# Denial of Service in Sensor Networks


Authors : Anthony D. Wood
John A. Stankovic
From: University of Virginia


Presented by: Luba Sakharuk

# Agenda for the DOS in Sensor Networks

- Abstract
- Theory and Application
- The Denial of Service Threat
- Physical Layer
- Link Layer
- Network and Routing Layer
- Transport Layer
- Protocol Vulnerabilities
- CONCLUSION

# Abstract

•Unless their developers take security into account at design time,

•sensor networks and the protocols they depend on will remain vulnerable to denial-of-service attacks

•DoS attacks again sensor networks may permit real-world damage to the health and safety of people

•The limited ability of individual sensor nodes to thwart failure or attack makes ensuring network availability more difficult

# Theory and Application

**•Developers build sensor networks to collect and analyze low-level data from an environment of interest**

**•Sensor networks maybe deployed in a host of different environments**

**•Possible Uses:**

- **Military (battlefield conditions, track enemy movement, monitor secured zone for activity, measure damage, casualties**

- **Could form communications network for rescue personnel at disaster sites, they could help locate casualties**

- **Could monitor conditions at the rim of volcano, along an earthquake fault, around critical water reservoir**

- **Could provide always0on monitoring of home healthcare for the elderly, detect chemical or biological thread at airport**

# Theory and Application

**Security issues for the USES listed on the previous slide:**

**•Disasters - It may be necessary to protect the location and status of casualties from unauthorized disclosure (particularly if the disaster relates to ongoing terrorist activities instead of natural causes)**

**•Public Safety - False alarms about chemical, biochemical, or environmental threats could cause panic or disregard for warning systems. An attack on the system's availability could precede a real attack on the protected resources**

**•Home healthcare - Because protecting privacy is paramount, only authorized users can query or monitor the network. These networks also can form critical pieces of an accidental-notification chain, thus they must be protected from failure**

# The Denial of Service Threat

•**DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function**

•**Each layer is vulnerable to different DoS attacks and has different options for its defense**

Table 1. Sensor network layers and denial-of-service defenses.

| Network layer | Attacks | Defenses |
|---|---|---|
| Physical | Jamming | Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change |
| | Tampering | Tamper-proofing, hiding |
| Link | Collision | Error-correcting code |
| | Exhaustion | Rate limitation |
| | Unfairness | Small frames |
| Network and routing | Neglect and greed | Redundancy, probing |
| | Homing | Encryption |
| | Misdirection | Egress filtering, authorization, monitoring |
| | Black holes | Authorization, monitoring, redundancy |
| Transport | Flooding | Client puzzles |
| | Desynchronization | Authentication |

•**Hardware failures, software bugs, resource exhaustion, environmental conditions, any complicated interaction between these factors can cause DoS**

# Example of Route Discovery mechanism

**DSR** - **D**ynamic **S**ource **R**outing

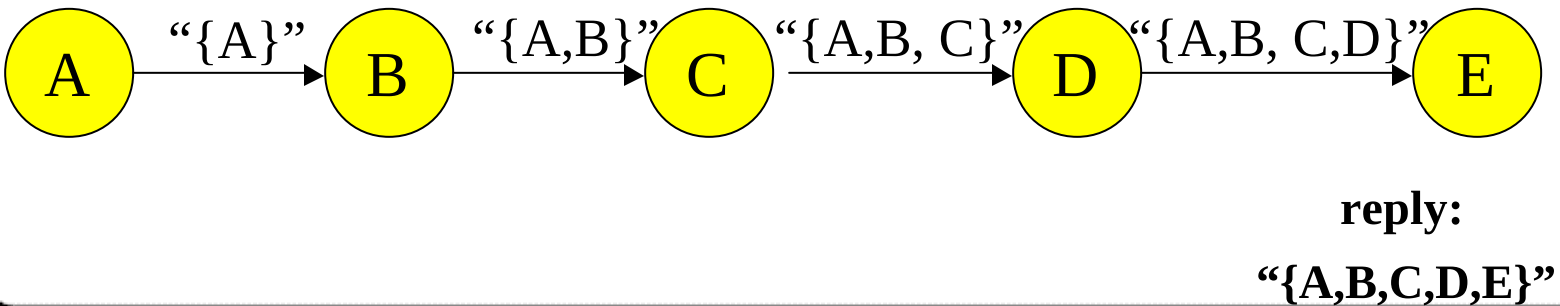
-Uses source routing rather than hop-by-hop routing with each packet to be routed carrying in its header the complete, ordered list of nodes through which the packet must pass

Route Discovery:

1) flood Route request message through network

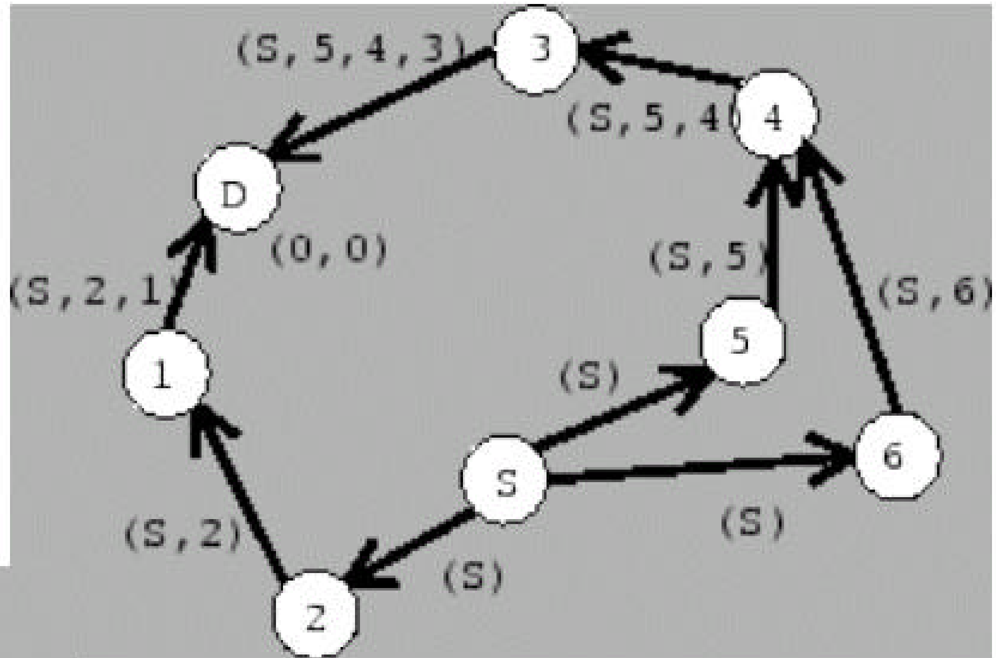
2) request answered with route reply by

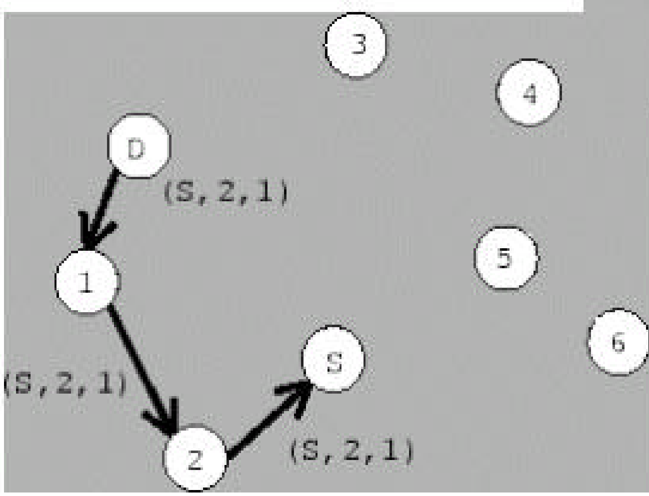
- -destination
- -some other node that knows a path to destination



# Example of Route Discovery mechanism

Route Request




Route Reply

# Physical Layer

## Jamming

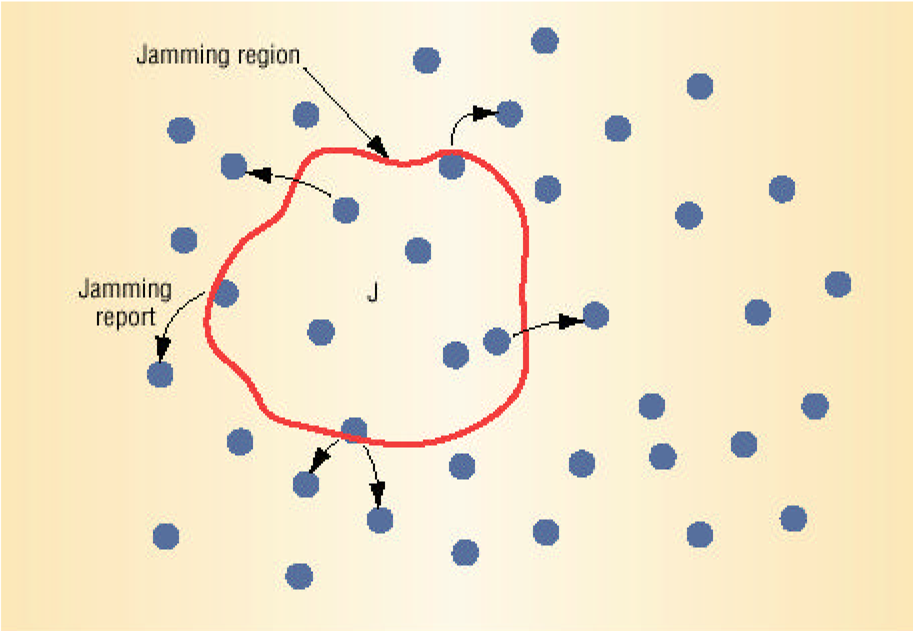



***Figure 1. Defense against a jamming attack, phase one. Nodes along the edge of a jammed region report the attack to their neighbors.***

# Physical Layer

## Jamming

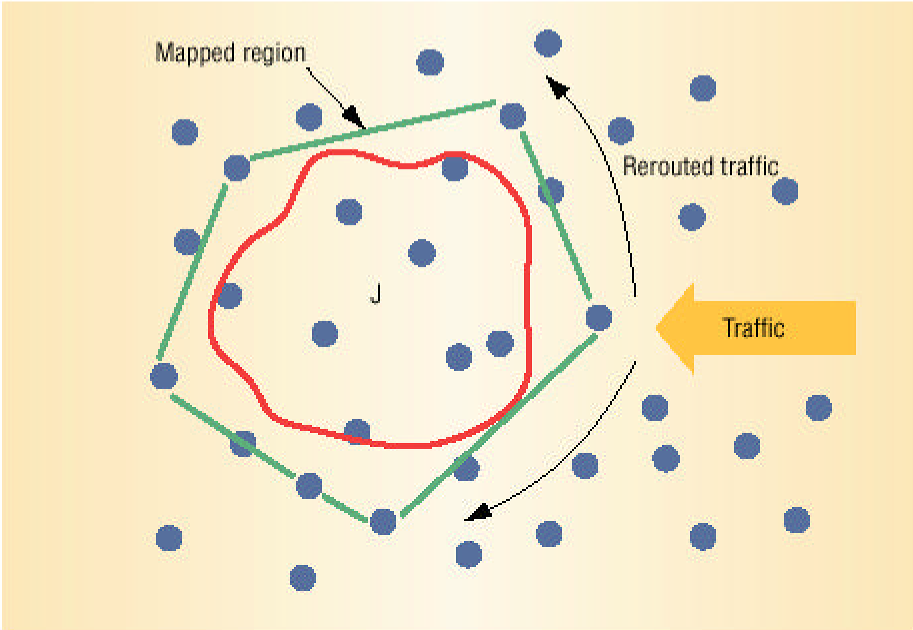



***Figure 2. Defense against a jamming attack, phase two. Neighboring nodes collaborate to map the jamming reports, then reroute traffic around the jammed region.***

# Physical Layer

An attacker can tamper with nodes physically and interrogate and compromise them—threats that the nature of sensor networks exacerbates.

## Tampering

**1 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 1 0**

**One defense involves tamper-proofing the node's physical package.  Its success depends on**

**•how accurately and completely designers considered potential threats at design time**

**•the resources available for design, construction, and test**

**•the attacker's cleverness and determination**

# Link Layer

## Collision

•A change in the data portion would cause a checksum mismatch at the receiver

•A corrupted ACK control message could induce costly exponential back-off in some MAC protocols

•Malicious collisions create a kind of link-layer jamming

•No completely effective defense is known

# Link Layer

## Exhaustion

•A  naïve link-layer implementations may attempt retransmission repeatedly (even if collisions at the end of the frame)

•This active DoS attack could culminate in the exhaustion of battery resources in nearby nodes

•One solution makes the MAC admission control rate limited, so the network can ignore excessive requests without sending expensive radio transmissions

•One design-time strategy for protection against battery-exhaustion attacks limits the extraneous responses the protocol requires

# Link Layer

## Unfairness

•Intermittent application of these attacks can cause unfairness

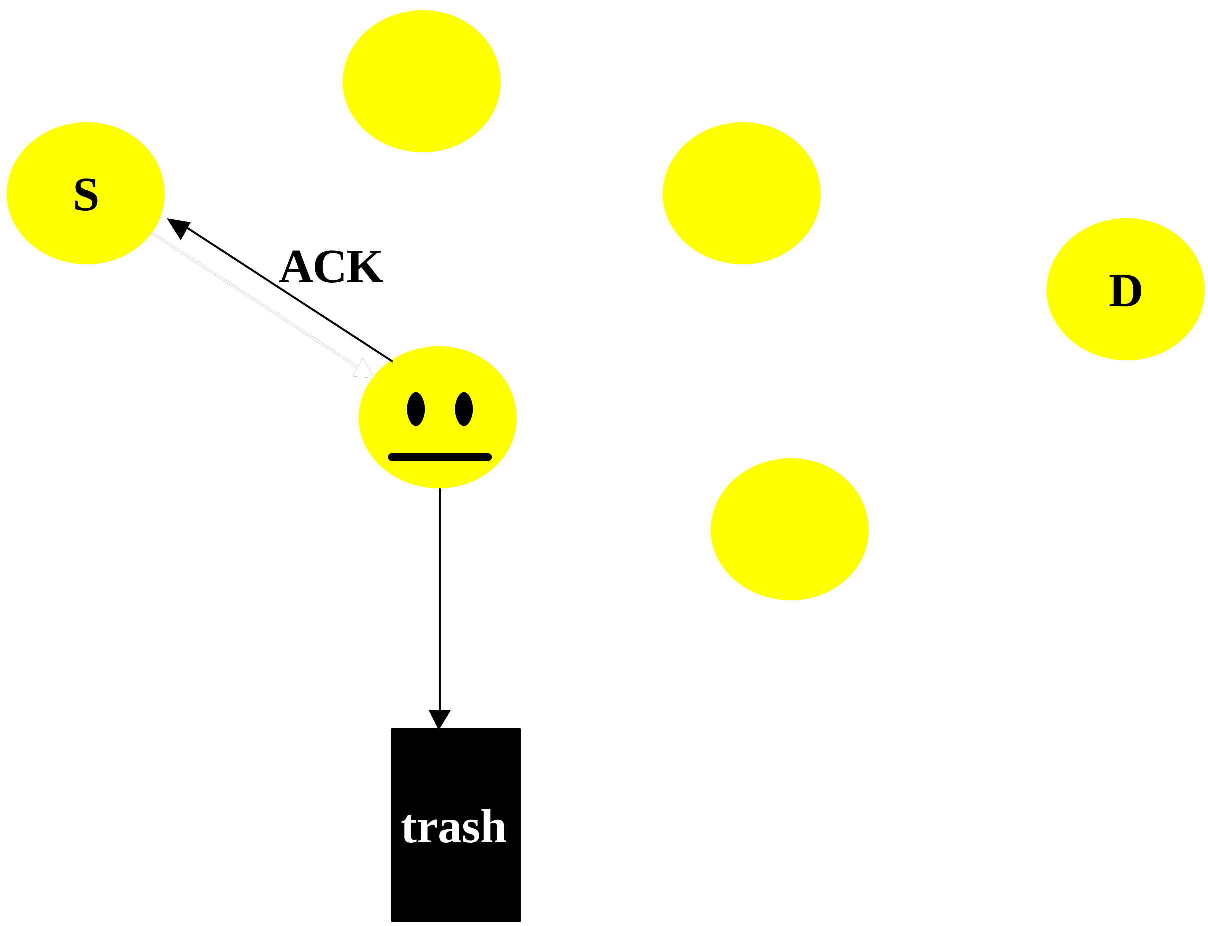
•May not entirely prevent legitimate access to the channel, BUT

•Could degrade service, causing users of a real-time MAC protocol to miss their deadlines

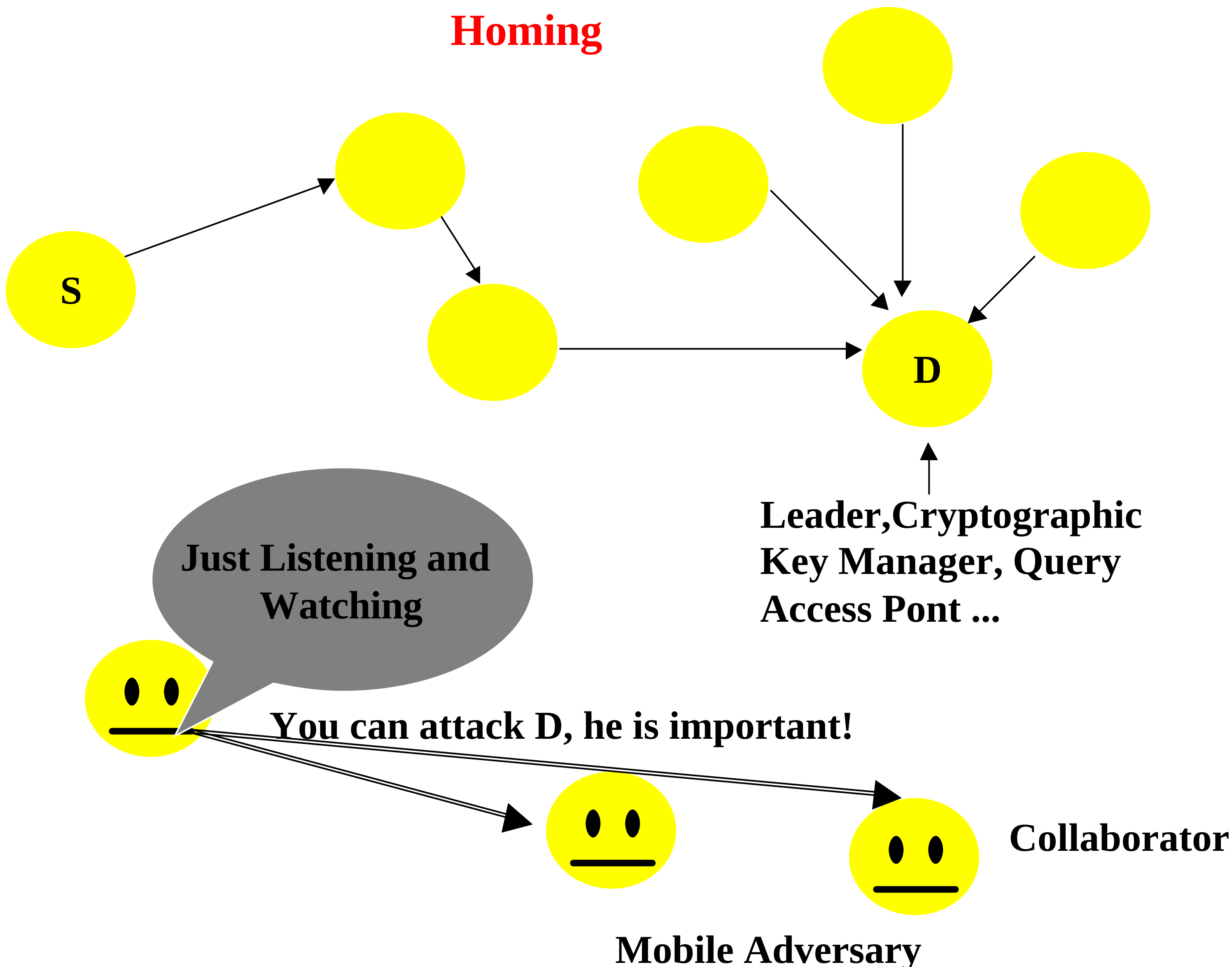
•One defense against this threat uses small frames, so that an individual node can capture the channel only for short time

# Network and Routing Layer

**Neglect and greed**

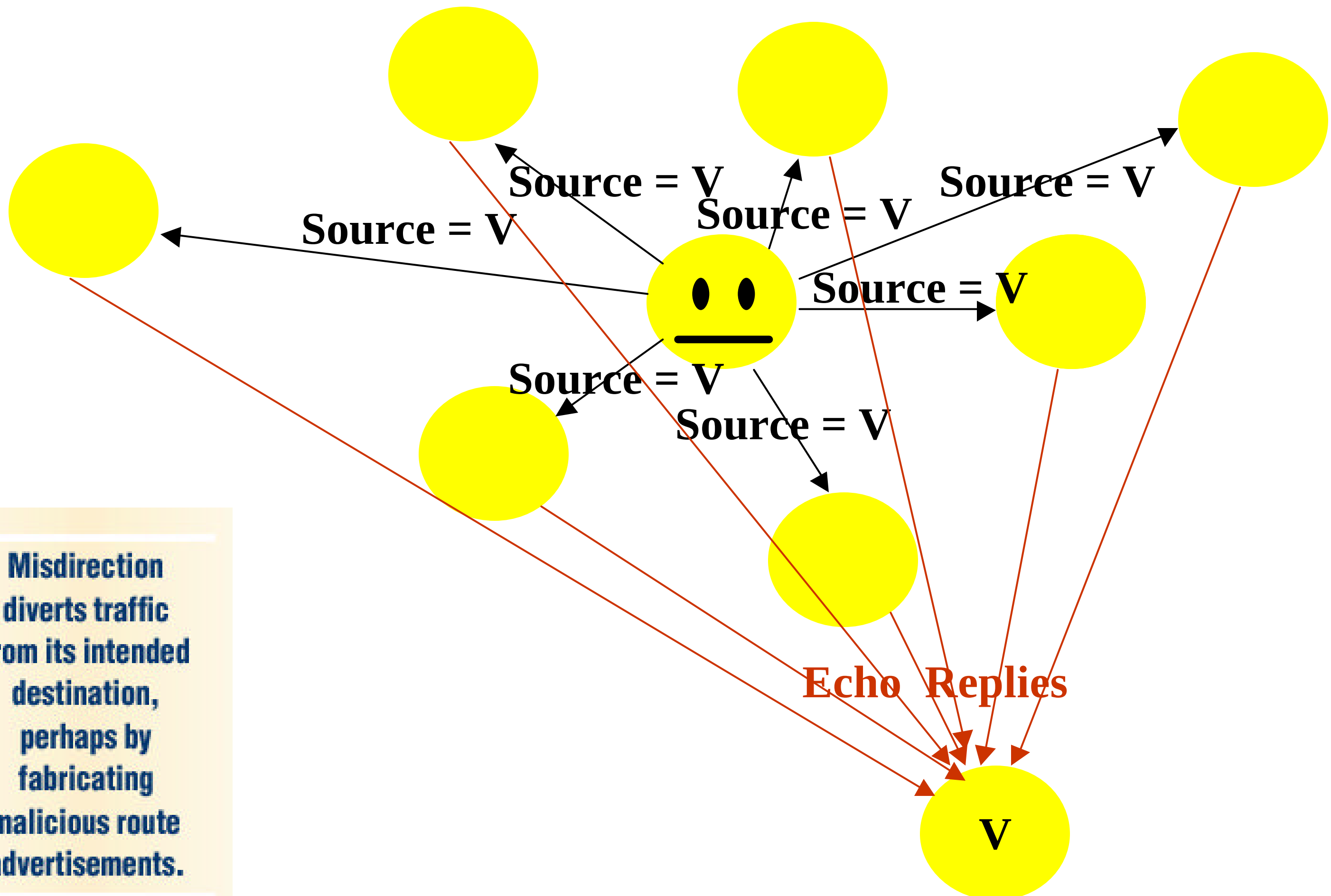


# Network and Routing Layer



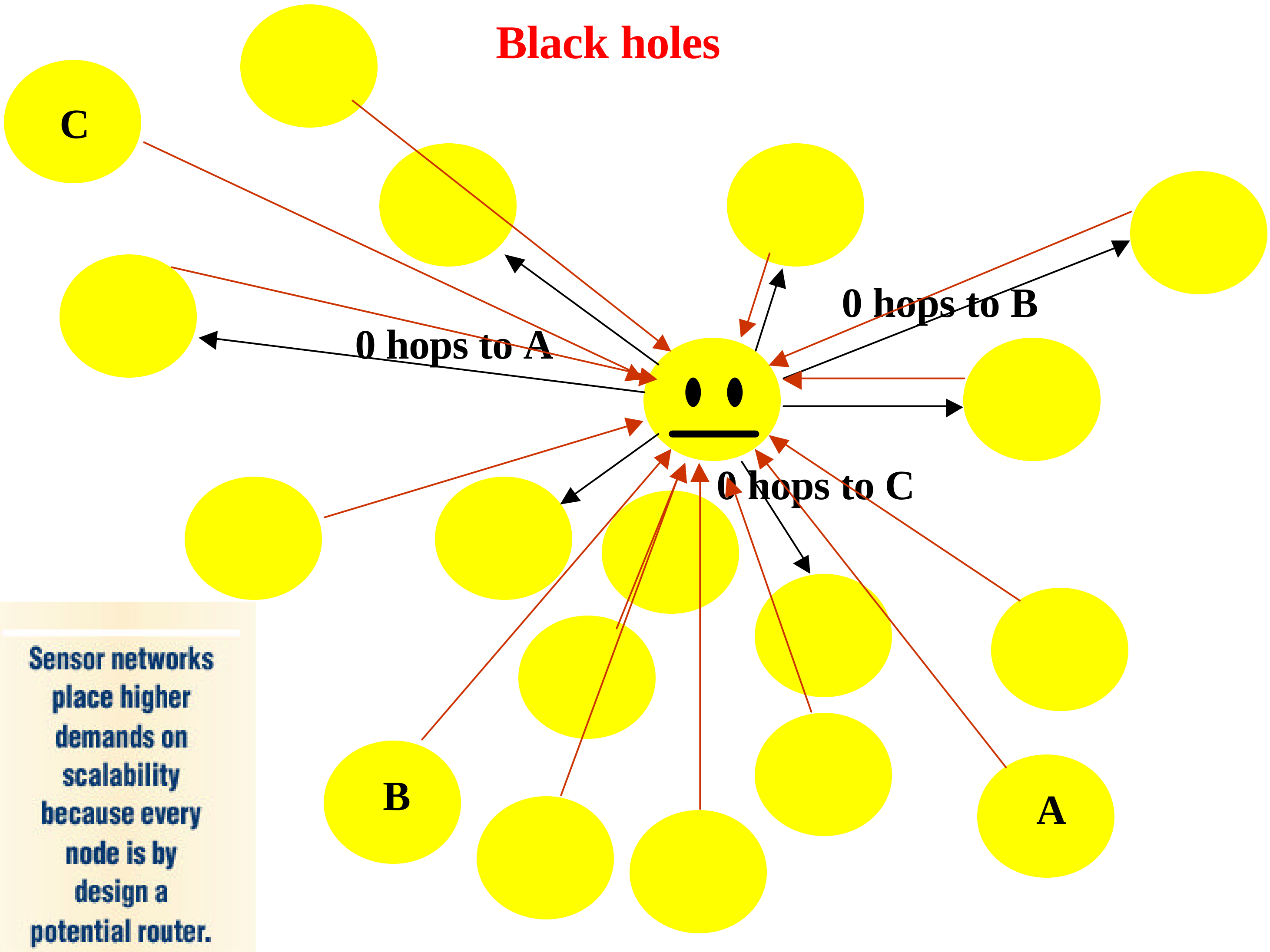
# Network and Routing Layer

**Misdirection (smurf attack)**




**Misdirection diverts traffic from its intended destination, perhaps by fabricating malicious route advertisements.**

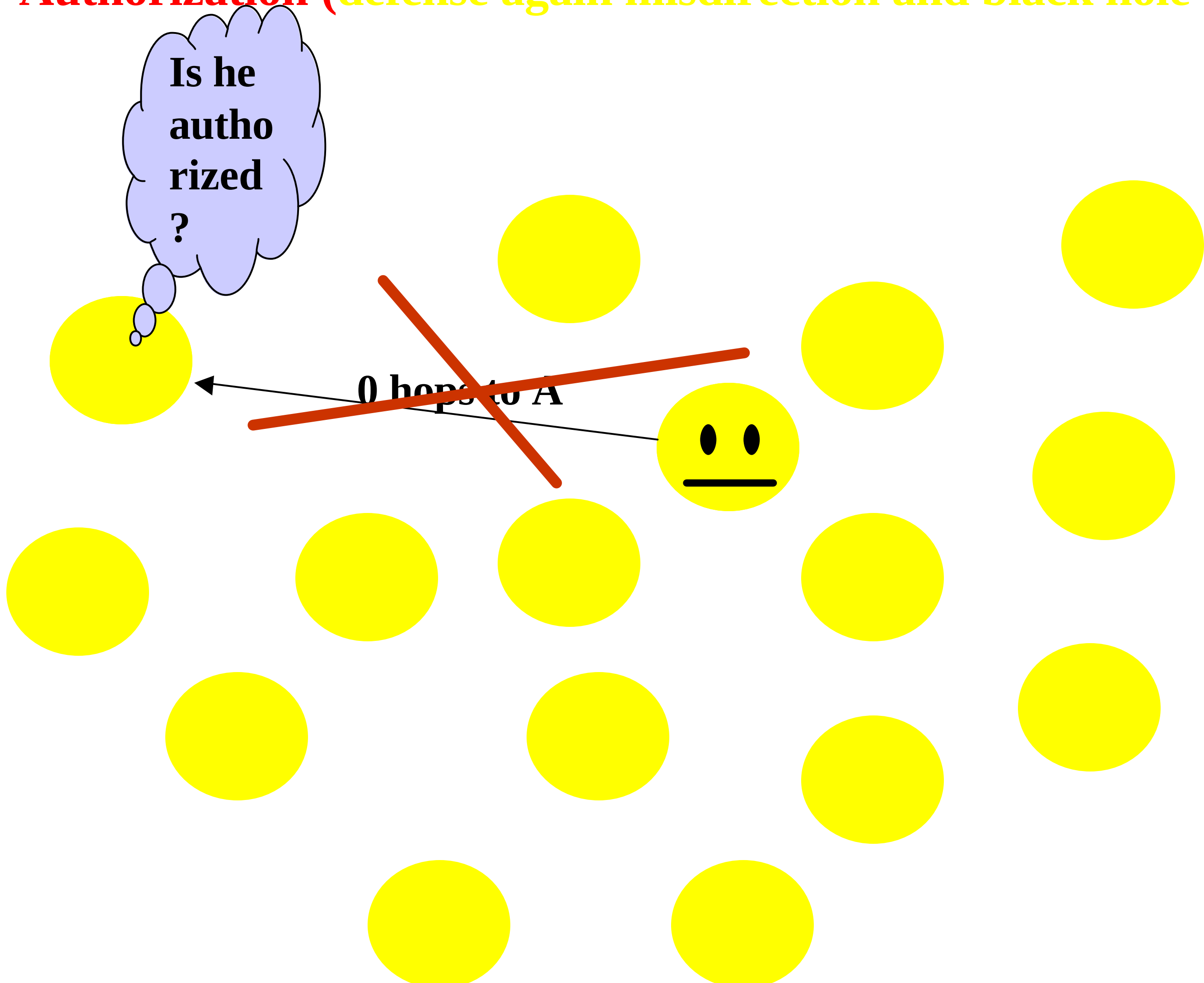
# Network and Routing Layer




Sensor networks place higher demands on scalability because every node is by design a potential router.

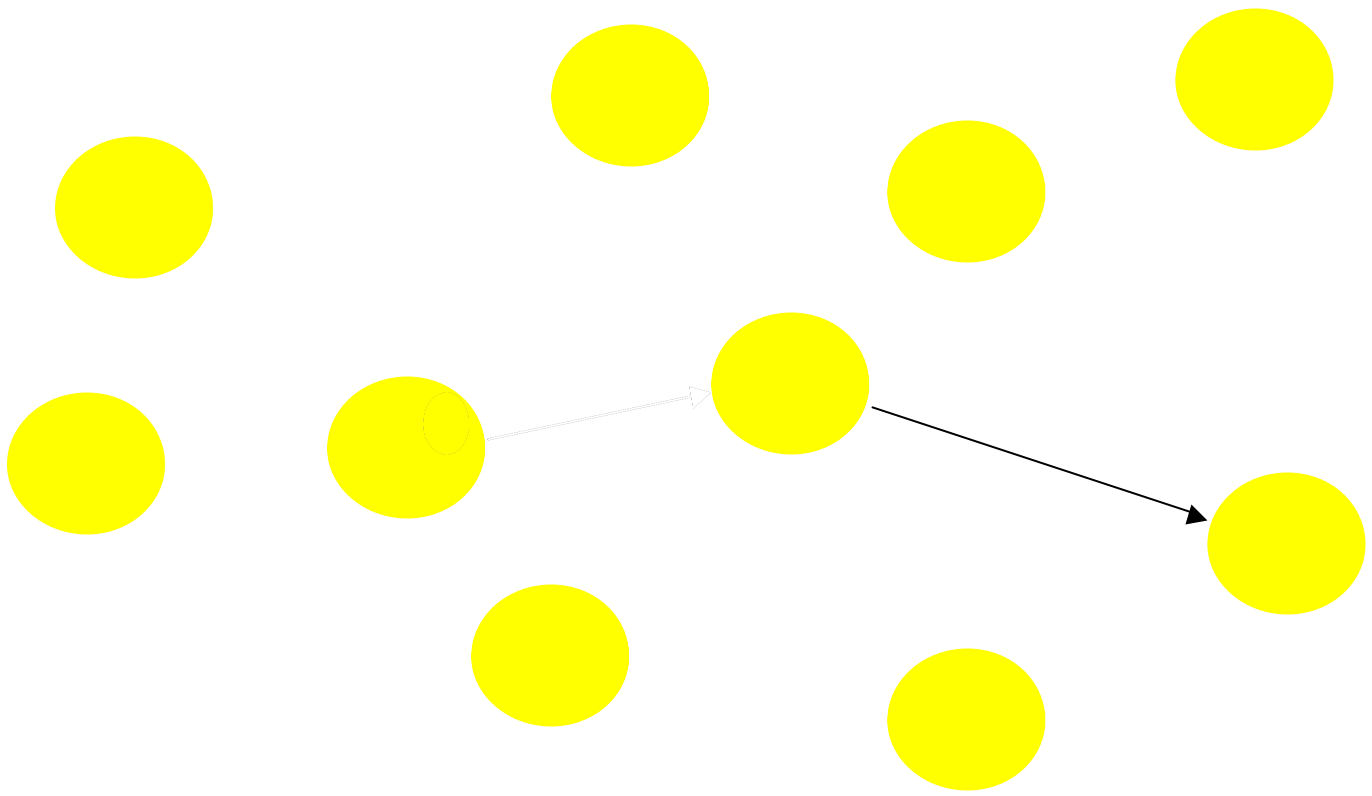
# Network and Routing Layer

**Authorization (defense again misdirection and black hole attacks)**



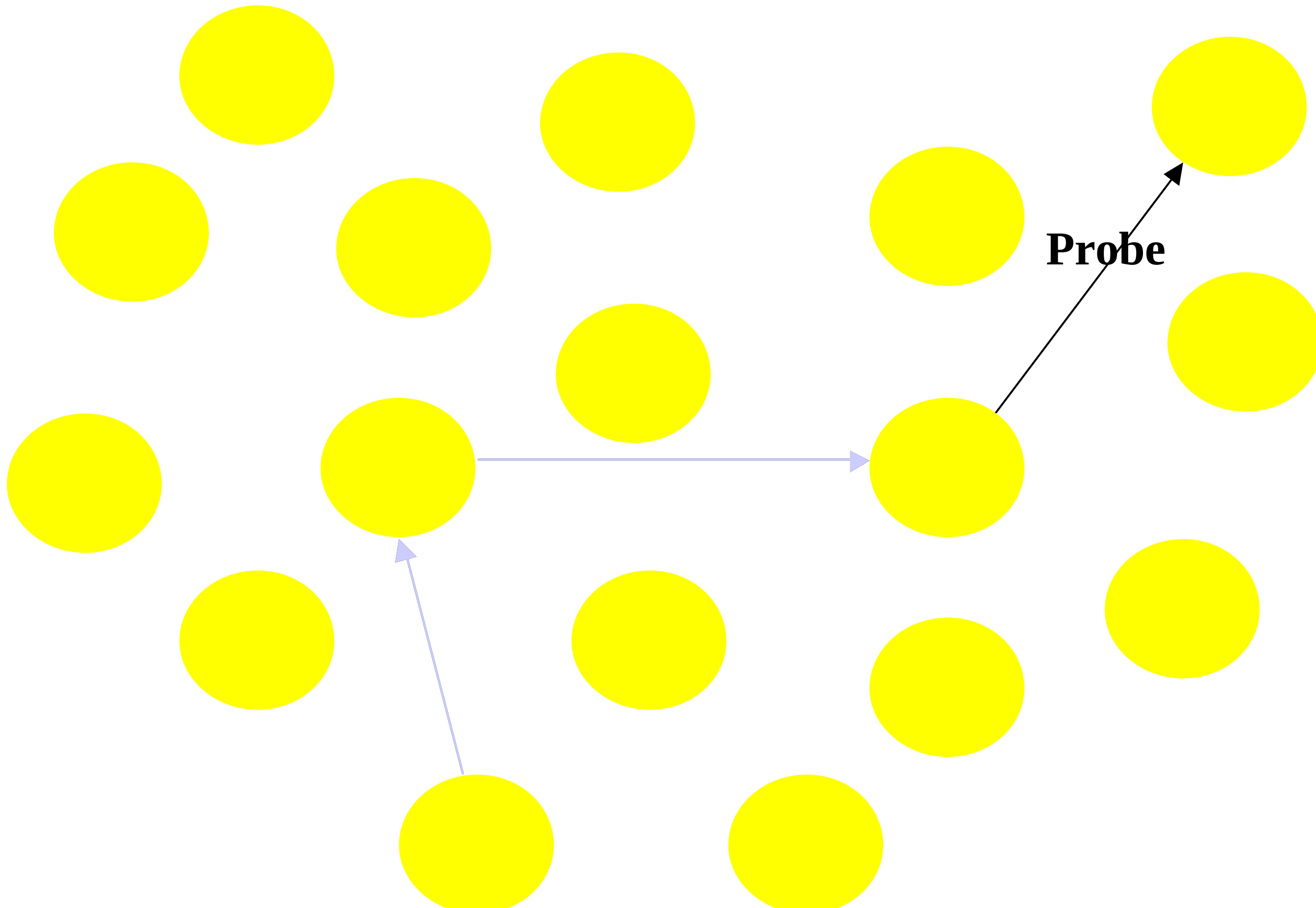
# Network and Routing Layer

**Monitoring**



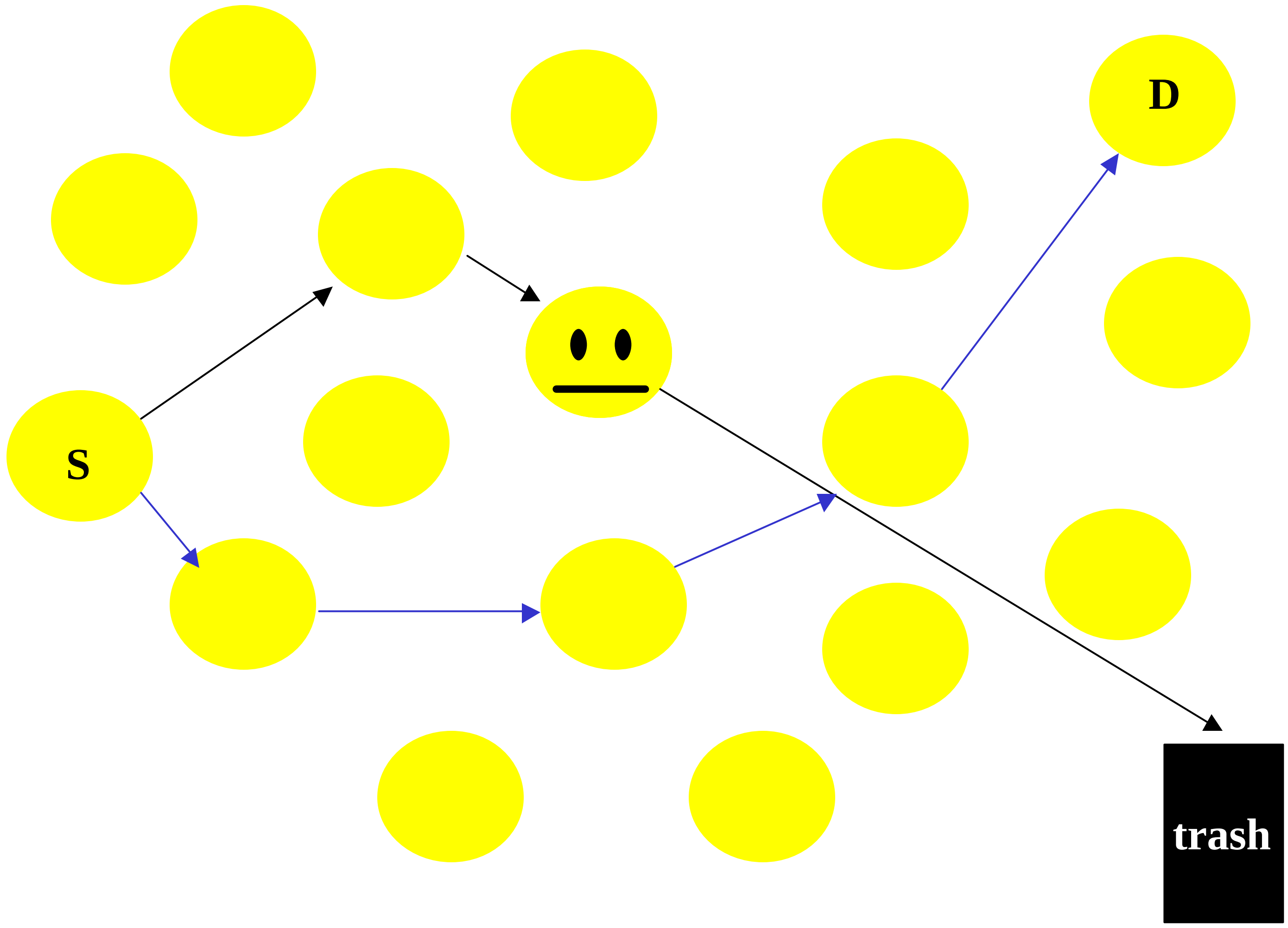
# Network and Routing Layer

**Probing**



# Network and Routing Layer

**Redundancy**



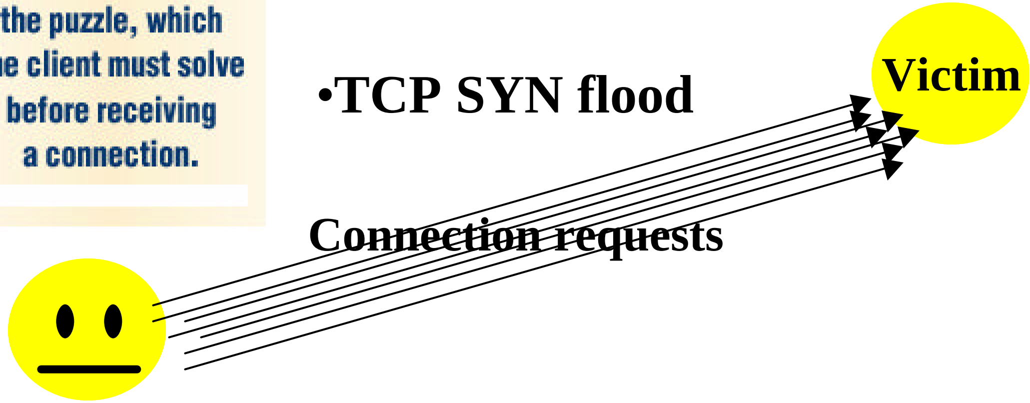
# Transport Layer

Puzzles require clients to demonstrate the commitment of their own resources to each connection. Servers distribute the puzzle, which the client must solve before receiving a connection.

## Flooding

•Protocols that must maintain state at either end are vulnerable to memory exhaustion through flooding

•TCP SYN flood




•One defense requires clients to demonstrate the commitment of their own resources to each connection by solving client puzzles

# Transport Layer

**Desynchronization**

**Forges messages to one or both end points**

- **Messages carry sequence numbers that cause the end point to request retransmission of missed frames**

- **Cause end point waste energy in an endless synchronization-recovery protocol**

- **One defense to this attack authenticates all packets exchanged**

# Protocol Vulnerabilities

## Adaptive rate control

•Alec Woo and David Culler describe a series of improvement to standard MAC protocols that make them more applicable in sensor networks

•Key mechanisms include:

- random delay for transmissions,
- back-off that shifts an application's periodicity phase,
- minimization of overhead in contention control mechanisms
- passive adaptation of originating and route-through admission control rates
- anticipatory delay for avoiding multi hop hidden-node problems

# Protocol Vulnerabilities

## Adaptive rate control

•Woo and Culler propose giving preference to route-through traffic in a admission control by making its probabilistic multiplicative back-off factor 50 percent less than the back-off factor of originating traffic

•This preserves the network's investment in packets that, potentially, have already traversed many hops

•This approach exposes a protocol vulnerability by offering an adversary the opportunity to make flooding attacks more effective.

•High Bandwidth packet streams that an adversary generates will receive preference during collisions that can occur at every hop along their route.

•Thus, the network must not only bear the malicious traffic, it also gives preference to it!

•An attacker can exploit a reasonable approach to power conservation and efficiency

# Protocol Vulnerabilities

## RAP

•Provides a real-time communication architecture integrating a query-event service API and geographic forwarding with novel velocity monitoring scheduling (VMS) policy

•An attacker can flood the entire network with high-velocity packets to waste bandwidth and energy

•The attack can also amounts to an attacker inducing the node to become a routing black hole

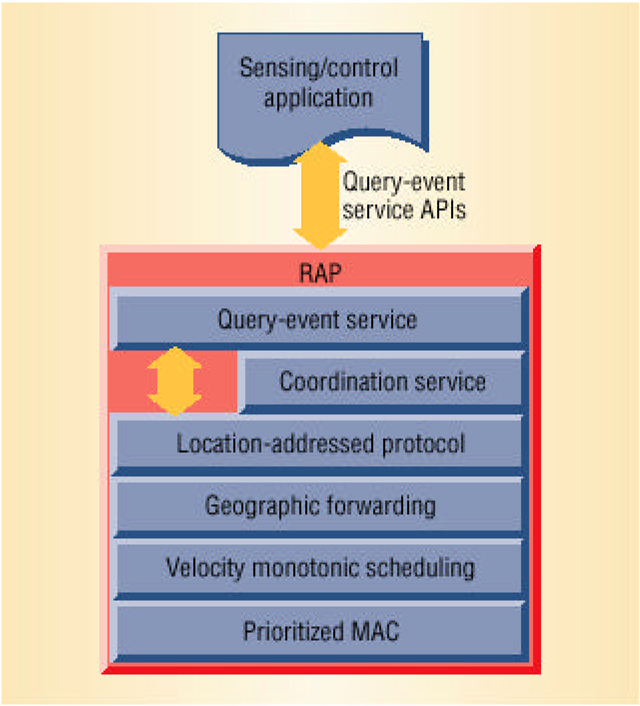



*Figure 3. Real-time location-based protocols (RAP) architecture. RAP encompasses several network layers, from a prioritized media-access-control layer to the query-event API just below the application layer.*

# Conclusion

- **DoS attacks against sensor networks may permit real-world damage to the health and safety of people**

- **Take security into account at design time**

**Table 1. Sensor network layers and denial-of-service defenses.**

| Network layer | Attacks | Defenses |
|---|---|---|
| Physical | Jamming | Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change |
| | Tampering | Tamper-proofing, hiding |
| Link | Collision | Error-correcting code |
| | Exhaustion | Rate limitation |
| | Unfairness | Small frames |
| Network and routing | Neglect and greed | Redundancy, probing |
| | Homing | Encryption |
| | Misdirection | Egress filtering, authorization, monitoring |
| | Black holes | Authorization, monitoring, redundancy |
| Transport | Flooding | Client puzzles |
| | Desynchronization | Authentication |