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

Sensor networks may be 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 always-on monitoring of home healthcare for the elderly, detect chemical or biological threat at airport
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>
<thead>
<tr>
<th>Network layer</th>
<th>Attacks</th>
<th>Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Jamming</td>
<td>Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change</td>
</tr>
<tr>
<td></td>
<td>Tampering</td>
<td>Tamper-proofing, hiding</td>
</tr>
<tr>
<td>Link</td>
<td>Collision</td>
<td>Error-correcting code</td>
</tr>
<tr>
<td></td>
<td>Exhaustion</td>
<td>Rate limitation</td>
</tr>
<tr>
<td></td>
<td>Unfairness</td>
<td>Small frames</td>
</tr>
<tr>
<td>Network and routing</td>
<td>Neglect and greed</td>
<td>Redundancy, probing</td>
</tr>
<tr>
<td></td>
<td>Homing</td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Misdirection</td>
<td>Egress filtering, authorization, monitoring</td>
</tr>
<tr>
<td></td>
<td>Black holes</td>
<td>Authorization, monitoring, redundancy</td>
</tr>
<tr>
<td>Transport</td>
<td>Flooding</td>
<td>Client puzzles</td>
</tr>
<tr>
<td></td>
<td>Desynchronization</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

• Hardware failures, software bugs, resource exhaustion, environmental conditions, any complicated interaction between these factors can cause **DoS**.
Example of Route Discovery mechanism

**DSR - Dynamic Source Routing**

-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

![Diagram]

```
{A}
{A,B}
{A,B, C}
{A,B, C,D}
```

reply:
```
{A,B,C,D,E}
```
Example of Route Discovery mechanism

Route Request

Route Reply
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.
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
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
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
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

S

ACK

D

trash
Network and Routing Layer

Homing

S

D

Leader, Cryptographic Key Manager, Query Access Point ...

Collaborator

Mobile Adversary

Just Listening and Watching

You can attack D, he is important!
Network and Routing Layer

Misdirection (smurf attack)

Source = V
Source = V
Source = V
Source = V
Source = V
Source = V

Echo Replies

Misdirection diverts traffic from its intended destination, perhaps by fabricating malicious route advertisements.
Sensor networks place higher demands on scalability because every node is by design a potential router.
Authorization (defense against misdirection and black hole attacks)

Is he authorized?

0 hops to A
Network and Routing Layer

Monitoring
Network and Routing Layer

Probing

Probe
Network and Routing Layer

Redundancy

S

D

trash
Transport Layer

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
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
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
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.
• 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.

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