Hacking Driverless Vehicles

Zoz
Intelligent Ground Vehicle Competition

RoboBoat

Student Unmanned Aerial Systems

RoboSub

International Aerial Robotics Competition
Advantages:

- Energy efficiency
- Time efficiency
- New applications
The Revolution Is Coming
Two posters are crossed out with the acronym FUD (Fear, Uncertainty, and Doubt). The left poster reads: "HITLER RIDES IN THE EMPTY CAR. DRIVE YOURSELF! KEEP DASTARDLY ROBOTS OFF PUBLIC ROADS." The right poster reads: "When the car drives itself you ride with Hitler!" The last poster reads: "Keep your hands on the WHEEL!"
Autonomous/Unmanned Systems
Autonomous/Unmanned Systems
Autonomous/Unmanned Systems

- No human driver/pilot on-board
- May have off-board controller/supervisor
- May have on-board safety pilot/passengers
- Military early adopters
“Unmanned Advanced Capability Aircraft and Ground Combat Vehicles
It shall be a goal of the Armed Forces to achieve the fielding of unmanned, remotely controlled technology such that by 2015, one-third of the operational ground combat vehicles of the Armed Forces are unmanned.”

Some UGVs are designed with threats in mind...
Civil Applications

Transportation  Oceanography  Mapping

Filmmaking  Powerline Inspection  Logistics
Civil Applications

• Priorities:
  • Precision Agriculture
  • Self-Driving Cars

• Roadblocks:
  • Shared Infrastructure (Airspace, Roads)
  • Acceptance (Safety, Robustness)

• Let’s Talk Failure!
Classic Failures

RQ-3 DarkStar

$10m Unit Procurement Cost (Units 11-20, 1994 $)

On its second flight, due to a software fault in the flight control system the aircraft's porpoising oscillations increased to a nose-high stall as it left the ground and the vehicle crashed.


- Expectations of the designers are critical!
- Exploitation happens at expectation boundary “cracks”
Classic Failures

- Deciding what the robot “knows” is a constant battle
- Correct state estimation is key to decision making
- Successful exploits will most likely subvert state estimation
**Autonomous Vehicle Logic Structures**

**Activity Hierarchy**

- Mission Task Planners/Reasoners
- Navigation & Localization
- Collision Avoidance
- Control Loops, Stability Maintenance

- Attacks lower in the stack defeat everything above
- More engineering effort spent on guaranteed robustness at lower levels
- Lower layers may be juicier but harder targets
### Autonomous Vehicle Logic Structures

**Examples**

<table>
<thead>
<tr>
<th>Mission Task Planners/Reasoners</th>
<th>Control Loops, Stability Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation &amp; Localization</td>
<td></td>
</tr>
<tr>
<td>Collision Avoidance</td>
<td></td>
</tr>
</tbody>
</table>

- Dynamic “bombing run” planner, impact point estimator
- GPS waypoint circuit
- None!
- Autopilot PID loops tuned for environmental conditions
- Dispense pizza to credit card
- Route planning from SLAM-generated sensor map
- Dynamic obstacle discrimination & avoidance
- Balancing, weight shifting

- Extremely vulnerable to collision
- High level logic depends on single sensor
- Vulnerable to redirection, trapping and map-confusion attacks
Autonomous Vehicle Logic Structures

Mission Oriented State Machines

- States may correspond to tasks
- Transitions may be task completions, context switches or timeouts
- States may themselves contain state machines, reasoners, planners etc
Autonomous Vehicle Logic Structures

Example: Robosub Mission

- Vulnerabilities may be in:
  - State estimation
  - Transitions (spoofing or preventing)
  - Unexpected conditions within states
Sensors

- Active vs Passive
- Common sensors:
  - GPS
  - LIDAR
  - Cameras
  - Millimeter Wave Radar
  - Digital Compass
  - IMU
  - Wheel Encoders
  - Doppler Velocity Logger (subsurface)
  - Scanning SONAR (subsurface)
  - Pressure Transducers (air & subsurface)
Sensors

- Sources of uncertainty:
  - Noise
  - Drift
  - Latency & update rate
- Uncertainty must be modeled under assumptions
- Sensor fusion:
  - Fused/registered data can be more useful than separate
  - What to do when sensors disagree?
- Robot robustness may come down to:
  - How smart is it at discounting 1 bad/spoofed sensor?
Sensor Attacks

- 2 kinds:
  - Denial
    - Preventing sensor from recovering useful data
  - Spoofing
    - Causing sensor to retrieve specifically incorrect data

- Basic attack mode choice:
  - Attack sensors directly
  - Attack aggregated sensor data
• Denial:
  • Jamming
• Spoofing:
  • Fake GPS satellite signals at higher power
LIDAR

- Originally industrial monitoring sensors
- Mechanically scanned operation
- Primarily for collision avoidance & map building
- Denial:
  - Active overpowering
  - Preventing return signal
- Spoofing:
  - Manipulating absorbence/reflectivity
LIDAR

- 2D sensor highly orientation dependent
- Inclines can look like obstacles
- May miss low obstacles & discontinuities
LIDAR

- Active emission sensor
- Can only see what returns a signal
- No return = nothing there
- Most of the world returns no data
• Absorbent things look like nothing
• Also transparent
• Reflective things can confuse laser
• Faraway things brought near
• Loss of return looks like ditch
• Reflective things can confuse laser
• Faraway things brought near
• Loss of return looks like ditch
Russian “Racal” GPS jammer

Use of reflective materials to thwart laser deignators
LIDAR

- Reflectance is also a feature
- Road line detection
- Can fake road markings invisibly to human
Cameras

- Specialized object detection
- Sometimes stereo for (noisy!) depth map
- Colorizing LIDAR
- Denial:
  - Easily dazzled
- Spoofing:
  - Camouflage techniques
  - Color assumptions
  - Repeating patterns
MMW RADAR

- Collision avoidance
- Lower resolution than laser
- Most things very reflective

Denial/spoofing:
- Chaff
- Overhead signs
IMU & Compass

- Primary navigation sensor for some systems
- High fidelity models available
  - Typical cumulative error: 0.1% of distance traveled
- Denial/spoofing:
  - Extremely difficult to interfere with
  - Physical attack with magnetic fields
Wheel Odometry

- Encoders
- Useful to know true speed & when stopped
- Attacks:
  - Change wheel diameter
  - Slippery surface
  - Removal may cause unpredictable behavior or stoppage
Bond vs Robots

- GPS Jammer
- Smoke/Dust/Vapor
- Chaff
- Glass caltrops
- Oil slick
The Map

- Great emphasis on preacquired map data
- Often considered to be reference ground truth
- Reduces recognition load
  - Traffic lights
  - Vegetation
  - Other speed control & traffic management features
The Map

- Traffic lights
- Camera knows where to look
- Difference in robot vs human assumptions
The Map

- Vegetation
- Colorized LIDAR
- Transmission classifier
- Overhanging foliage
- Map dependence may exacerbate brittleness of discrimination rules
The Map

- Map requires constant updates
- Local map:
  - Vulnerable to unexpected real world features
- Remote map:
  - Vulnerable to denial (4G jamming)
  - Vulnerable to spoofing (MITM attack, standard cellular intercept techniques)
Exploiting the Logic Structure

- Goal: Maximize uncertainty
- Requiring manual assistance
- Confusing/annoying occupants
- Inconveniencing other road users
- Concentrate on fragile maneuvers
Logic-Based Physical Attacks

• 21st century sabotage
• Dependent on vehicle configuration & mission
• 4G, GPS-enabled electromagnet
  • Near IMU/compass/MMW
• Triggered by map location/activity
Trapping/Redirecting

- Attacks at collision avoidance & navigation layers
- Force robot to postpone high level tasks
  - Moving obstacles
  - Obstacle swarms
  - Artificial stop lights
- Human driver wouldn’t notice, robot can’t ignore
Clobbering

- Goal: make robot run into something
- Subvert collision avoidance
  - Incapacitate vehicle
  - Damage/remove sensors
- Subtle map deviations
- Imitate light vegetation
- Simulate obstacles at speed
- Disguise entrance walls with reflective/absorbent material within GPS noise
- Dynamic obstacles under overhead signs
Remember...

Driverless vehicles are cool!
Don’t do any of these things!

Don’t hassle the Hoff!

Don’t hax0r the Bots!
Instead...

Hack on them!
SUAS

- Tasks:
  - Waypoint navigation
  - Search for & ID secret symbols on ground
  - Connect to narrow-beam wi-fi network
  - Coming soon: package drop?

- Challenges
  - Image/GPS registration
  - Panorama stitching & auto target ID
Roboboat

• Tasks:
  • Channel navigation
  • Direct water cannon on target
  • Identify thermally hot ground item
  • Disable shore-based water spray
  • Deploy ground rover & retrieve package

• Challenges
  • Camera/LIDAR sensor fusion
  • Vegetation/water discrimination
  • Fouling detection
Robosub

- **Tasks:**
  - 3D Navigation
  - Visual target recognition
  - Torpedo shoot
  - Marker drop
  - Object manipulation
  - SONAR pinger seek & package recovery

- **Challenges**
  - GPS-free navigation
  - Robust color discrimination
  - Underwater constraints (e.g. thermal management)
Hack The Rules!

- Nontraditional vehicles
- Experimental power supplies
- Dimension limits apply at start only
- Vehicle swarms
- Hacker sports: find loopholes... and exploit them!
Use those Empty Seats

The car drives itself while you "SHAG"!