanical interfaces. Medium and recurrence choice is a significant issue for correspondence between sensor networks. One alternative is to utilize radio and the industrial, scientific, and medical (ISM) groups that are sans permit in many nations. The principle favorable circumstances of utilizing the ISM groups incorporate free use, enormous range, and worldwide accessibility. Be that as it may, the ISM groups as of now have been utilized for some correspondence frameworks, for example, cordless telephone frameworks and wireless local area networks(WLANs). Then again, sensor systems require a minuscule, minimal effort, and ultra-low-power handset.

4

MEDIUM ACCESS CONTROL & STANDARDS

The principal objective of the MAC layer is to ensure reliable data transmission across the link that the physical layer has already determined. Furthermore, the MAC layer determines the way access is controlled in the communication channel, a fundamental function in case of broadcast WSNs where the physical medium is shared by a large number of sensors. Generally, in any broadcast network, the prominent issue is determining the node that uses the wireless channel at which time and over with which frequency. Therefore, message transmission regulation is needed to achieve an efficient channel allocation amongst the nodes. MAC layer and its associated protocols that set the rules for the communication between the sending and the receiving node refer mainly to mechanisms that control the timing of frequency intervals for sending a message or packet through the channel and listening for it.

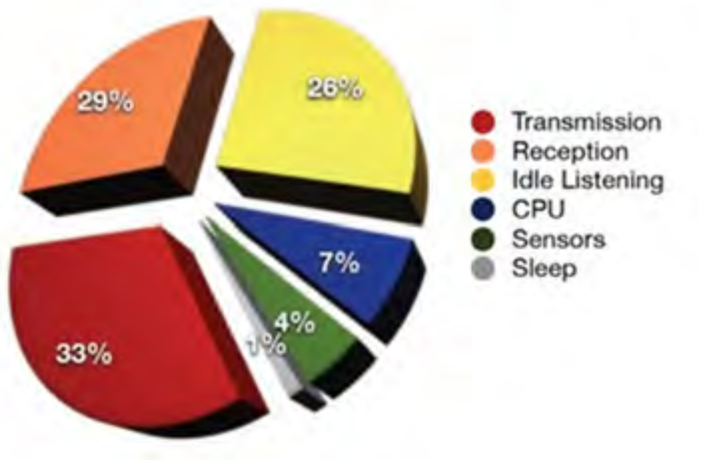


Figure 10: Power consumption of a WSN node

4.1 Characteristics of MAC Protocols

The important assignment of any MAC protocol is to have control of the access of the nodes to the wireless channel in order that that few application-established overall performance necessities are satisfied. Some of the conventional overall performance criteria are transmission put off, throughput, and equity, whereas, in WSNs, the extra overall performance criterion of energy conservation is important. The characteristics of the MAC protocols are:

Throughput: Throughput is described with the aid of using the rate at which messages are served. The throughput may be measured in messages or symbols per second however most generally is measured in bits per second and the main purpose is to maximize it.

Transmission delay: Transmission put off is described as the quantity of time that a single message spends inside the MAC protocol. It can be categorized in deterministic delay and probabilistic delay that permits best an approx. Of the delay, giving the opportunity to calculate the relative worst or nice case bound. The delay trouble calls for MAC protocols to be easy and feature as few mechanisms as possible. Designing concepts must compromise on simplicity and occasional delay with the error control, retransmissions, and collision avoidance.

Fairness: A MAC protocol is taken into consideration truthful if it allocates a channel a number of the competing nodes in step with a few equity standards. However, equity is a complicated term in WSN. WSN may be regarded as a distributed system and envisaging it so the ratio of channel allocation among nodes might also additionally or won't be fair.

Scalability: Scalability describes the cap potential of the communication system to satisfy overall performance traits notwithstanding the dimensions of the network and the number of competing nodes. Although this metric belongs more to the network structure the designer of a MAC protocol has to don't forget a way to deal with opposition for channel get entry to, retransmission, and what occurs if the site visitors load will increase due to the growth of the number of nodes.

Stability: Stability describes how suitable the protocol handles fluctuation of site visitors load over a sustainable length of time.

Robustness: Robustness is known as a composition of reliability, availability, and dependability. It describes protocol sensibility for site visitors load over a sustained length of time.

4.2 Classification of MAC Protocols

Contingent upon the manner in which MAC conventions manage access on the common medium, they can be arranged into two expansive classes: Schedule- based or contention-free and contention-based protocols. Conventions having a place with the top-notch, permit just a single node at once to get to the remote channel. A schedule manages which node may utilize which time or recurrence space at which time. The schedule can be fixed or registered on request bringing about a further characterization into fixed-task and on-request conventions, separately. For this situation, impacts, catching, and inactive listening are maintained a strategic distance from, however, time synchronization among nodes is required. Then again, contention-based protocols permit nodes to get to the remote channel at the same time. The fundamental standard of these conventions is irregular access. Consequently, systems are actualized to deal with or decrease the happening message crashes. MAC conventions that don't fit into this arrangement having attributes of both contention-free and contention-based procedures are cross breed approaches frequently planning to acquire the upsides of these principle classes, while limiting their shortcomings.

4.2.1 Schedule-based (Contention-free) MAC Protocols:

Typical protocols of this magnificence are TDMA, FDMA, and CDMA. TDMA(The Time Division Multiple Access) scheme splits the time axis into slots. These time slots are assigned to every node solely and consequently, each node transmits periodically simplest in its very own time slot. In maximum cases, a central node makes a decision about the TDMA schedules. Synchronization is likewise wished most of the nodes to keep away from message collisions in adjoining time slots. This scheme is beneficial in small networks or whilst the network is split into smaller clusters, where, in every one of them, MAC may be managed at a nearby cluster head. In Frequency Division Multiple Access (FDMA), the to be had frequency band for transmissions is split into sub-channels, every of that is assigned to the specific node. Since every node has its very own personal frequency band, focused round a service frequency, there's no interference among specific nodes. In this case, frequency synchronization in addition to narrowband filters are required.

Code Division Multiple Access (CDMA) assigns a specific code to every node. Each node then makes use of its specific code to encode the information bits it sends. If the codes are selected carefully, specific nodes can transmit concurrently and but have their respective receivers successfully obtain a sender's encoded message bits (assuming the receiver is aware of the sender's CDMA code and the codes are "orthogonal") regardless of interfering transmissions through different nodes. The above stated schedule-based techniques are efficient and offer higher overall performance whilst the range of nodes inside the network is small and constant. On the contrary, whilst the range of nodes is huge and constantly various or the site visitors is bursty, schedule primarily based totally on techniques presents a few problems. In specific, in TDMA, a delay takes place every time a user does now no longer use the allotted slot. In FDMA, if the service frequency is split into N slots and less than N nodes are presently inquisitive about communicating, a huge piece of the precious spectrum is wasted. Furthermore, if extra than N nodes need to communicate, a number of them may be denied permission because of loss of bandwidth, even supposing a number of the sensors which have been assigned a frequency band not often transmit or obtain anything.

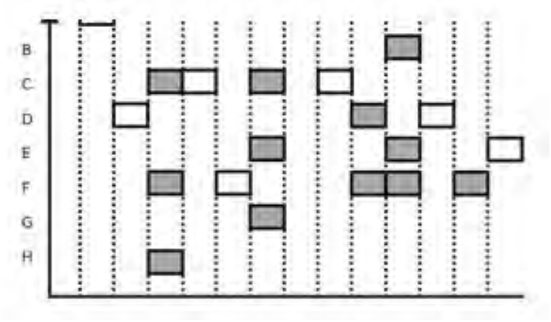


Figure 11: Slotted ALOHA protocol

4.2.2 Contention-based MAC Protocols :

When the quantity of nodes is huge and variable or the traffic is reasonably bursty, schedule-based schemes are terrible choices. In this case, few contention-based MAC protocols had been proposed as an alternative. Typical protocols of this magnificence are the ALOHA and CSMA protocols.

ALOHA Protocols:

Slotted ALOHA is taken into consideration as one of the most effective contention-based MAC protocols. It works on the pinnacle of TDMA as time is split into slots of length identical to the time interval a message calls for to be transmitted. In this scheme, nodes are synchronized and begin to transmit messages best on the beginnings of the slots. In case that or extra messages collide throughout a slot, then all of the nodes locate the collision occasion earlier than the slot ends. In particular, permit be a possibility that a node can transmit a message.

1. When a node has a brand new message to send, it waits till the start of the following slot and transmits the complete node inside the slot.
2. If no collision occurs, the node has correctly transmitted its node and for that reason need not take into account retransmitting the message.
3. If a collision occurs, the node detects the collision earlier than the cease of the slot and retransmits its message in every next slot with possibility till the message is transmitted without a collision.

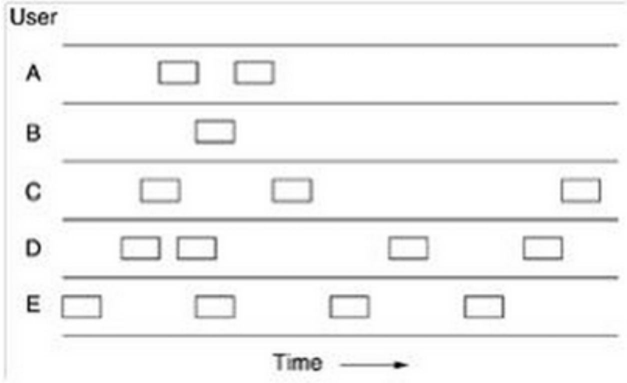


Figure 12: Pure ALOHA protocol

4.3 The IEEE 802.15.4 Standard for WSNs

IEEE 802.15.4 is the de-facto reference well-known for low information price and low power WSNs. The IEEE 802.15.4 well-known specifies layers: the physical and MAC layer. The predominant function of IEEE 802.15.4 is the low information price for ad hoc self-organizing networks of cheaper fixed, portable, and shifting nodes. In general, the nodes are called “devices”. The standard offers excessive network flexibility and really low power consumption. The standard introduces a MAC with a super-frame structure with consecutive periods. The network is thought to be clustered and every cluster head, i.E., Personal Area Coordinator (PAN) coordinator, announces the frame structure and allocates slots to prioritized site visitors inside a contention-free period. In the contention period, nodes contend the usage of both CSMA/CA or slotted CSMA/CA to get entry to the wireless channel. The winners can allocate the channel for their transmissions for a selected quantity of time. This offers a flexible get admission to technique for nodes with infrequent traffic. During the contention-free period, nodes with better precedence traffic are served by the PAN coordinator. Based on the traffic requirements, every node is assigned slots at some point of the contention-free period. These slots are allotted to the simplest one pair and channel contention is avoided to offer precedence. As a result, the IEEE 802.15.4 protocol offers a hybrid operation thru a CSMA-based and a TDMA-based operation.

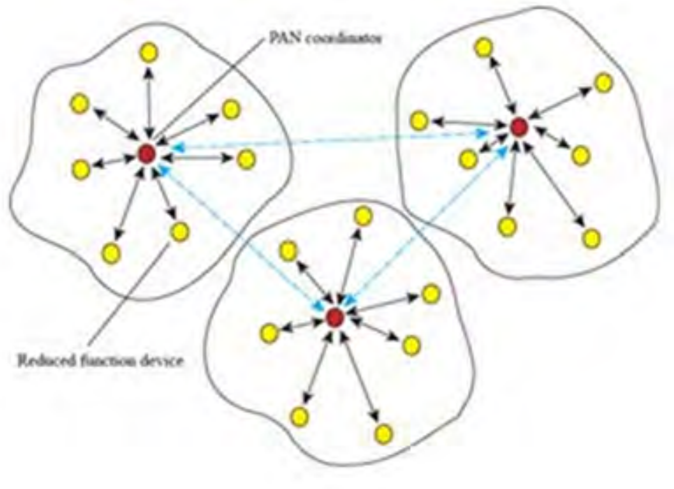


Figure 13: An IEEE 802.15.4 WSN

An IEEE 802.15.4 Network:

An IEEE 802.15.4 network consists of one-of-a-kind varieties of network devices; full-function devices (FDD) and reduced-function devices (RFD). The network consists of as a minimum one FFD that could function in 3 modes; as a personal area network (PAN) coordinator, as an easy coordinator, or as an easy tool.

RFDs are destined for easy programs and they may be concerned in transmissions of small quantities of data. An IEEE 802.15.4 network can function in 3 one-of-a-kind topologies; Star topology, peer-to-peer topology, and cluster tree topology.

In the star topology, the communication is set up among the devices and a principal controller this is known as PAN coordinator. A PAN coordinator, except the utility that wishes to perform, is accountable for important network tasks, inclusive of the start, the termination, and the routing of the communication.

In this kind of topology, the PAN coordinator has to be continuously linked to a power delivery while the rest devices will have batteries as their supply of energy. A neighborhood network organized in a star topology is characterized with the aid of using a completely unique PAN identifier variety that lets in it to function independently from all of the different neighborhood networks inside its transmission variety.

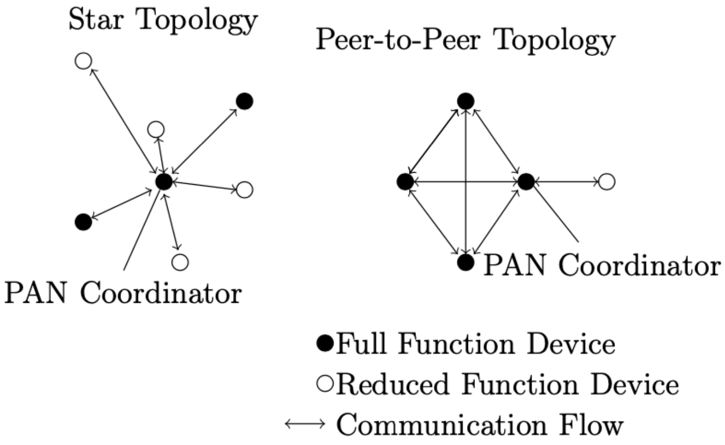


Figure 14: Star and peer-to-peer topology of IEEE 802.15.4

The most important distinction with respect to the star topology is that now all of the devices are capable of communicating with every difference as far as a tool is positioned in the variety of another. This kind of topology additionally lets in network implementations with a better complexity degree and, therefore, it is very famous in WSN programs because it permits self-corporation and self-configuration or ad hoc networks.

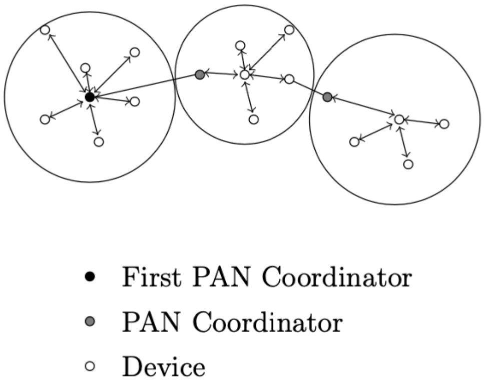


Figure 15: Cluster-tree topology of IEEE 802.15.4

Cluster-tree topology is a unique case of a peer-to-peer topology wherein each FFD is capable of function as a coordinator and offers synchronization each to different devices and to different coordinators. In this topology, an RFD is hooked up only on the cease of a cluster department as it can communicate with only one FFD at a time. Moreover, the coordinator of the primary cluster operates as a worldwide PAN coordinator and consumes a maximum of the computational network sources with admire to some other tool. The most important benefit of this precise topology is the extensive coverage of a region; however, the propagation pace of the messages stays low.

Physical Layer:

The IEEE 802.15.4 physical layer gives primary services:

The information carrier and the control carrier.

Data carrier lets in transmitting and receiving packets (physical layer data units) throughout the wireless channel.

Each packet includes the subsequent primary components:

SHR, which lets in a receiving tool to synchronize and lock into the bitstream PHR, which includes frame duration information a variable-length payload, which incorporates the MAC sublayer frame Start of Frame Delimiter (SFD) suggests the cease of the SHR and the beginning of the message information. The preamble subject this is used for synchronization collectively with the SFD subject shapes the SHR (SyncH) header. PHR header suggests the duration of the PSDU (PHY Service Data Unit) payload which has a non-constant value that is less than <128 bytes. The predominant capabilities of the physical layer consist of the activation and deactivation of the radio transceiver, the energy detection (ED, from RSS), the link quality indication (LQI), the clear channel assessment (CCA) and the dynamic channel choice through scanning a listing of channels looking for a beacon. ED method consists of an assessment of the acquired signal's strength and the end result is saved so as to be utilized by better layers. LQI determines a method in line with which, while a packet is acquired inside the physical layer, and assessment of its fine is done primarily based totally at the cost of ED. Moreover, in the course of CCA, the channel is checked so as to discover if it is busy or idle.

	Frequency band	Coverage	Channels	Data rate
Physical layer	2.4 - 2.4835 GHz	Global	16	250 Kbps
	902.0 - 928.0 MHz	America	10	40 Kbps
	868 - 868.6 MHz	Europe	1	20 Kbps

Table 1: Characteristics of IEEE 802.15.4 Physical layer

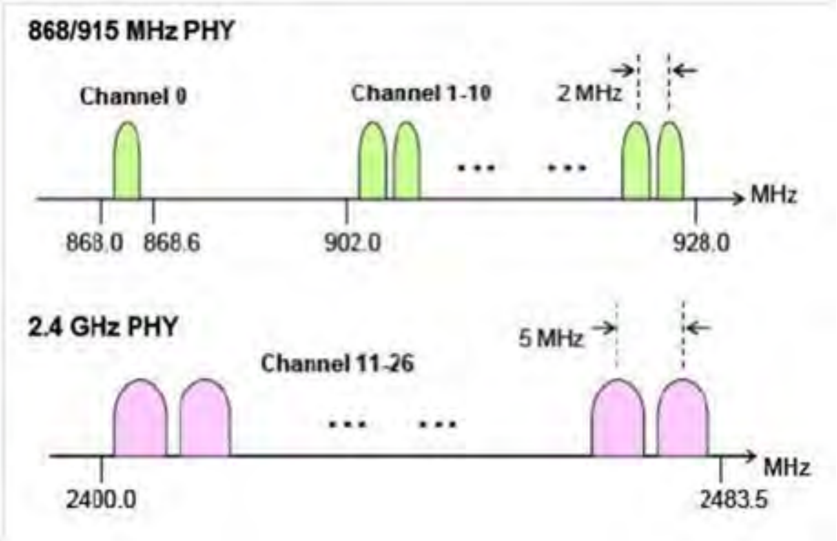


Figure 16: Frequency channels of the IEEE 802.15.4 standard

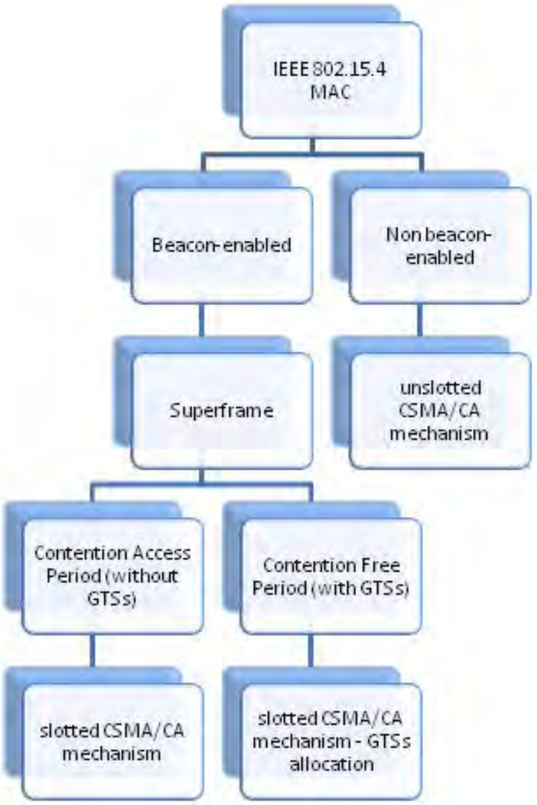

IEEE 802.15.4 MAC
Beacon-enabled
Non beacon-enabled
Superframe
unslotted CSMA/CA mechanism
Contention Access Period (without GTSs)
Contention Free Period (with GTSs)
slotted CSMA/CA mechanism
slotted CSMA/CA mechanism - GTSs allocation

Figure 17: MAC options in IEEE 802.15. 4

MAC Layer:

The IEEE 802.15.4 MAC layer offers services; information provider and control provider. The information provider lets in transmitting and receiving packets i.E, MAC layer information units via the interplay with the information provider of the IEEE 802.15.4 physical layer. The important functions of the MAC layer encompass the beacon control, the channel gets admission to, GTS (Guaranteed Time Slots) control, frame validation, acknowledged frame delivery, and the affiliation and disassociation with the PAN. There are distinctive channel get admission to mechanisms. In the contention-based access mechanism (beacon-enabled network) a Carrier Sense Multiple Access / Collision Avoidance

(CSMA/CA) set of rules is applied via way of means of the devices on the MAC layer. On the opposite hand, the access without contention (non-beacon-enabled network) is solely managed via way of means of the PAN coordinator via way of means of suitable allocation of the GTSs.

Superframes:

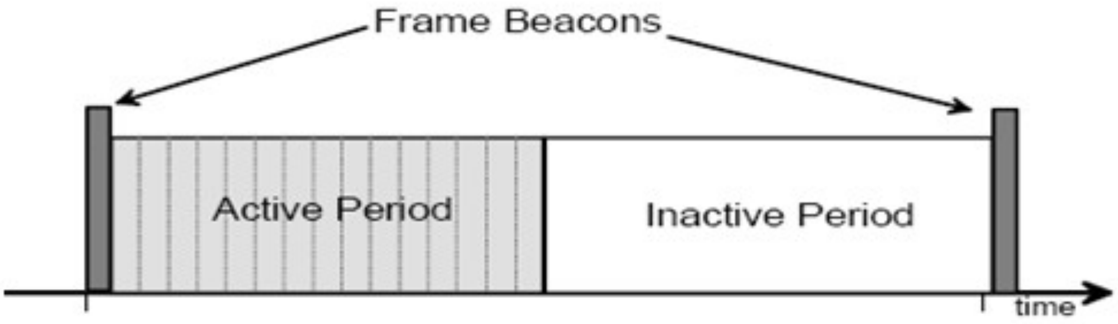


Figure 18: Super frame structure of IEEE 802.15.4

The layout of a super frame is decided via way of means of the PAN coordinator. It is commonly bounded via way of means of community beacon frames and divided into sixteen similarly sized slots. The beacon body is despatched inside the first slot of every super frame. If a coordinator does now no longer need to apply the super frame structure, it can turn off the beacon transmissions. The beacon frames are used as a way to synchronize the connected nodes, pick out the PAN, and describe the structure of the super frames. Beacons are despatched in the course of the primary slot of every super frame and they're turned off if a coordinator does now no longer use the super frame structure. During the active portion, communication is performed. In particular, the active duration is similarly divided into periods; the contention access period

(CAP) wherein any tool wishing to speak competes with other devices the usage of a slotted CSMA/CA mechanism and the contention-free period (CFP) which incorporates assured time slots. The PAN coordinator can also additionally allocate as much as seven GTSs wherein every of them can occupy multiple super frame slot duration. A GTS lets in a tool to function inside a part of the super frame this is devoted solely to it. A tool tries to allocate and use a GTS simplest if it is monitoring the beacons. As far because the GTS allocation is concerned, it is undertaken via way of means of the PAN coordinator only. A GTS is used only for communications among the PAN coordinator and a tool and its course is distinctive as both transmit or receive. On the contrary, inside the inactive portion, a node does now no longer has interaction with its PAN and might input a low-power mode.

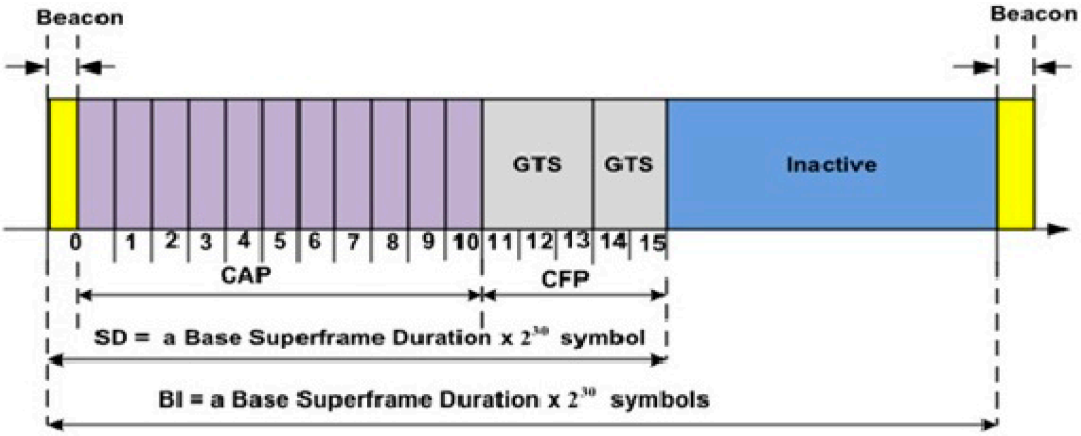

Beacon
Beacon
GTS
GTS
Inactive
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
CAP
CFP
SD = a Base Superframe Duration x 2^{SO} symbol
BI = a Base Superframe Duration x 2^{BO} symbols

Figure 19: GTSs in a IEEE 802.15.4 super frame

5

ROUTING PROTOCOLS FOR WIRELESS SENSOR NETWORKS

The important mission of wireless sensor nodes is to sense and accumulate information from a target domain, process the information, and transmit the data returned to particular sites in which the underlying application resides. Achieving this task effectively calls for the improvement of an energy-efficient routing protocol to installation paths among sensor nodes and the data sink. The path choice has to be such that the life of the network is maximized. The traits of the surroundings inside which sensor nodes generally operate, coupled with extreme aid and energy limitation, make the routing hassle very challenging.

5.1 Classification of WSN Routing Protocols

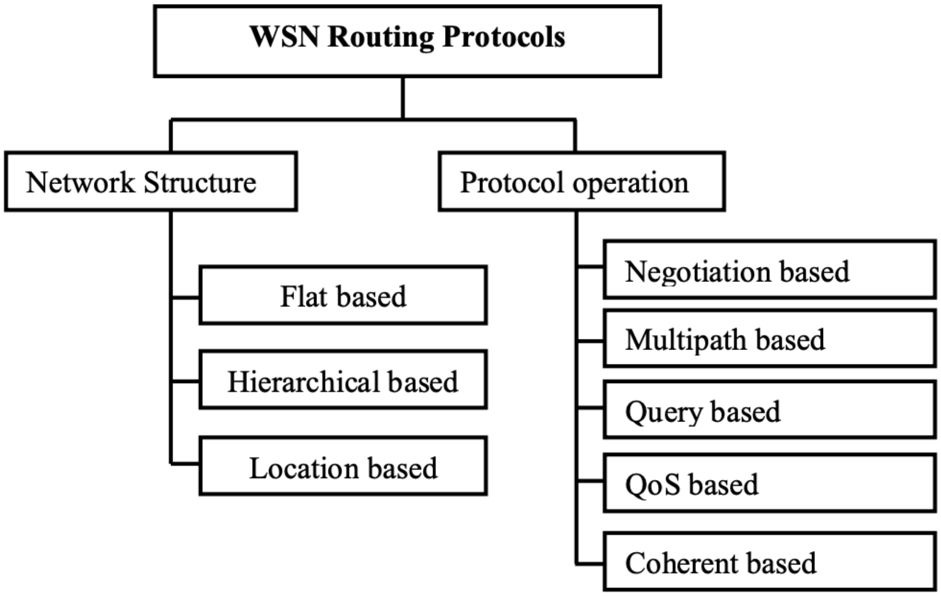


Figure 20: Classification of WSN Routing Protocols

A. **Flat based:** In flat-based protocols all nodes play an identical position and there may be truly no hierarchy. Flat routing protocols distribute data as had to any accessible sensor node inside the sensor cloud. No attempt is made to prepare the network or its site visitors, only to find out the nice path hop with the aid of using hop to a destination with the aid of using any route.

B. **Hierarchical based:** Hierarchical based routing protocols got down to try to preserve energy with the aid of using arranging the nodes into clusters. Nodes in a cluster transmit to a head node inside near proximity which aggregates the accumulated data and forwards it to the base station. Good clustering protocols play a crucial function in network scalability in addition to energy-efficient communication. On the poor aspect of it, clusters may also cause a bottleneck. This is due to the fact that only one head communicates on behalf of the whole cluster. Energy depletion may be most powerful in that head.

C. **Location-based:** In Location-based routing protocols, location data is used to calculate the gap among specific nodes in order that energy intake may be estimated.

D. **Multi-path based:** Multi-path based community derives benefit from the truth that there can be a couple of paths among a node and the destination. Using other paths guarantees that energy is depleted uniformly and no single node bears the brunt. This may be multiplied with the aid of using preserving a couple of paths among the source and the destination on the price of multiplied energy intake and visitors generation. These alternate paths are saved alive with the aid of using sending periodic messages. Hence, network reliability may be multiplied on the price of the multiplied overhead of preserving the trade paths.

E. **Query-based:** In Query-based protocols, the point of interest lies at the propagation of queries in the course of the network with the aid of using the nodes which require a few information. Any node which gets a query and additionally has the requested information, replies with the information to the inquiring for node. This method conserves energy with the aid of using minimizing redundant or non-requested information transmissions.

F. **Negotiation based:** In negotiation based protocols, the nodes exchange various of messages among themselves earlier than the transmission of information. The gain of that is that redundant information transmissions are suppressed. It must but be ensured that the negotiation transmissions aren't allowed to exceed the volume that the energy-saving gain is offset with the aid of using the negotiation overhead.

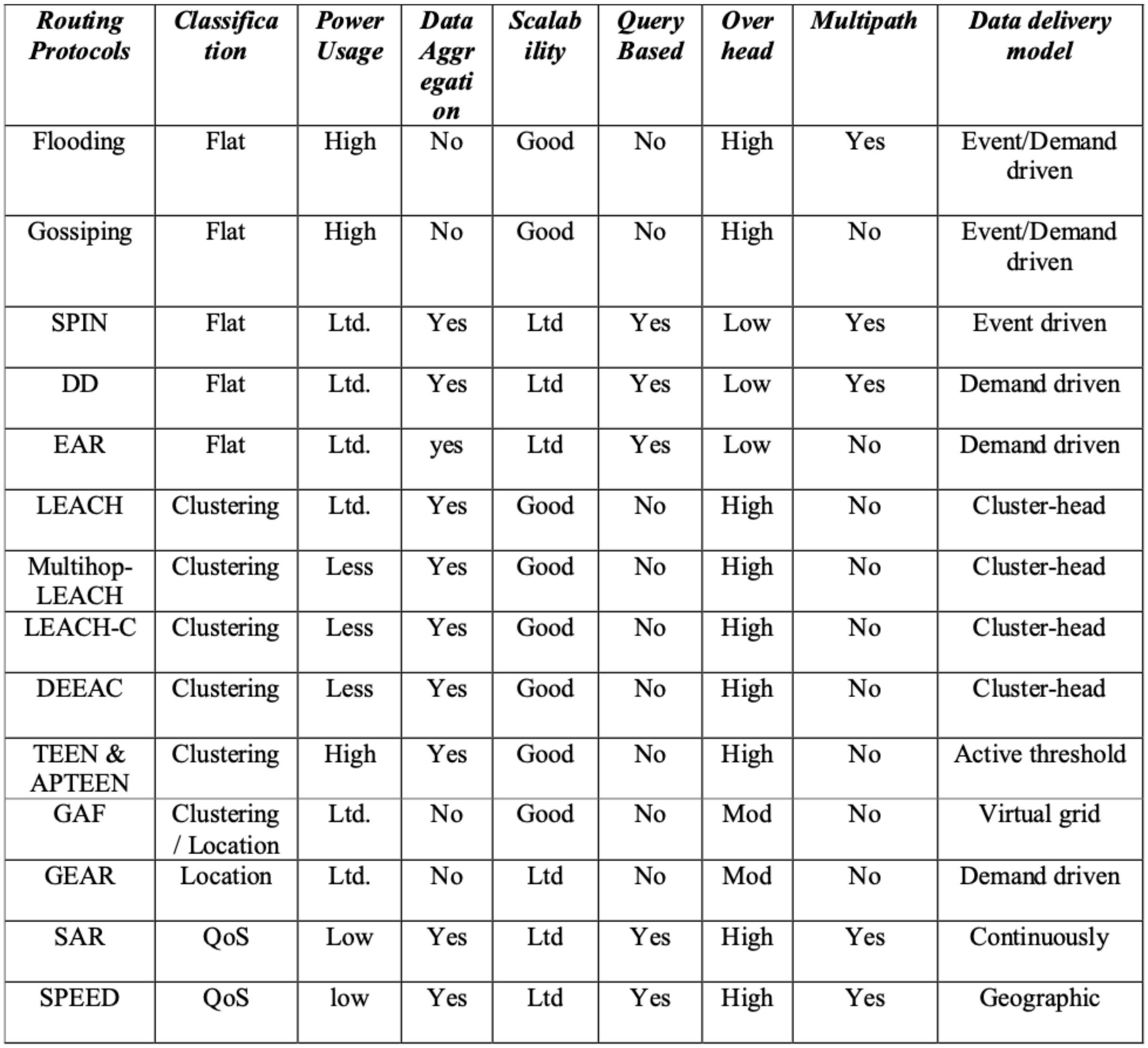
G. **QoS based protocols:** In QoS-based routing protocols, the network has to balance among energy intake and information quality. In specific, the network has to fulfill sure QoS metrics, e.G., delay, energy, etc. QoS based protocols must discover a trade-off among energy intake and the quality of service. An excessive energy intake route or method can be followed if it improves the QoS. So while inquisitive about energy conservation, those varieties of protocols are normally now no longer very beneficial and need to be avoided. The SPEED protocol is some other QoS routing protocol for WSNs that gives smooth real-time end-to-end ensures became introduced.

H. **Coherence based:** Coherence based protocols attention on how tons information processing takes region at every node. Incoherent protocols, information is despatched to an aggregator node after minimal feasible processing, and in addition, the processing is then completed on the aggregator. Coherent processing is normally followed for energy-efficient routing due to the fact they lessen the computation steps according to the node. However, the aggregator nodes need to have extra energy than the alternative ordinary nodes, in any other case, they'll be depleted rapidly.

5.2 Routing strategies in WSNs

The WSN routing problem provides a totally tough venture that may be posed as a traditional trade-off among responsiveness and performance. This trade-off needs to stabilize the want to deal with the restricted processing and communication abilities of sensor nodes in opposition to the overhead required to conform to those. In a WSN, overhead is measured usually in phrases of bandwidth utilization, power consumption, and the processing necessities at the mobile nodes. Finding a method to stabilize those competing desires effectively forms the idea of the routing venture. Furthermore, the intrinsic traits of wireless networks supply upward thrust to the crucial question of whether or not or now no longer current routing protocols designed for ad hoc networks are enough to fulfill this venture.

Routing algorithms for ad hoc networks may be categorized in step with the way wherein data is obtained and maintained and the way wherein this data is used to compute paths based on the obtained data. Three distinct techniques may be identified: proactive, reactive, and hybrid. The proactive approach, additionally called table-driven, is based on periodic dissemination of routing data to keep steady and correct routing tables throughout all nodes of the network.



Routing Protocols	*Classification*	*Power Usage*	*Data Aggregation*	*Scalability*	*Query Based*	*Over head*	*Multipath*	*Data delivery model*
Flooding	Flat	High	No	Good	No	High	Yes	Event/Demand driven
Gossiping	Flat	High	No	Good	No	High	No	Event/Demand driven
SPIN	Flat	Ltd.	Yes	Ltd	Yes	Low	Yes	Event driven
DD	Flat	Ltd.	Yes	Ltd	Yes	Low	Yes	Demand driven
EAR	Flat	Ltd.	yes	Ltd	Yes	Low	No	Demand driven
LEACH	Clustering	Ltd.	Yes	Good	No	High	No	Cluster-head
Multihop-LEACH	Clustering	Less	Yes	Good	No	High	No	Cluster-head
LEACH-C	Clustering	Less	Yes	Good	No	High	No	Cluster-head
DEEAC	Clustering	Less	Yes	Good	No	High	No	Cluster-head
TEEN & APTEEN	Clustering	High	Yes	Good	No	High	No	Active threshold
GAF	Clustering / Location	Ltd.	No	Good	No	Mod	No	Virtual grid
GEAR	Location	Ltd.	No	Ltd	No	Mod	No	Demand driven
SAR	QoS	Low	Yes	Ltd	Yes	High	Yes	Continuously
SPEED	QoS	low	Yes	Ltd	Yes	High	Yes	Geographic

Table 2: Classification and comparison of Routing Protocols in WSN

The structure of the community may be both flat or hierarchical. Flat proactive routing techniques have the capability to compute the highest quality paths. The overhead required to compute those paths can be prohibitive in a dynamically converting environment.

Hierarchical routing is higher applicable to fulfill the routing needs of massive ad hoc networks. Reactive routing techniques set up routes to a restricted set of locations on demand. These techniques do now no longer commonly keep worldwide records throughout all nodes of the network. They need to, consequently, depend upon a dynamic path search to set up paths among a supply and a destination. This typically includes flooding a path discovery query, with the replies traveling back alongside the opposite path. The reactive routing techniques range inside the manner they manipulate the flooding procedure to lessen communication overhead and the manner wherein routes are computed and reestablished whilst a failure occurs.

Hybrid techniques depend upon the life of network structure to obtain balance and scalability in massive networks. In those techniques, the community is prepared into at the same time adjoining clusters, which might be maintained dynamically as nodes are part of and depart their assigned clusters. Clustering gives a structure that may be leveraged to restrict the scope of the routing set of rules response to adjustments inside the network environment. A hybrid routing method may be followed wherein the proactive routing is used inside a cluster and reactive routing is used throughout clusters. The major venture is to lessen the overhead required to keep the clusters. In summary, conventional routing algorithms for ad hoc networks have a tendency to showcase their least ideal conduct below quite dynamic conditions. Routing protocol overhead commonly will increase dramatically with expanded network length and dynamics.

A massive overhead can effortlessly weigh down network resources. Furthermore, conventional routing protocols working in massive networks require large inter-nodal coordination, and in a few instances worldwide flooding, to keep steady and correct data, that is important to obtain loop-free routing. The use of those strategies will increase routing protocol overhead and convergence times.

6

TRANSPORT CONTROL PROTOCOLS

6.1 TCP

TCP is the normally used connection-orientated transport manage protocol for the Internet. Some applications, which include FTP and HTTP, reside in the TCP layer. TCP makes use of network services supplied with the aid of using the IP layer, with the goal of providing dependable, orderly, controllable, and elastic transmission. TCP operation includes 3 levels:

1. Connection establishment. A logical connection for TCP is set up at some point in this phase. A logical connection is an affiliation among the TCP sender and receiver recognized uniquely with the aid of using the pair (IP address, TCP port identifier) of the TCP sender and receiver. There can be numerous connections among endpoints at the same time. These connections have an identical IP address, however, they may have different TCP port identifiers. TCP makes use of a 3-manner handshake to set up a connection. During the handshake, the TCP sender and receiver will negotiate parameters which include preliminary sequence number, window size, and others, and notify every difference that information transmission can begin.

2. Data transmission. TCP gives dependable and orderly transmission of data among the sender and the receiver. TCP makes use of accumulative ACK to get back misplaced segments. The orderly transmission is found out thru the sequence number inside the segment header. Furthermore, TCP helps flow manage and congestion manage thru adjustment of transmission rate with the aid

of using the sender. TCP makes use of a window-based mechanism to carry out this task, wherein the sender continues a variable congestion window. The TCP sender can transmit some of the segments much less than or identical to the congestion window is up to date after receiving the ACK from the receiver or after a timeout. Since ACK is used for each delivery notification and flow management, the 2 features are quite coupled. There are 3 phases inside the process of congestion control in TCP.

3. Disconnect. After completion of information transmission, the relationship could be eliminated and the associated aid released.

6.2 UDP

UDP is a connectionless delivery protocol. It exchanges datagrams without a sequence number, and if the data is misplaced inside the procedure of exchange among the transmitter and the receiver, this protocol does now no longer have the mechanisms to get back it. Since it does now no longer provide a sequence number inside the datagrams it, therefore, does now no longer assure orderly transmission.

It additionally does now no longer provide skills for congestion or flow management. In occasions in which each TCP and UDP are present, considering UDP does now no longer carry out congestion or flow control, it could turn out that it outperforms TCP. In current years a TCP-friendly rate control TFRC has been proposed for UDP to put in force a sure degree of manipulate on this protocol. The simple concept at the back of TFRC is to offer nearly the same throughput to each TCP and UDP while they're present on a connection.

6.3 Feasibility of Using TCP or UDP for WSNs

Although TCP and UDP are famous transport protocols and deployed extensively on the Internet, neither can be a very good preference for WSNs. For the maximum part, there's no interplay among TCP or UDP and the lower-layer protocols. In wireless sensor networks, the lower layers can offer wealthy and beneficial data to the transport layer and enhance the badly wanted system performance. Following are different issues that make both TCP or UDP improper for implementation in WSNs:

1. TCP is a connection-oriented protocol. However, in WSNs, the wide variety of sensed information for event-based packages is normally very small. The three-manner handshake method required for TCP is a massive overhead for the sort of small extent of information.

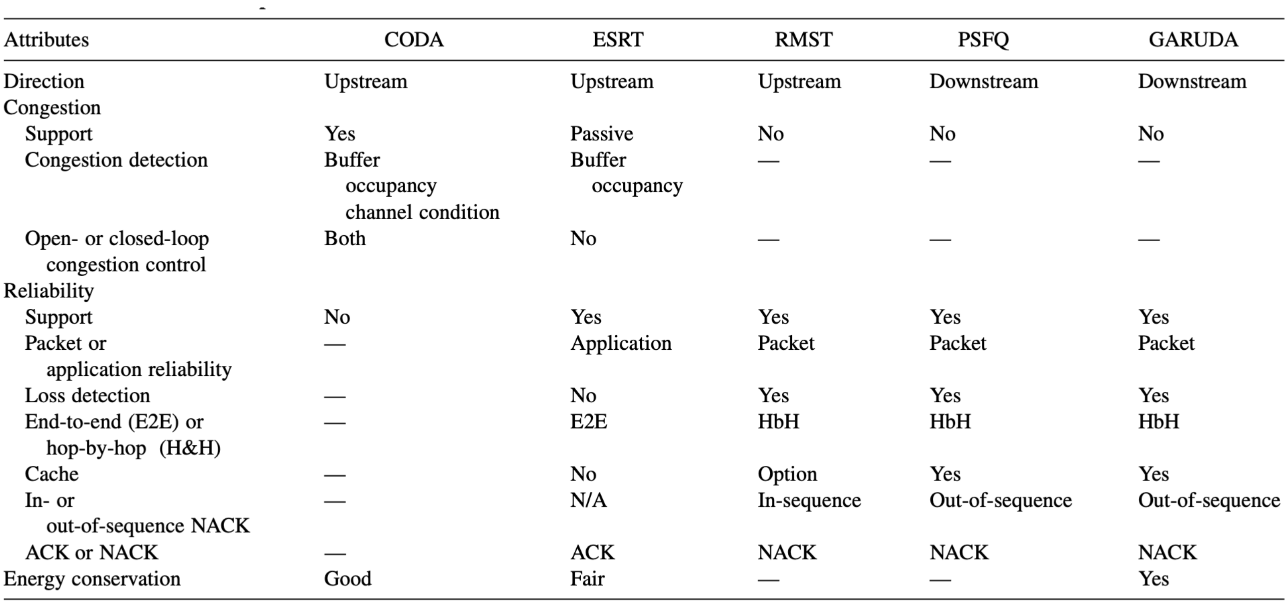
2. In TCP, segment loss can probably cause window-based to go with the drift and congestion manage. This will lessen the transmission charge unnecessarily whilst, in fact, packet loss may also have taken place because of hyperlink mistakes and there can be no congestion. This conduct will result in low throughput, especially under a couple of wireless hops, which can be usual in WSNs.

3. TCP makes use of an end-to-end procedure for congestion control. Generally, these outcomes in longer reaction to congestion, and in turn, will bring about a massive quantity of segment loss. The section loss, in turn, outcomes in energy waste inside the retransmission. Furthermore, an extended reaction time to congestion outcomes in low throughput and usage of wireless channels. TCP makes use of end-to-end ACK and retransmission whilst necessary. This will bring about tons of lower throughput and

longer transmission time whilst RTT is long, as is the case in maximum WSNs.

4. Sensor nodes can be inside a specific hop count and RTT from the sink. The TCP operates unfairly in such environments. The sensor nodes close to the sink may also acquire greater possibilities to transmit (which ends up in them depleting remote nodes and the sink. As a connectionless transport control protocol, UDP is likewise now no longer appropriate for WSNs.

Most recent Transport Protocols may be grouped in one of the 4 groups: upstream congestion management, downstream congestion management, upstream reliability assurance, and downstream reliability assurance.



Attributes	CODA	ESRT	RMST	PSFQ	GARUDA
Direction	Upstream	Upstream	Upstream	Downstream	Downstream
Congestion					
Support	Yes	Passive	No	No	No
Congestion detection	Buffer occupancy channel condition	Buffer occupancy	—	—	—
Open- or closed-loop congestion control	Both	No	—	—	—
Reliability					
Support	No	Yes	Yes	Yes	Yes
Packet or application reliability	—	Application	Packet	Packet	Packet
Loss detection	—	No	Yes	Yes	Yes
End-to-end (E2E) or hop-by-hop (H&H)	—	E2E	HbH	HbH	HbH
Cache	—	No	Option	Yes	Yes
In- or out-of-sequence NACK	—	N/A	In-sequence	Out-of-sequence	Out-of-sequence
ACK or NACK	—	ACK	NACK	NACK	NACK
Energy conservation	Good	Fair	—	—	Yes

Table 3: Various Transport protocols for WSNs

6.4 Problems with Transport Control Protocols

The major functions of transport protocols for wireless sensors networks that should be considered carefully in the design of these protocols are congestion control, reliability guarantee, and energy conservation. Most of the existing protocols reviewed here and reflected in the literature provide either congestion or reliability in either upstream or downstream (not both). Certain applications in wireless sensor networks require it in both directions: for example, re-tasking and critical time- sensitive monitoring and surveillance operations. Another problem with the existing transport protocols for wireless sensor networks is that they only control congestion either end-to-end or hop-by-hop. Although in CODA there are both end-to-end and hop-by-hop mechanisms for congestion control, it uses them simultaneously rather than adaptively.

An adaptive congestion control that integrates end-to-end and hop-by-hop mechanisms may be more helpful for wireless sensor networks with diverse applications, and useful due to energy conservation and simplification of sensor node operation. Transport protocols studied so far provide either packet- or application-level reliability (if reliability is provided at all). If a sensor network supports two applications, one that requires packet-level reliability and the other application-level reliability, the existing transport control protocols will face difficulty. None of the existing transport protocols implement cross-layer optimization. As discussed earlier, lower layers, such as the network and MAC layers, can provide useful information to the transport layer.

7

NODE LOCALIZATION

Generally, the procedure for acquiring a region estimate entails specific degrees of complexities. From this radio frequency (RF) waveform, it's far viable to extract the applicable range measurements. On the opposite hand, for TOA primarily based systems, the distance is predicted by means of sending an RF signal and recording the time it takes to get hold of it.

7.1 Localization of Wireless Sensor Node

The predominant distinction among conventional localization and WSN localization is cooperative localization. Cooperative localization refers back to the collaboration among sensor nodes to estimate their area data. In conventional wireless networks, range data is transferred among RPs to an MT(Mobile Terminal). The RP(Anchor/Reference Point)s are terminals with a few a priori understanding in their personal coordinates, typically preprogrammed or received with a few minor uncertainty via GPS. In WSNs, RPs are regularly known as anchors, and MTs are known as either nodes or blind nodes.

7.1.1 Cooperative Localization

The WSN cooperative localization is typically carried out via predominant approaches: centralized and distributed. The difference is the reliance of the previous on committed hardware to clear up an optimization hassle. The latter, however, permits individual sensor nodes to share range data to attain a few worldwide area estimates. In centralized localization, huge analytical computations are completed to clear up an optimization hassle of the whole network. Naturally, this complicated computation technique calls for a significant processing unit external to the sensor network that plays the localization method and informs the network of the solution. In either technique, worldwide area estimates can best be carried out if anchors are used. In the absence of anchors, only relative area estimates are possible. The overall performance of WSN localization algorithms may be decided via thoroughly set up CRLB evaluation that has these days attracted interest from specific students and researchers. The definitions of the certain, and hence the analytical derivation involved, are similar, however, they typically fluctuate of their assumptions approximately the traits of the corrupting noise.

Due to its simplicity and applicability to sensor networks, we now offer an outline of the CRLB evaluation supplied for an impartial estimate of the sensor positions. Although this isn't always the case in positive environments, for instance, indoors, it provides, nonetheless, a completely vital analytical basis for analyzing the localization overall performance in WSNs.

The WSN algorithms have to then evaluate the localization overall performance to the broadly to be had CRLB evaluation inside the literature. One vital be aware right here is that each the bound and the set of rules overall performance depend especially on the information of the ranging error. Although sensor density and geometry have an effect on the overall performance, the facts of the ranging blunders especially offer the primary venture for correct localization. If the ranging mistake assumptions taken into the algorithm and the CRLB evaluation do now no longer reflect the real conduct of the propagation channel, both the set of rules overall performance and the bound can be nonrealistic.

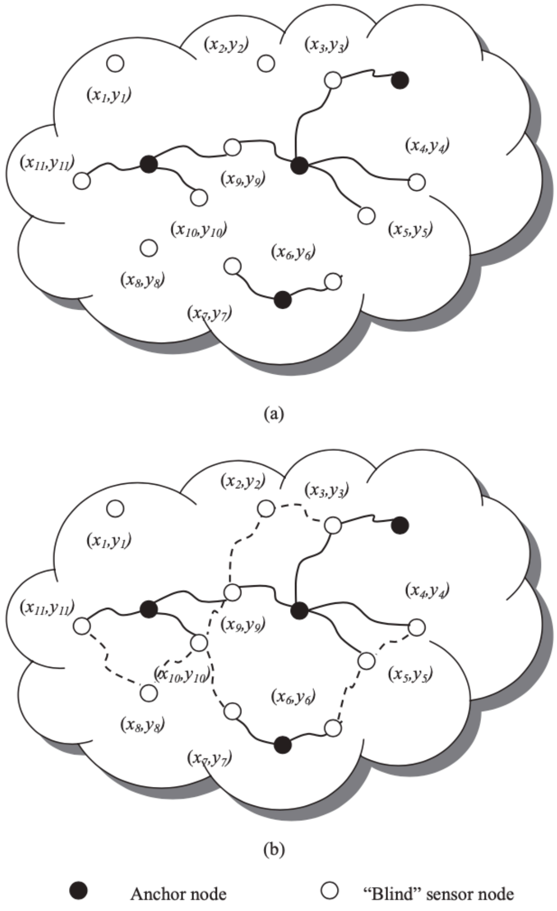


Figure 21: Cooperative localization: (a) Traditional wireless networks. (b) WSNs.

7.1.2 Centralized Localization

This section introduces examples of famous centralized algorithms. With this set of rules, the peer-to-peer communication inside the network is modeled as a set of geometric constraints on the node location.

Thus for nodes working with a particular sort of RF ranging (RSS or TOA), the restrictions for the estimates of the area may be furnished in a place bounded by the set of constraints. For instance, ranging from RSS or TOA causes the restrictions to be based on the radial communication coverage. As the wide variety of anchors will increase, the restrictions yield smaller viable sets As the wide variety of constraints will increase, the accuracy of estimating the node location will increase. In convex position estimation, the hassle is considered as a graph with the nodes placed on the vertices and the bidirectional communication constraints as the edges. Using the proximity constraints and the N sensor nodes and M anchor nodes, it is feasible to estimate the placement of the sensor nodes.

The complexity of the method calls for centralized computation. Thus all nodes ought to communicate their connectivity data to an outside pc as a way to resolve the optimization hassle. The principal gain of this set of rules is that each one connectivity data in a single community is used to attain the answer. The disadvantage, however, is that the communication load among the nodes and the pc can also additionally create a bottleneck that interprets right into a hindrance on the dimensions of the deployed sensor network. The set of rules additionally affords a rectangular upper bound on every viable set received thru the solution. Naturally, the accuracy of this set of rules relies upon on the sensor node density. As the radius of connectivity will increase, the wide variety of connections will increase, that's equal to a growth in node density. The stronger connectivity (or better node density) improves the imply error performance. Similarly, because the wide variety of anchors will increase, the mistake extensively decreases. These network parameters spotlight the significance of preserving enough node densities as a way to attain an appropriate localization performance. The different famous set of rules is Multi-Dimensional Scaling (MDS). This set of rules has been carried out inside the fields of machine learning and computational chemistry, wherein it includes a set of information evaluation strategies that show the structure of distance-like information as a geometric picture. The MDS set of rules starts with one or more distance matrices derived from points in a multidimensional area. It is normally used to discover a placement of the points in a low-dimensional area. It is regularly used as a part of exploratory information evaluation or data visualization. In classical MDS, the information is quantitative and the proximities of objects are dealt with as distances in a Euclidean space. One gain of this set of rules is that regardless of the mistake present, the answer furnished may be dependable because of the overdetermined nature of the answer. The simple classical MDS includes 3 steps. The first is to compute the shortest paths among all pairs of nodes inside the areas under consideration. These shortest-path distances are used to assemble the distance matrix. The 2nd is to use MDS to the distance matrix, wherein the 2(3) biggest eigenvalues and eigenvectors assist to assemble a 2D(3D) relative map. Finally, with enough anchors, it is feasible to convert the relative map to an absolute map based on the absolute coordinates of the anchors.

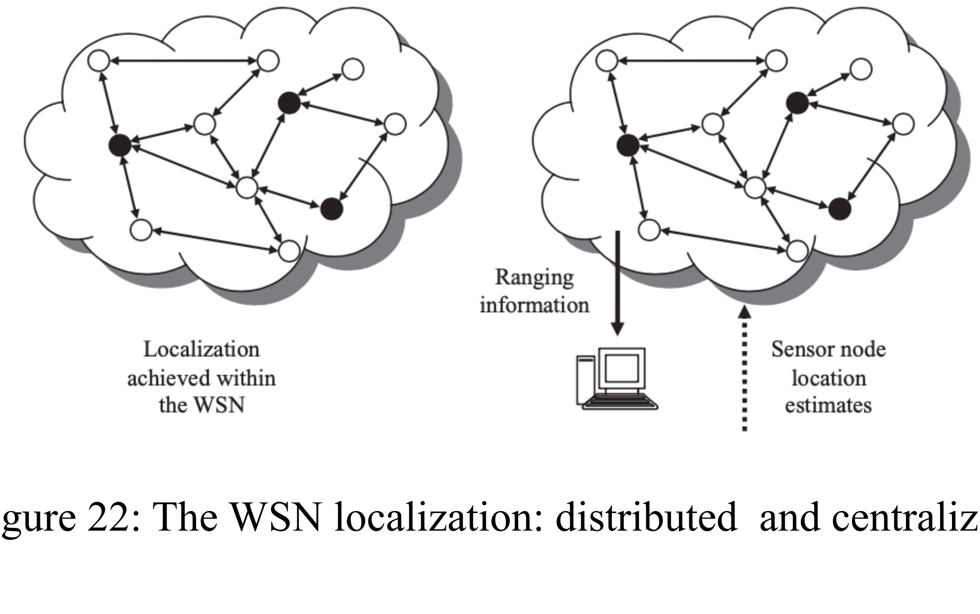


Figure 22: The WSN localization: distributed and centralized.

7.1.3 Distributed Localization

These algorithms attain an approximation based on the range. Extended ranging (ER) based and Direct ranging (DR) based are two types of this localization. Figure 23 is Direct Ranging and 24 is Extended Ranging. ER based algorithms are normally known as multi hop network localization (MNL) and DR based algorithms are normally known as recursive position estimation (RPE). Note that one downside of this set of rules is that it's far viable that a few nodes on the brink of the network lack enough direct connectivity anchors and accordingly are not able to localize themselves.

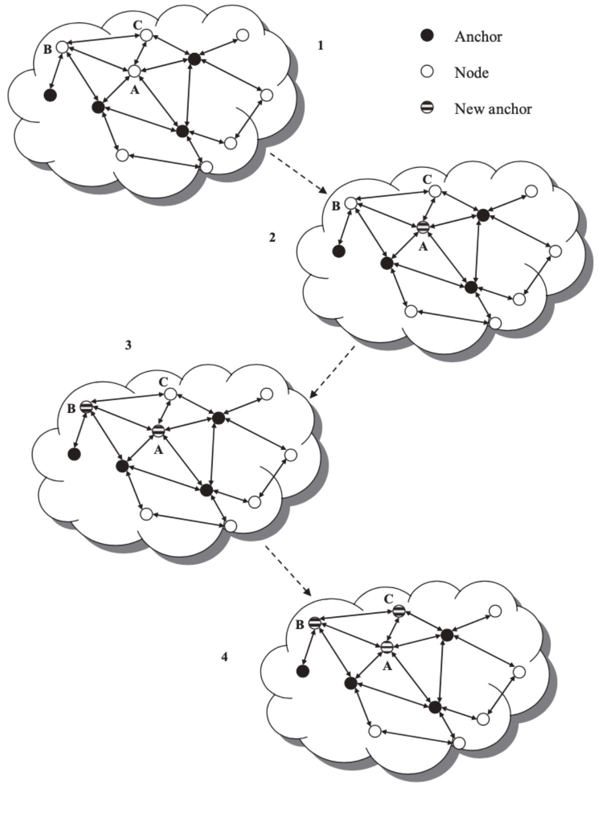


Figure 23: Recursive position estimation distributed localization

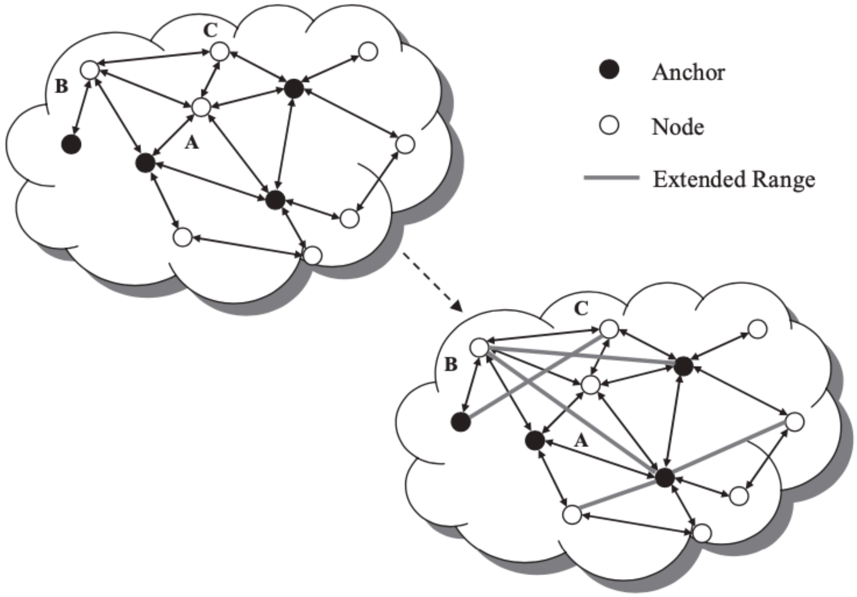


Figure 24: Multi hop distributed localization

Intuitively, the DR primarily based algorithms are more accurate due to the fact there are no blunders accumulation inside the range information. The advantages consist of very correct localization and considerably much less blunders propagation. The ER based algorithms were used inside the N-hop multi lateration, robust positioning set of rules, and ad hoc positioning set of rules.

The MNL set of rules is less difficult to enforce than the RPE set of rules due to the fact the multi hop positioning set of rules calls for not less than 3 reference nodes in the entire operational field, assuming mobile nodes can communicate with all reference nodes thru multi hop communications, whilst the RPE set of rules has a stricter requirement at the deployment density of reference nodes and mobile nodes.

It is reasonable to anticipate progressed overall performance by integrating the 2 algorithms. For example, the MNL set of rules may be carried out as a supplement of the RPE set of rules; that is, the iterative multi lateration set of rules can be used every time it's far viable and while it isn't viable, the multi hop positioning set of rules can be used to achieve a rough estimate of the area coordinates of the remaining mobile nodes.

8

NETWORK SECURITY AND ATTACK DEFENSE

Network security is a research area that entails many technical issues. To shield a network, there are generally numerous security requirements, which need to be taken into consideration inside the layout of a security protocol, which include confidentiality, integrity, and authenticity.

8.1 Confidentiality

Confidentiality is a guarantee of legal entry to data. In the context of networking, confidentiality means that the data about communications need to be stored secret from anybody without legal entry permission.

Eavesdropping

Providing confidentiality is a tough mission in wireless networks. The primary hassle is that the radio spectrum is an open useful resource and may be utilized by anybody geared up with right radio transceivers. An attacker can listen in on the packets transmitted inside the air so long as he's capable of preserve track of the radio channels used inside the communication. In general, a packet incorporates an information portion, referred to as a protocol data unit (PDU), and a header. A packet header incorporates the network addresses of the source and destination nodes, which can be used for intermediate nodes to course the packet from the source to the destination, and different control data, which describes the assets of the PDU and/or tells a way to method the PDU. At every hop alongside the path from the source to the destination, the packet is encapsulated into one or more than one link-layer frames. Similar to a packet, a frame additionally incorporates a link-layer PDU and a frame header. The frame header incorporates the medium get entry to manage (MAC) addresses of neighboring nodes alongside the path from the source to the destination, in addition to different frame manage data. Without the right protection, the PDU of a packet might be disclosed to the public. If the PDU incorporates crucial data, for example, enterprise or navy secrets and techniques, this data disclosure will cost invaluable loss. Moreover, the packet header and the frame header also are of interest to attackers. Since the headers incorporate data about the communicating nodes and PDUs, the disclosure of headers will result in the privateness hassle. For example, an attacker can discover visitors flow based on the source and the destination addresses contained inside the packet headers. By monitoring the drift, the attacker can decide the area of the source node or the destination node. In the programs of tracking wild lives, the area of the source node can suggest the advent of the wild animals, that's appealing to unlawful hunters. In addition to packet headers, an attacker also can listen in on manipulate or control packets exchanged amongst nodes, inclusive of routing preservation packets, after which derive the network topology from them. This renders the attacker the capacity to decide the identities and places of all of the nodes of interest. By attacking the ones crucial nodes, the attacker can break the network very easily. An active attack failing confidentiality is referred to as node compromise. In an instantaneous way, an attacker can seize a node, dig into it with unique tools, and discover beneficial information. In an oblique way, the attacker can derive the secrets and techniques in a node without capturing it, which may be accomplished with the aid of using studying the secret information gathered from different compromised nodes and/ or packet PDUs. Under the attacker’s manipulate, the brand new compromised node may be used to release greater malicious assaults. Node compromise is one of the maximum adverse assaults to WSNs. A WSN is generally deployed in adversarial surroundings, for example, military battlefields. Continuously tracking the network in such surroundings isn't always guaranteed. This renders attackers the possibility to compromise sensor nodes. Because sensor nodes are manufactured as low-cost devices without robust protection, node compromise maybe instead easy in WSNs.

Privacy

Privacy is turning into a totally critical protection issue as the concerns at the disclosure of private data, for example, identification to unauthorized attackers, are becoming a great deal stronger. As mentioned before, an attacker can track visitors waft to discover the identities and then the places of the source and destination nodes. In WSNs, this area monitoring may be less complicated due to the fact in maximum situations sensor nodes are static. From the network administrator’s factor of view, it is ideal if the area data of the source and destination nodes may be hidden from attackers. As mentioned inside the preceding section, encryption is a way to shield the privateness of node identities and for this reason, recognize nameless communications to a point on the value of expanded routing inefficiency. A link-layer symmetric key is used to encrypt frame PDUs and the corresponding MAC addresses in frame headers. In order to preserve the frame forwarding function, node anonymous are used as new MAC addresses. A comparable technique is taken in MASK, anonymous on-demand routing protocol, however, MASK makes use of link anonymously to discover links and forward frames. There are different strategies using non-cryptographic designs to shield privateness. For example, the source area privateness may be very critical in WSNs due to the fact the vicinity of the source is normally a place in which a target of excessive price is located. In order to enhance the source area privateness, a brand new routing protocol, referred to as phantom routing is explored. A subsequent flooding/single-path routing phase for handing over the packet to the destination. The phantom routing substantially will increase the source area privateness via way of means of introducing phantom sources while marginally growing the communication overhead as compared with the flooding and the single-route routing. The destination area privateness is a dual hassle to the source area privacy. The base station can emerge as a failure factor of interest to attackers due to the fact all traffic flows will undergo it. In order to conceal the vicinity of the base station, fake traffic is replicated in which every forwarding node creates faux traffic flows towards the guidelines contrary to the destination in any such manner that the traffic pattern inside the network is sort of evenly distributed.

8.2 Integrity

Integrity is a guarantee that packets aren't changed in transmission. This is a primary requirement for communications due to the fact the receiver wishes to recognize precisely what the sender needs her to recognize. However, this isn't always a smooth mission in wireless communications.

Transmission Errors

Transmission mistakes are inherent in wireless communications due to the instability of wireless channels, that's because of many reasons, for example, channel fading, time-frequency coherence, and inter-band interference. A packet bearing mistakes is useless and causes greater processing on the sender and the receiver.

Processing Errors

Errors also can occur in every forwarding node due to the fact no electronic devices are perfect. When the operation conditions, for example, temperature or humidity, are out of the normal range, electronic devices can run into malfunction, which could reason mistakes in packets. Those mistakes might not be observed via way of means of the forwarding node and accordingly, those error packets can also additionally still be despatched out, inflicting problems at downstream nodes.

Packet Modifications

In a hostile environment, an attacker can modify a packet earlier than it reaches the receiver. This can cause many problems. More severe damages may be brought on if the attacker is familiar with the packet layout and the semantic which means of the communication protocol. In that case, the attacker can modify a packet to change its content material in order that the receiver obtains the incorrect information. In a WSN, for example, a packet containing the area of a critical event may be changed in order that an incorrect area is suggested to the base station. Control and management packets may be modified in order that nodes have inconsistent expertise on the network topology, which causes many routing problems.

Error Control

There are a few error control mechanisms at the link-layer dealing with the transmission mistakes. The concept is to connect every link-layer frame with a few redundancy bits, that's calculated in keeping with an error detection algorithm and is typically known as a checksum. Each receiving node can discover whether or not there may be mistakes in an obtained frame via way of means of examining its checksum. If a mistake happens, the receiver can deliver a notice frame to the sender to request a retransmission of the original frame. This remarks mechanism is known as an automatic repeat request (ARQ). If extra redundancy bits are connected to every frame, the receiving node can also add even correct mistakes and accordingly avoiding ARQ. This mechanism is known as forward error correction (FEC) and the checksum in every frame is computed in keeping with a mistake correction code algorithm.

Both ARQ and FEC also can be used on the transport layer to address the processing mistakes incurred in intermediate forwarding nodes. The source node computes a checksum for every transport-layer PDU and the destination node inspects the checksum to discover or correct mistakes.

Message Integrity Code

Neither ARQ nor FEC may be used to address malicious amendment via way of means of attackers. The motive is that every one of the mistake detection/correction code algorithm is publicly properly known. The attacker can modify a frame and recalculate its checksum making it meaningless. Therefore, a receiving node can't discover the amendment due to the fact the modified frame fits its checksum. In order to assure integrity, cryptographic techniques may be used. One is message integrity code (MIC) and the alternative is the usage of a signature.

8.3 Authenticity

To identity communicating nodes authenticity is required. Every node wishes to realize that an obtained packet comes from an actual sender. Otherwise, the receiving node may be cheated into doing some incorrect actions.

Packet Injection

In addition to enhancing present packets, an attacker can at once inject packets if he is aware of the packet layout described inside the network protocol stack. The injected packets can convey fake information, which can be regularly occurring via way of means of receiving nodes. Applications deployed in a WSN, for instance, environmental tracking or item tracking, maybe disrupted via way of means of the fake information. The Sybil attack is a typical instance of packet injection. In a Sybil attack, an attacker illegitimately takes on a couple of identities via way of means of injecting fake packets containing spoofed source IP or MAC addresses, that could pose a severe chance to distributed storage, routing protocols, data aggregation, voting, honest useful resource allocation, intrusion detection, and so on.

Message Authentication Code

In order to cope with fake packets, authentication is fundamental to make sure the starting place of obtained packets. Message authentication code (MAC) is a device to remedy the problem. It also can be known as MIC as it guarantees packet integrity as well. To compute a MAC, asymmetric key shared among the sender and the receiver is required. The packet such as payload M and the MAC C is despatched to the receiver. The receiver recomputes a MAC C¢ with the payload M and the shared key K after which checks whether or not C¢ = C holds. If the equation holds, the payload M is authenticated and now no longer changed due to the fact most effective the sender is aware of the shared key.

Signature

Signature is an asymmetric key technique, that's broadly utilized in authentication. A sender node continues its personal key Ks in secret even as publishing its public key Kp. In order to authenticate a plaintext M to the receiver, the sender makes use of its personal key Ks to sign M right into a signature S = S(M, Ks) after which transmits the signature S, in addition to the plaintext M to the receiver. Only the sender can generate the signature because Ks is secret. Because Kp is publicly nicely-known, any receiver can affirm the signature S via way of means of inputting the signature S, the plaintext M, and the general public key Kp right into a verification set of rules M to compute V(S, M, Kp). If the output is TRUE, the plaintext M is authenticated, and in any other case now no longer.

Authenticating Public Key

The reason that the MiM assault is viable is that the authenticity of the general public key can not be assured. Therefore, authenticating public keys in asymmetric key systems is a totally vital problem. The traditional approach to the general public key authentication is to depend on a public key infrastructure (PKI). In the PKI, there may be a certificate authority (CA), that is relied on via way of means of all of the participants the usage of the PKI. The public key of the CA is accepted via way of means of all of the member nodes as an authenticated one in default. The CA signs the general public key of every member node and issues a certificate which includes the general public key and the corresponding signature to the member node. When nodes want to communicate, one in every of them sends its public key certificates to the alternative node which could confirm the authenticity of the general public key inside the certificates with the famous public key of the CA.

In this way, the 2 nodes can authenticate each other. In reality, a PKI may be defined as a multilevel tree. Public key certificates were extensively used inside the Internet and different wireless networks, for example, wireless local area networks (WLANs). Another method of authenticating public keys tries to keep away from public-key certificates via way of means of the usage of the symmetric key method or IBC. Merkle tree is a type of asymmetric method which uses public key authentication. The root may be recovered primarily based totally on every leaf node and its witness. The sensor node attaches its public key with its witness when it desires to authenticate its public key to other nodes. Other sensor nodes confirm whether or not they are able to get better the root wherein to authenticate the general public key. Otherwise, the MiM assault is viable. In the identification - based cryptography (IBC), however, this key-node binding relationship is eliminated due to the fact the publicly acknowledged identification records of a node are without delay used as its public key. Therefore, IBC gets rid of the need of a public-key certificate and consequently saves the price on certificates verification.

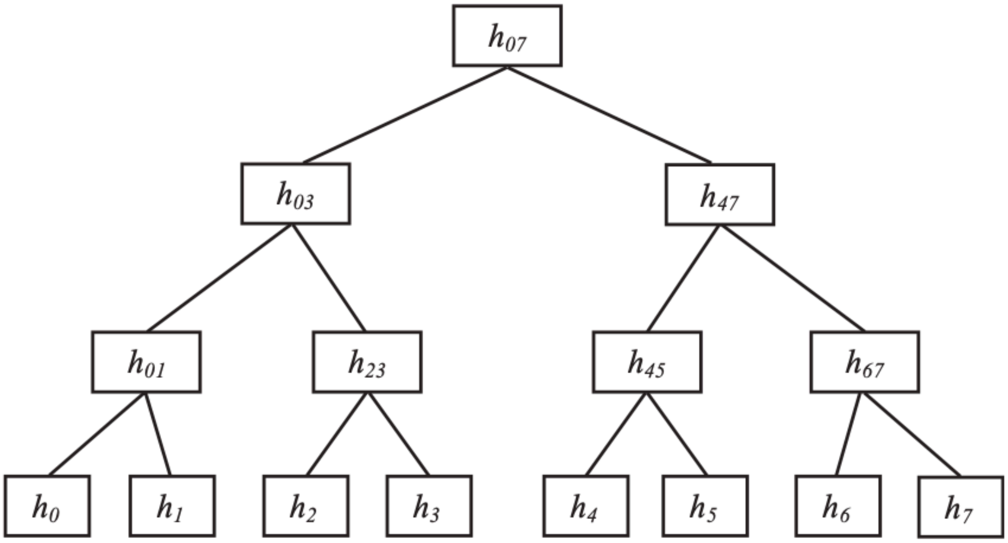


Figure 25: Sample of a Merkle Tree

9

CONCLUSION AND FUTURE TRENDS IN WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) have attracted incredible interest from the research community in current years. A substantial quantity of research work has been carried out to clear up the realistic and theoretical troubles which can be nonetheless open, which has ended in a surge of civil and army programs over the previous couple of years. In general, maximum sensor networks are designed for delay-tolerant and low-bandwidth programs.

Future studies on WSN may be directed in the direction of maximizing vicinity throughput in clustered Wireless Sensor Networks designed for temporal or spatial random process estimation, accounting for a radio channel, MAC, PHY and NET protocol layers and information aggregation techniques, simulation and experimental verification of lifetime-aware routing sensing spatial coverage and the enhancement of the preferred sensing spatial coverage assessment techniques with realistic sensor model. We agree with that inside the near future, WSN studies will place an exquisite effect on our each day lifestyles.

For example, it'll create a system for persistent observation of physiological alerts even as the patients are at their homes. It will decrease the value concerned with tracking patients and growth the efficient exploitation of physiological information and the patients can have get right of entry to the very best pleasant hospital treatment of their very own homes. Thus, it'll keep away from the misery and disruption due to a prolonged inpatient stay.

Acronyms

GPS	Global Positioning System
ADC	Analog to Digital Converter
QOS	Quality Of Service
TCP	Transport Control Protocol
WLANs	Wireless Local Area Networks
RF	Radio Frequency
ISM	Industrial, Scientific, and Medical
FEC	Forward Error Correction
ARQ	Automatic Repeat reQuest
MAC	Medium Access Control
SMP	Sensor Management Protocol
SQTL	Sensor Query and Tasking Language
SQDDP	Sensor Query and Data Dissemination Protocol
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
CDMA	Code Division Multiple Access
PAN	Personal Area Network
RFD	Reduced-Function devices
FDD	Full-Function devices
SFD	Start of Frame Delimiter
PSDU	PHY Service Data Unit
LQI	Link Quality Indication
CCA	Clear Channel Assessment
GTS	Guaranteed Time Slots
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CFP	Contention Free Period
CAP	Contention Access Period
BER	Bit Error Rate
TOA	Time of Arrival
IBC	Identification - Based Cryptography
MIC	Message Integrity Code
PKI	Public Key Infrastructure
PDU	Protocol Data unit
MDS	Multi-Dimensional Scaling
MT	Mobile Terminal
RP	Anchor/Reference point
MNL	Multi Hop Network Localization
RPE	Recursive Position Estimation

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, Y., and E. Cayirci, “Wireless sensor networks: A survey”, Computer Networks (Elsevier) Journal, vol. 38, no. 4, Mar. 2002, pp. 393–422.

[2] J. Yuan, Z. Li, W. Yu, and B. Li, “A Cross-Layer optimization framework for multicast in multi-hop wireless networks wireless internet”, in *Proceedings of WICON’05*, Visegrad-Budapest, Hungary, July 2005, pp. 47–54.

[3] J. Reed, Introduction to Ultra Wideband Communication Systems, Prentice Hall, Englewood Cliffs, NJ, June 2005.

[4] Revision of Part 15 of the Commission’s Rules Regarding Ultra-Wideband Transmission Systems. First note and Order, Federal Communications Commission, ET-Docket 98-153, Adopted Feb. 14, 2002, released Apr. 22, 2002.

[5] M. Z. Win and R. A. Scholtz, “Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communication”, IEEE Transactions on Communications, vol. 48, no.4, Apr. 2000, pp. 679–689.

[6] Bharathidasan, A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science, University of

[7] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Elsevier Journal of Ad Hoc Networks 3 (3) (2005) 325–349.

[8] S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, “Routing protocols in wireless mesh networks: challenges and design considerations,” Multimedia Tools Appl., vol. 29, no. 3, pp. 285–303, 2006.