#### Q1: Describe the architecture and primary tasks of a WSN node including the main HW components characteristics and their energy consumption characteristics. Explain the typical methods to save energy according to the energy consumption characteristics of different hardware components. Give examples.

In the motes we have five major components

* Controller
  + Microcontroller

Suitable for building computationally less intensive, standalone applications, because of its compact construction, small size, low-power consumption, and low cost. It also features power different power states. Provides a high speed programming and eases debugging, because of higher-level programming languages.

Not as powerful and as flexible as some custom-made processors (such as DSPs and FPGAs).

* + Digital Signal Processors (DSPs)

Powerful, and complex digital filters can be realized with commonplace DSPs. useful for applications that require the deployment of nodes in harsh physical settings.

Lack of flexibility tasks require protocols (and not numerical operations) that need periodical upgrades or modifications (i.e., the networks should support flexibility in network reprogramming)

* + FPGA (Field Programmable Gate Array)

Flexible in their application, support parallel processing, can be reprogrammed.

Design and realization process is costly and reprogrammed take time

and energy.

* + ASIC (Application-specificIntegrated Circuit)

They ment to complement the Microcontroller or DPS for rudimentary and low-level tasks.

Simple design, can be optimized to meet a specific customer demand.

High development costs and lack of re-configurability.

* Memory
  + Ram is fast but losses content, when power is lost.
  + ROM can be read fast, but write slow.
  + Flash can be reprogrammed and erased.
* Comm Device
  + RF

Long range and working in NLOS scenarios. Offer high data rates. Different sates.

* + Optical, Need LOS, power energy per bit.
* Power Supply
  + Primary battery

This type is not rechargeable(Alkaline)

* + Secondary battery

This type is rechargeable(Litume), only makes sense in a setup with form of energy harvesting.

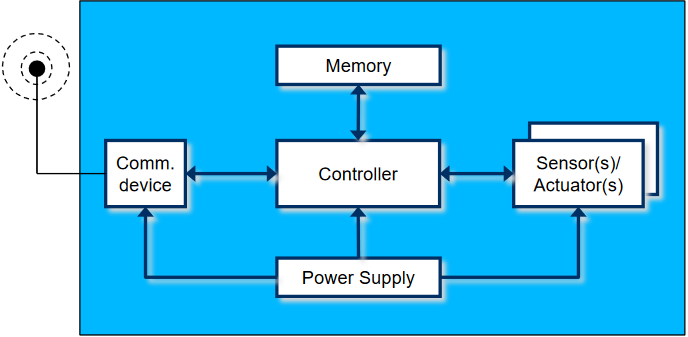
* Sensors / Actuators
  + Active sensors

Thermometer, microphones

* + Passive sensors
  + Actuators

Controls motors that can be used in many different usecases ex open a garden house window.

* + Active sensors

Radar

#### Q2: Describe the possible energy sources for WSN nodes including energy harvesting. What are the pro and cons of the different sources? Describe the energy modeling of transmitter and receiver. What aspects should be taken into account when deciding if using single hop and multi-hop? Explain the typical methods to save energy using examples.

#### Q3: What are the optimization goals of WSNs? What are the basic design principles in WSNs? Give one or two examples in the protocol design which can reflect the design principles.

#### Q4: Explain the pro and cons of contention based MAC protocols and schedule based MAC protocols. What are the main energy issues in WSN MAC? Describe the basic schemes of SMAC and its additional functions. Explain how SMAC tackles the energy issues in its design.

The objectives of a WSN MAC protocols is Collision Avoidance, Energy Efficiency, Scalability. But it also have Energy problems, such as. Collision wasted energy when two packets collide. Overhearing Receiving packets that was destined for another node. Idle listings wasted energy to receive when no one is sending.

Contention based mac, can scale to many nodes. But with more nodes there is an increased probability of collicons.

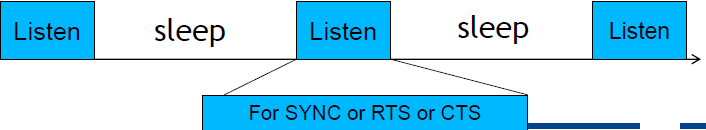
SMAC have features that can help solve energy waste.

* Sleep/listening ( Idle Listening and overhearing energy waste )

Trades energy efficiency for lower throughput and higher latency

Nodes can go to sleep during other nodes transmission

While sleeping, radio is off. Hence packet exchanges can’t happen

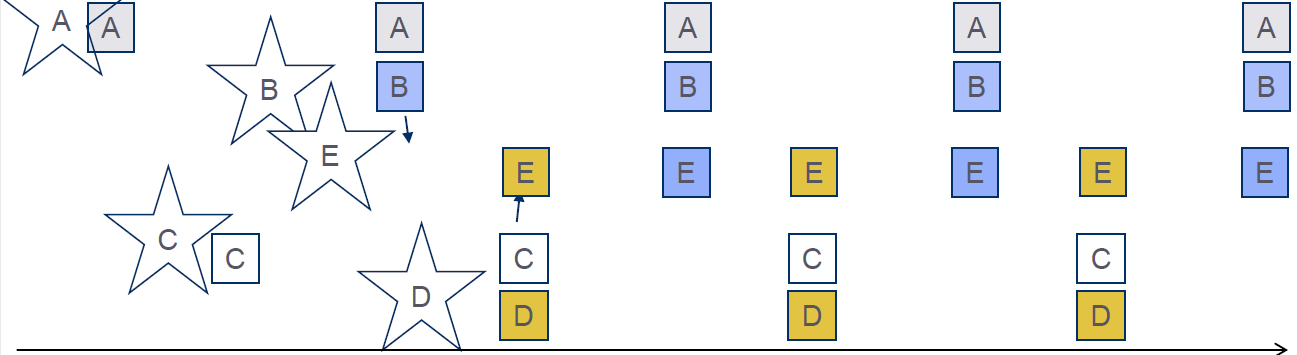


* Synchronization

First listens to the medium and If it receives a SYNC it becomes a follower.

Uses a sync PHASE to exchange wakeup schedules between neighbors, if none received it will choose it’s own schedule and broadcast it with a SYNC packet.

If a node recvies a different schedule after it chooses and announces its own. If it had no neighbors, it discards it’s own schedule, if It has then adopts both.



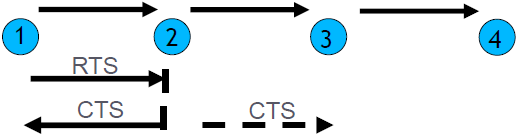
* Message passing ( Minimize overhead )

A receiver often needs to need get all messages before it can do in-network processing like aggregation. But with more packets there is a higher probability of corruption.

The solution is to fragment long messages into many small fragments and send them in a burst, *using only one set of RTS/CTS to reserve the channel and acks for each fragment*. Nodes that wake up in the middle of a burst by back to sleep by hearing acks.

* Adaptive listening ( Reduce latency, but paid in energy )

Let a node who overhears it’s neighbors transmission stay awake instead of following Sleep/listening. Reduces latency by staying awake(node 3 ) and forward to 4 if it is still hearing.



#### Q5: Explain the difference of distributed MAC and centralized MAC. What is preferable for most use cases in WSNs and Why? What are the main energy issues in WSN MAC? Clear channel assessment (CCA) and low power listening (LPL) are the two highlight features of BMAC. Explain how CCA and LPL work in BMAC.

**Centralized MAC.**

Having a central station control when a node may access the medium. Example is the polling and centralized of TDMA schedules. For this to work there is a need for time synchronization.

Simple , Usually no issues with collisions, overhearing and idle listening. Only burdens the central station

Not directly feasible for non-trivial wireless network sizes, but can be usefully if the network is divided into smaller groups.

Centralized multiplexing access, therefore, lacks flexibility and scalability to adapt to the variation of WSN applications

**Distributed MAC.**

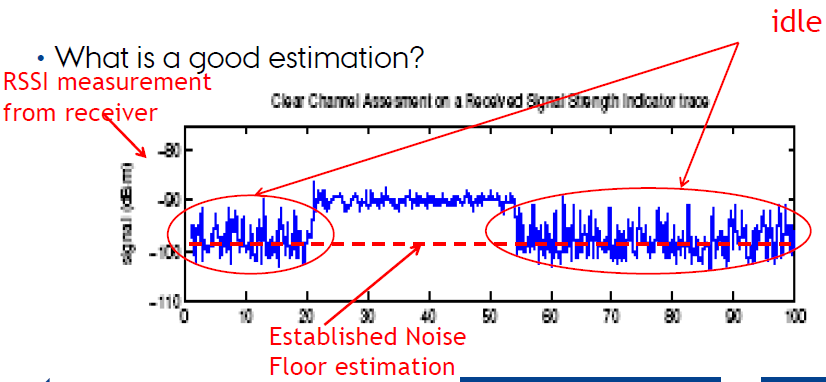
Using distributed MAC protocols allow nodes operate in a decentralized manner. Therefor it is easier to implement and perform more flexible and scalable control mechanisms, which may fit well with the requirements of WSNs.

But it is not collision-free protocols and need listen-before-talk(CSMA) schemes so nodes to keep sensing the channel. This results in high energy wastage due to collisions, idle listening, overhearing, and message overhead. S-MAC attempts to reduce all four types of energy wastage.

#### B-MAC

**Carrier sensing using clear channel Assessment ( CCA )**

For effective collision avoidance, MAC must accurately determine if the channel is clear. To do that it needs to tell what is the signal and what is the noise. If not handled correctly it could lead to waste if a real signal is taken as noise or packet collisions.

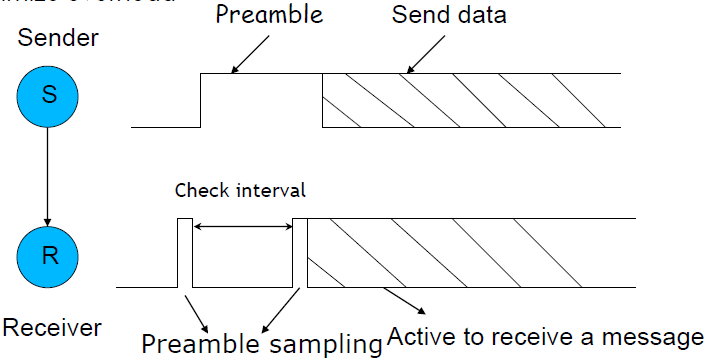


**Sleep/Wake scheduling using low power Listening (LPL) Reduce listening cost**

Nodes periodically wakes up, turns radio on and checks the channel

If activity on the channel is detected, node powers up and stays awake for the time required to receive packet.

It goes back to sleep if a received or after timeout.



#### Q6: Explain the basic two approaches for error control in WSNs. What are the pros and cons of each approach? What are the tradeoffs between FEC, ARQ and transmission power? What is the difference ofreliability in the link layer and in the transport layer? Explain the tradeoff between pure end-to-end reliability and end-to-end reliability plus link layer retransmission.

#### Q7: Explain the data centric networking, the motivation using it in WSNs and its difference comparing with ID-based routing. Explain how directed diffusion works.

#### Q8: Explain the motivation to use data aggregation in WSN. What is the relation between data aggregation and networking in WSNs? Explain how data aggregation works, the challenges of data aggregation, and the pros and cons using data aggregation.

#### Q9: Explain why TCP is not suitable for transport layer in WSN. Explain how PSFQ and ESRT work? What is the difference between PSFQ and ESRT?

**TCP is not suitable for transport layer in WSN**

* TCP has a large overhead, each TCP segment has a minimum header of 20 bytes for port numbers, sequence numbers, checksum, window size, and more. In a WSN packets will be small, just a few bits of sensor data.
* TCP requires perfect reliability and accept no loss. But in a WSN as long as we detect events we may not need all packets.
* TCP connects two end nodes and the intermediate nodes just forward blocks of bits and don’t care the content. In sensor networks, intermediate perform in-network processing or aggregation of data.

**Pump Slow Fetch Quick (PSFQ)** - packet reliability. It is applied in scenarios that are *pack losses are not tolerable, delay not critical* such as firmware update, Eg Downstream sink to source.

The user slowly injects packets into the network. Intermediate nodes store packets, forward if *in-sequence*

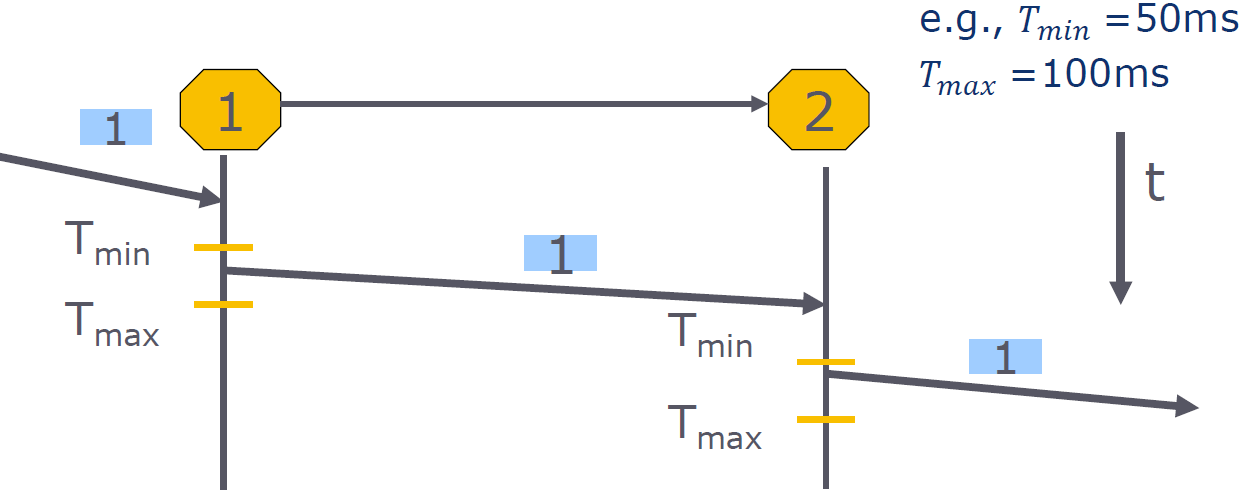
Out-of-sequence: buffer, request missing packet(s) hence *a fetch* operation (a NACK). This allows a previous node to resends missing *packet => local recovery*.

PSFQ has three functions:

**Message Relaying (PUMP Operation)**

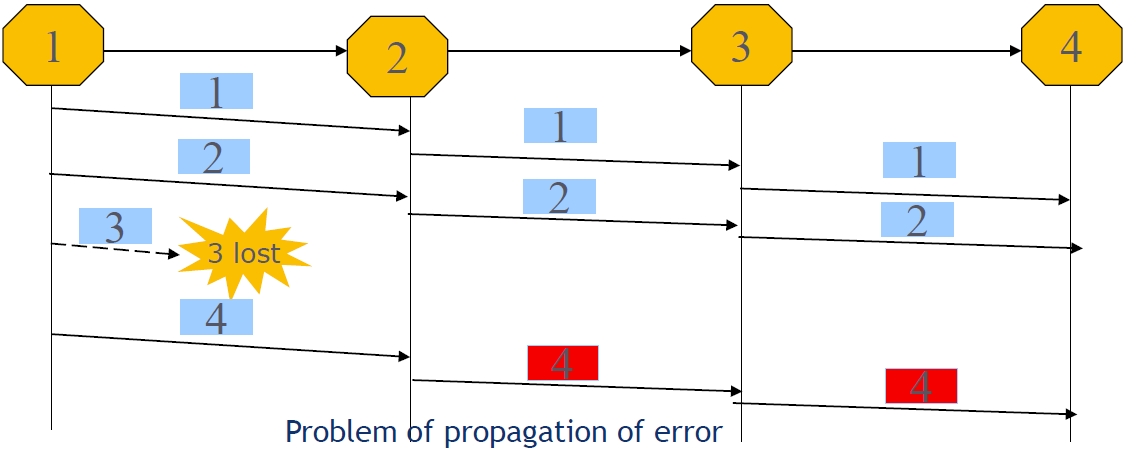
A user node broadcasts a packet to its neighbors every Tmin until all the data fragments have been sent out. If not *duplicate* and *in-order* and *TTL not 0*, cache and schedule for forwarding at time Tx where ( Tmin< Tx < Tmax ).

Random delay allows a downstream node to recover the missing packets before the next packet arrives from an upstream node Also allows reducing the number of redundant broadcasts of the same packet by neighbors.



**Relay initiated error recovery (FETCH Operation)**

A node goes into fetch mode when a sequence number gap is detected. A node aggressively sends out NACK messages to its immediate upstream neighbors to request missing packets. If no reply is heard or only a partial set of missing packets are recovered within a period 𝑇𝑇𝑟𝑟(~20ms) (𝑇𝑇𝑟𝑟< 𝑇𝑇𝑚𝑚𝑚 𝑚 (~100ms) ) then the node will resend the NACK every 𝑇𝑇𝑟𝑟interval until all packets are recovered. Since it is very likely that consecutive packets are lost because of fading conditions, PSFQ aggregates losses such that the fetch operation deal with a “window” of lost packets

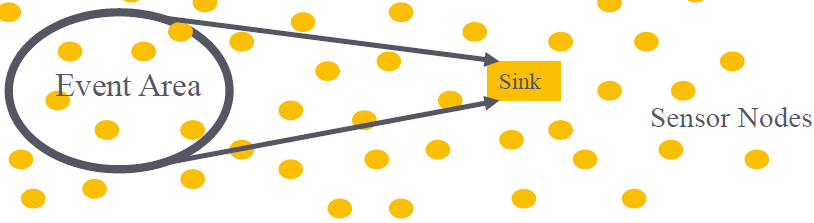


**Selective status reporting (REPORT Operation)**

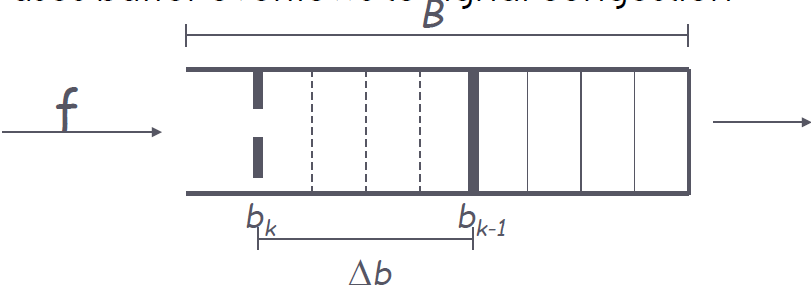
The report operation allows the data source to assess how many nodes have already received the complete code block and can thus switch to the new software. The sink node requests reporting by setting a reserved bit in the TTL field of an inject message. Report messages are generated by the most distant nodes (those that receive packets with a TTL of one) and travel back to the data source. The data generated by an end node or an intermediate node contains the node’s own address and a summary of the already received segments.

**Event-to-Sink Reliability Transport (ESRT)**

GOAL: To reliably detect/estimate event features based on the collective reports of several sensor nodes observing the event. (to guarantee event reliability)



ESRT uses buffer overflows to signal congestion

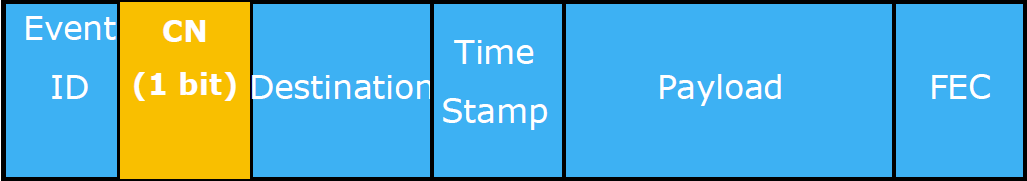


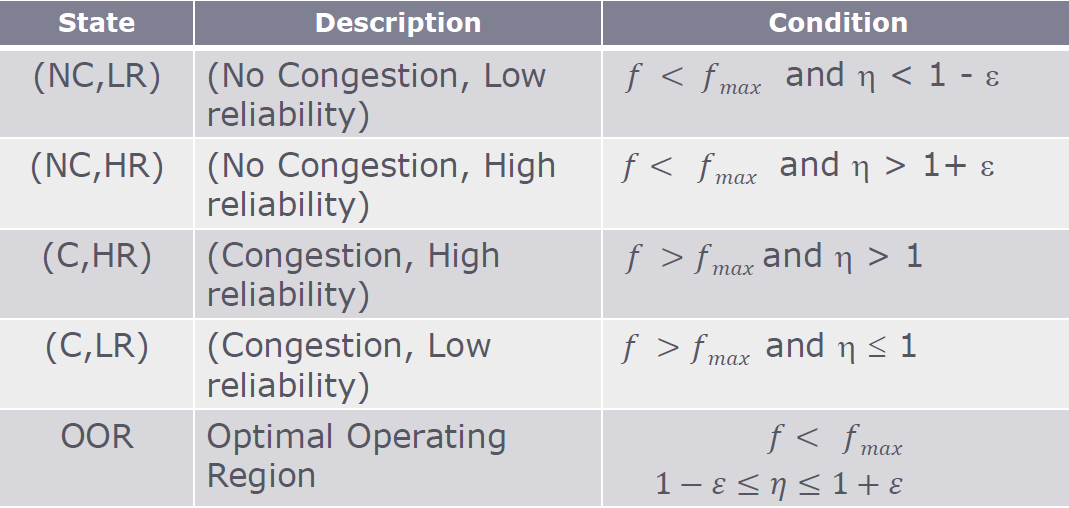
bk: Buffer fullness level at the end of reporting interval k

Δb: Buffer length increment over past interval Δb=bk-bk-1

B: Buffer size

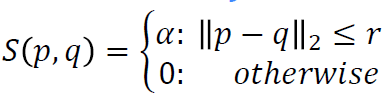
f: Reporting frequency





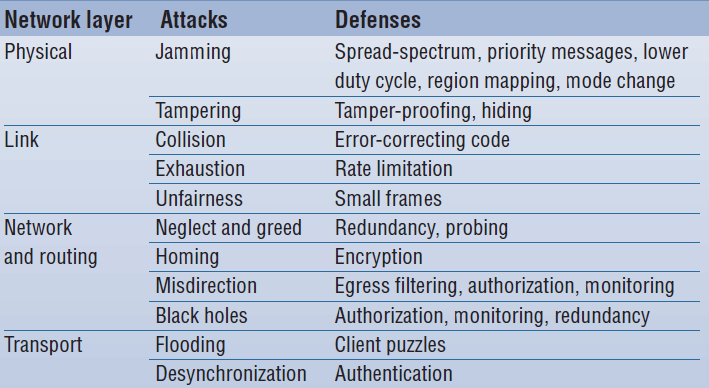
Two sensing models

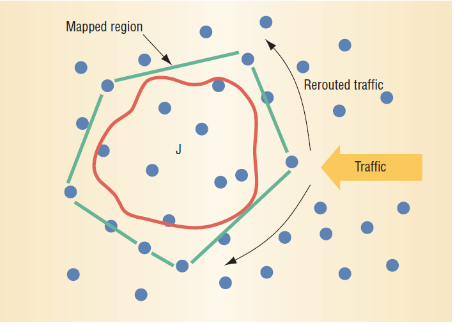
Boolean sensing model: all sensors of the same sensor modality. Assumes they are counting packets.



#### Q10: Explain the possible vulnerabilities and security attacks at different protocol layers in WSNs and the corresponding countermeasures.

A attack on a WSN could do a denial of service or be used to steal information using a passive attack such as overhearing. Active attacks can also happen such as reporting cheap routes to the routing protocols or exploiting access to the medium.



**Physical layer**

Jamming - by jamming the wireless medium, you can just the WSN from working. If the attack is intermittent nodes may be able to send a few messages with high power and priority back to the BS. The nodes can work together ensure that such messages will be received. Using the Jamming reports the nodes can form a zone around the jamming spot and work around it.

**Link - layer**

The link layer is responsible for node to node delivery and must do it in an energy efficient and fair manner. Attackers can abuse this fact and send messages to make collisions and this uses less energy than full on jamming. To defend this, we can use Error correcting codes for tolerating variable levels of corruption in messages at any layer. However, this introduces additional overhead. There are no really good defense agents this and A subverted node could intentionally and repeatedly deny access to the channel, expending much less energy than in fulltime jamming.

**Network - layer**

As the network layer has the responsible for routing packets attack type would be to advertise routes as basically free and then drop the packets this is known as a black hole attack. To defend against this type of attack, one could use Authorization.

**Transport - layer**

As we know the transport layer protocols provide end-to-end reliability. So the obvious attack scenario is abusing this fact by flooding. An adversary node sends out multiple end-to-end connection establishment requests, effectively exhausting the memory of a node. A defense requires clients to demonstrate the commitment of their own resources to each connection by solving client puzzles. The server can create and verify the puzzles easily, and storage of client-specific information is not required while clients are solving the puzzles. Servers distribute the puzzle, and clients wishing to connect must solve and present the puzzle to the server before receiving a connection. An adversary must therefore be able to commit far more computational resources per unit time to flood the server with valid connections. Under heavy load, the server could scale the puzzles to require even more work by potential clients. This solution is most appropriate for combating adversaries that possess the same limitations as sensor nodes. It has the disadvantage of requiring more computational energy for legitimate sensor nodes, but it is less costly than wasting radio transmissions by flooding.