Non-invasive Spoofing Attacks for Anti-lock Braking Systems

Yasser Shoukry[1,2], Paul Martin[2],
Paulo Tabuada[1], and Mani Srivastava[2]

Cyber-Physical Systems Laboratory[1]
Networked and Embedded Systems Laboratory[2]

Department of Electrical Engineering
University of California at Los Angeles

Agenda

- Motivation: Attacks on Control Systems
- Anti-Lock Braking Systems (ABS)
- ABS Spoofing Algorithm
- ABS Hacker Hardware
- Implementation Results
- Conclusions

Attacks on Cyber-Physical Systems

- **Side-channel attacks:** How to use the interaction between the physical environment and the embedded processing components to **leak information about** the behavior of the cyber components.
- **Active physical attacks (our work):** How to use the interaction between the physical environment and the embedded processing components to **influence/alter** the behavior of the cyber components.

Attacks on Cyber-Physical Systems

- **Side-channel attacks:** How to use the interaction between the physical environment and the embedded processing components to **leak information about** the behavior of the cyber components.
- **Active physical attacks (our work):** How to use the interaction between the physical environment and the embedded processing components to **influence/alter** the behavior of the cyber components.

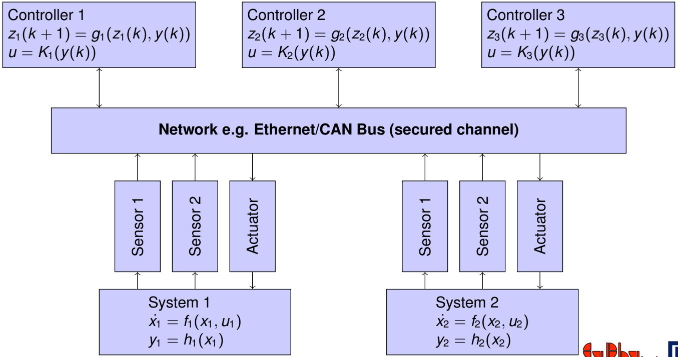
Attacks on Cyber-Physical Systems

- **Side-channel attacks:** How to use the interaction between the physical environment and the embedded processing components to **leak information about** the behavior of the cyber components.
- **Active physical attacks (our work):** How to use the interaction between the physical environment and the embedded processing components to **influence/alter** the behavior of the cyber components.
  - Feedback control system are active systems. Information collected form the physical environment **influence** the decisions of the controller.

Typical control architecture

- Attacks on Control System :
  1. Timing attacks on scheduling over communication bus.
  2. Spoofing or replay of control signals and/or sensor outputs.
  3. Physical attacks on sensors and/or actuators.

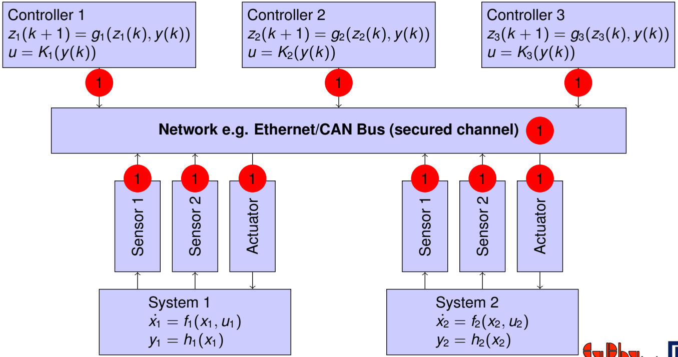
Multiple loops with physically distributed sensors, controllers, and actuators.



Typical control architecture

- Attacks on Control System :
  1. Timing attacks on scheduling over communication bus.
  2. Spoofing or replay of control signals and/or sensor outputs.
  3. Physical attacks on sensors and/or actuators.

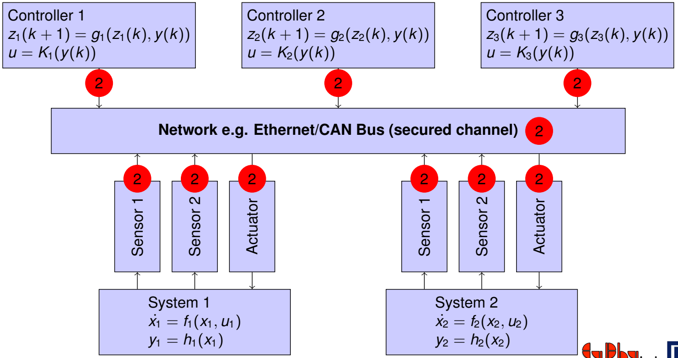
Multiple loops with physically distributed sensors, controllers, and actuators.



Typical control architecture

- Attacks on Control System :
  1. Timing attacks on scheduling over communication bus.
  2. Spoofing or replay of control signals and/or sensor outputs.
  3. Physical attacks on sensors and/or actuators.

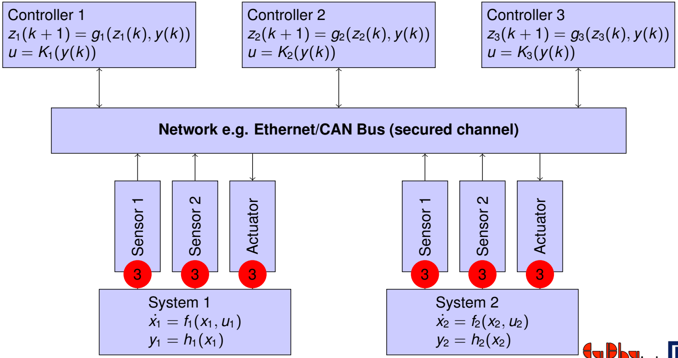
Multiple loops with physically distributed sensors, controllers, and actuators.



Typical control architecture

- Attacks on Control System :
  1. Timing attacks on scheduling over communication bus.
  2. Spoofing or replay of control signals and/or sensor outputs.
  3. Physical attacks on sensors and/or actuators.

Multiple loops with physically distributed sensors, controllers, and actuators.



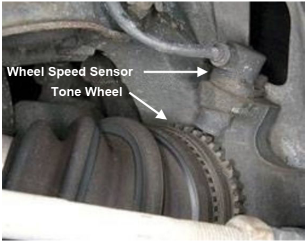
CyPhyLab NESL UCLA

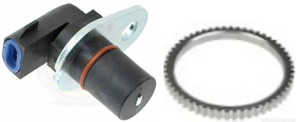
Anti-Lock Braking System

- **In this work:**
  - We play the role of an attacker.
  - Objective: discover how much the attacker can harm the ABS system through its sensors.
- **ABS sensors:**
  - Magnetic speed sensors to measure individual wheel speeds.
  - Sensors are exposed to an external attacker from underneath the body of a vehicle.

Anti-Lock Braking System

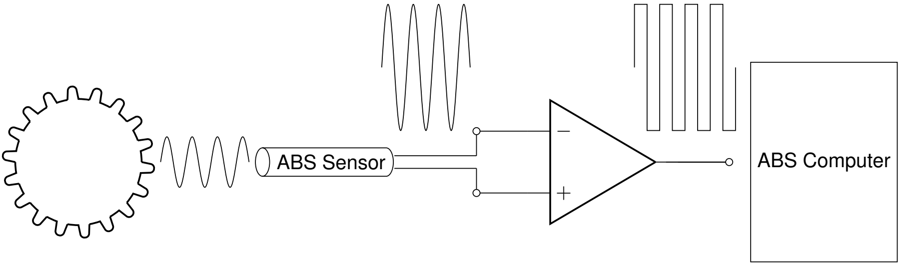
- **In this work:**
  - We play the role of an attacker.
  - Objective: discover how much the attacker can harm the ABS system through its sensors.
- **ABS sensors:**
  - Magnetic speed sensors to measure individual wheel speeds.
  - Sensors are exposed to an external attacker from underneath the body of a vehicle.





CyPhyLab NESL UCLA

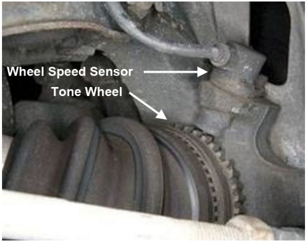
Anti-Lock Braking System



Basic speed sensor operation for ABS systems

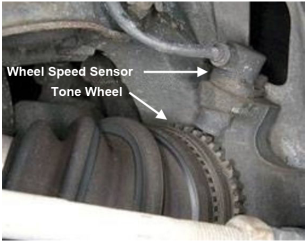
Physical Attacks on ABS Sensors

- **Invasive attacks:**
  - Attacker has to tamper with internal components, e.g., internal circuitry, wiring, or change software.
  - Can be easily detected by smart circuit design and/or tamper proof packaging.
- **Non-invasive attacks:**
  - Attacker alters the physical environment around the sensor.
  - More difficult to detect. System designer can no longer blindly trust the output of the sensor.



Physical Attacks on ABS Sensors

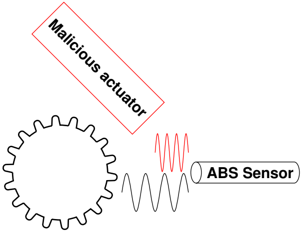
- **Invasive attacks:**
  - Attacker has to tamper with internal components, e.g., internal circuitry, wiring, or change software.
  - Can be easily detected by smart circuit design and/or tamper proof packaging.
- **Non-invasive attacks:**
  - Attacker alters the physical environment around the sensor.
  - More difficult to detect. System designer can no longer blindly trust the output of the sensor.



CyPhyLab NESL UCLA

Non-Invasive Physical Attacks

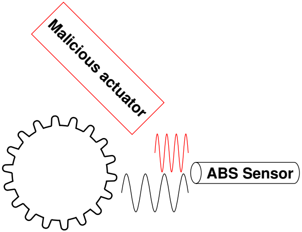
- **Disruptive attack:**
  - Malicious actuator is placed near the ABS sensor.
  - The generated magnetic field is superimposed to the original magnetic field.
  - Result: sensor will measure "wrong" wheel speed.



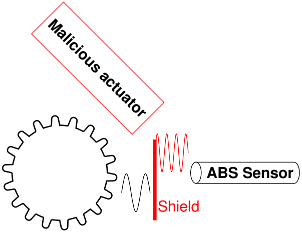
- **Spoofing attack:**
  - Attacker shields the sensor from its environment.
  - ABS sensor measures the synthetic signal.
  - Result: attacker can precisely control the "measured" wheel speed.

Non-Invasive Physical Attacks

- **Disruptive attack:**
  - Malicious actuator is placed near the ABS sensor.
  - The generated magnetic field is superimposed to the original magnetic field.
  - Result: sensor will measure “wrong” wheel speed.



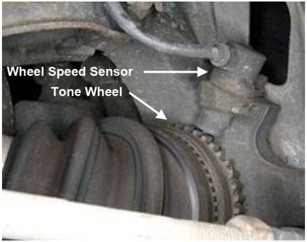
- **Spoofing attack:**
  - Attacker shields the sensor from its environment.
  - ABS sensor measures the synthetic signal.
  - Result: attacker can precisely control the “measured” wheel speed.

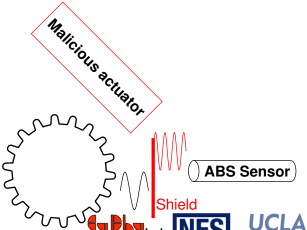


CyPhyLab NESL UCLA

Non-Invasive Spoofing Physical Attacks

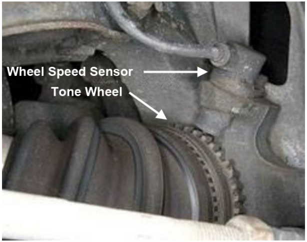
- Passive shield:
  - High permeability ferromagnetic material.
  - Provides return path for the magnetic flux, and thus significantly decreases the magnetic flux reaching the sensor.
  - However, air gap is very small (2-5 mm).
- Active shield:
  - Generates an opposing and canceling magnetic field.
  - Only sensor and actuator need to be mounted in the air gap.

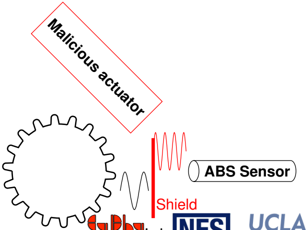




Non-Invasive Spoofing Physical Attacks

- Passive shield:
  - High permeability ferromagnetic material.
  - Provides return path for the magnetic flux, and thus significantly decreases the magnetic flux reaching the sensor.
  - However, air gap is very small (2-5 mm).
- Active shield:
  - Generates an opposing and canceling magnetic field.
  - Only sensor and actuator need to be mounted in the air gap.

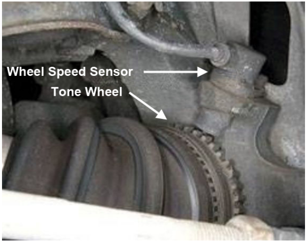


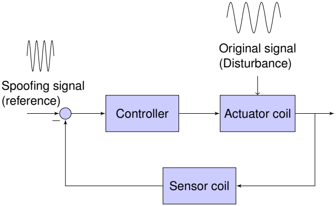


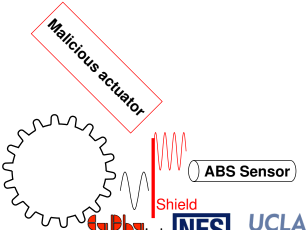
CyPhyLab NESL UCLA

Non-Invasive Spoofing Physical Attacks

- Passive shield:
  - High permeability ferromagnetic material.
  - Provides return path for the magnetic flux, and thus significantly decreases the magnetic flux reaching the sensor.
  - However, air gap is very small (2-5 mm).
- Active shield:
  - Generates an opposing and canceling magnetic field.
  - Only sensor and actuator need to be mounted in the air gap.





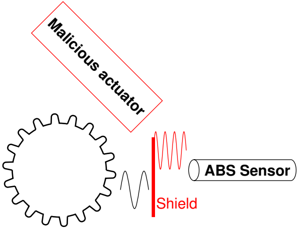


Non-Invasive Spoofing Physical Attacks

- **System Model:**

$$\dot{x} = Ax + Bu + Pw, \qquad (1)$$
$$\dot{w} = Sw, \qquad e = Cx - Qw.$$

$$S = \begin{pmatrix} 0 & \omega_o & 0 & 0 \\ -\omega_o & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_a \\ 0 & 0 & -\omega_a & 0 \end{pmatrix} P = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} Q = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

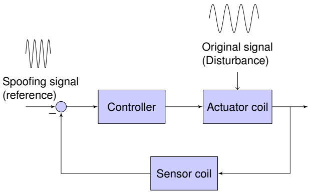


- **Objective** (Error-Feedback Output Regulation): Design a dynamic controller

$$\dot{z} = g(z, e), \qquad u = f(z) \qquad (2)$$

such that

$$(x, z) = (0, 0) \text{ of (1) and (2) is stable}$$
$$\lim_{t \to +\infty} e(t) = 0$$

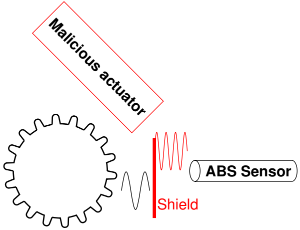


Non-Invasive Spoofing Physical Attacks

- **System Model:**

$$\dot{x} = Ax + Bu + Pw, \qquad (1)$$
$$\dot{w} = Sw, \qquad e = Cx - Qw.$$

$$S = \begin{pmatrix} 0 & \omega_o & 0 & 0 \\ -\omega_o & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_a \\ 0 & 0 & -\omega_a & 0 \end{pmatrix} P = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} Q = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

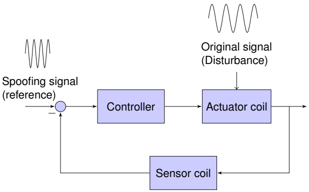


- **Objective** (Error-Feedback Output Regulation): Design a dynamic controller

$$\dot{z} = g(z, e), \qquad u = f(z) \qquad (2)$$

such that

$$(x, z) = (0, 0) \text{ of (1) and (2) is stable}$$
$$\lim_{t \to +\infty} e(t) = 0$$



Error Feedback Output Regulation

- R. Marino, G. Santosuosso, and P. Tomei, “Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency”, Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
  - Transforms the dynamics into the adaptive observer form.
  - Constructs an observer to estimate the unknown frequency.
  - Generates a sinusoidal wave with opposite sign.
- I. D. Landau, A. Constantinescu, and D. Rey, “Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach”, Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
  - Fixes a certain controller structure based on internal model principle.
  - Instead of estimating the frequency of the disturbance, the controller is parametrized such that only one parameter needs to be adapted.
  - A simple optimization procedure is used to adapt the controller parameter.
- A. Isidori, L. Marconi, and L. Praly, “Robust design of nonlinear internal models without adaptation”, Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.
  - Unlike the adaptive techniques, the objective is to design a robust observer and controller.
  - Utilizes a non-linear high-gain observer and a non-linear controller to suppress the unknown frequency.

Error Feedback Output Regulation

- R. Marino, G. Santosuosso, and P. Tomei, “Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency”, Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
  - Transforms the dynamics into the adaptive observer form.
  - Constructs an observer to estimate the unknown frequency.
  - Generates a sinusoidal wave with opposite sign.
- I. D. Landau, A. Constantinescu, and D. Rey, “Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach”, Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
  - Fixes a certain controller structure based on internal model principle.
  - Instead of estimating the frequency of the disturbance, the controller is parametrized such that only one parameter needs to be adapted.
  - A simple optimization procedure is used to adapt the controller parameter.
- A. Isidori, L. Marconi, and L. Praly, “Robust design of nonlinear internal models without adaptation”, Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.
  - Unlike the adaptive techniques, the objective is to design a robust observer and controller.
  - Utilizes a non-linear high-gain observer and a non-linear controller to suppress the unknown frequency.

Error Feedback Output Regulation

- R. Marino, G. Santosuosso, and P. Tomei, “Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency”, Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
  - Transforms the dynamics into the adaptive observer form.
  - Constructs an observer to estimate the unknown frequency.
  - Generates a sinusoidal wave with opposite sign.
- I. D. Landau, A. Constantinescu, and D. Rey, “Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach”, Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
  - Fixes a certain controller structure based on internal model principle.
  - Instead of estimating the frequency of the disturbance, the controller is parametrized such that only one parameter needs to be adapted.
  - A simple optimization procedure is used to adapt the controller parameter.
- A. Isidori, L. Marconi, and L. Praly, “Robust design of nonlinear internal models without adaptation”, Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.
  - Unlike the adaptive techniques, the objective is to design a robust observer and controller.
  - Utilizes a non-linear high-gain observer and a non-linear controller to suppress the unknown frequency.

Error Feedback Output Regulation

- R. Marino, G. Santosuosso, and P. Tomei, “Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency”, Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
  - Transforms the dynamics into the adaptive observer form.
  - Constructs an observer to estimate the unknown frequency.
  - Generates a sinusoidal wave with opposite sign.
- I. D. Landau, A. Constantinescu, and D. Rey, “Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach”, Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
  - Fixes a certain controller structure based on internal model principle.
  - Instead of estimating the frequency of the disturbance, the controller is parametrized such that only one parameter needs to be adapted.
  - A simple optimization procedure is used to adapt the controller parameter.
- A. Isidori, L. Marconi, and L. Praly, “Robust design of nonlinear internal models without adaptation”, Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.
  - Unlike the adaptive techniques, the objective is to design a robust observer and controller.
  - Utilizes a non-linear high-gain observer and a non-linear controller to suppress the unknown frequency.

- R. Marino, G. Santosuosso, and P. Tomei, “Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency”, Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
  - Transforms the dynamics into the adaptive observer form.
  - Constructs an observer to estimate the unknown frequency.
  - Generates a sinusoidal wave with opposite sign.
- I. D. Landau, A. Constantinescu, and D. Rey, “Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach”, Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
  - Fixes a certain controller structure based on internal model principle.
  - Instead of estimating the frequency of the disturbance, the controller is parametrized such that only one parameter needs to be adapted.
  - A simple optimization procedure is used to adapt the controller parameter.
- A. Isidori, L. Marconi, and L. Praly, “Robust design of nonlinear internal models without adaptation”, Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.
  - Unlike the adaptive techniques, the objective is to design a robust observer and controller.
  - Utilizes a non-linear high-gain observer and a non-linear controller to suppress the unknown frequency.

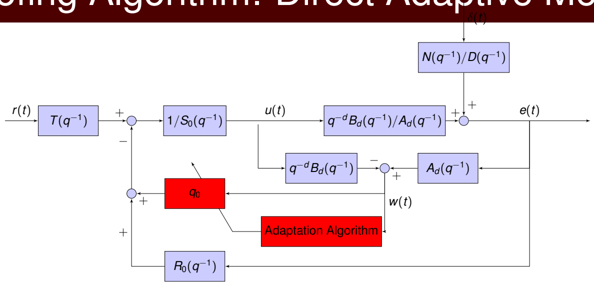
Error Feedback Output Regulation

- R. Marino, G. Santosuosso, and P. Tomei, "Robust adaptive compensation of biased sinusoidal disturbances with unknown frequency", Automatica, vol. 39, no. 10, pp. 1755 – 1761, 2003.
- I. D. Landau, A. Constantinescu, and D. Rey, "Adaptive narrow band disturbance rejection applied to an active suspension-an internal model principle approach", Automatica, vol. 41, no. 4, pp. 563 – 574, 2005.
- A. Isidori, L. Marconi, and L. Praly, "Robust design of nonlinear internal models without adaptation", Automatica, vol. 48, no. 10, pp. 2409 – 2419, 2012.

Metric	**Indirect Adaptive Method**	**Direct Adaptive Method**	**Nonlinear High gain Observer**
Number of states	18	12	8
Matrix Inversion	9×9	N/A	8×8

CyPhyLab NESL UCLA

ABS Spoofing Algorithm: Direct Adaptive Method

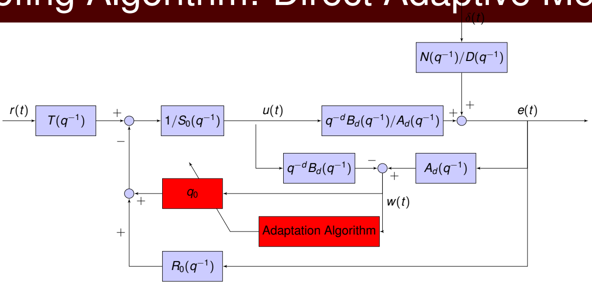


Idea: Design an adaptive filter as following:

1. Fix the filter structure.
2. Allow only one parameter q_0 to be adapted.
3. Use gradient descent to update q_0 such that:

$$\arg\min_{\hat{q}_0} [e(t)]^2$$

ABS Spoofing Algorithm: Direct Adaptive Method

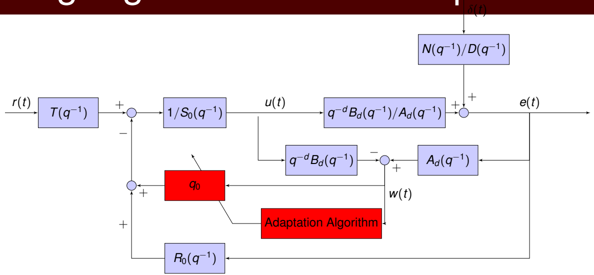


Idea: Design an adaptive filter as following:

1. Fix the filter structure.
2. Allow only one parameter q_0 to be adapted.
3. Use gradient descent to update q_0 such that:

$$\arg\min_{\hat{q}_0} [e(t)]^2$$

ABS Spoofing Algorithm: Direct Adaptive Method



Idea: Design an adaptive filter as following:

1. Fix the filter structure.
2. Allow only one parameter q_0 to be adapted.
3. Use gradient descent to update q_0 such that:

$$\arg\min_{\hat{q}_0} [e(t)]^2$$

$$q_{0_{n+1}} = q_{0_n} + F_n \phi_n \epsilon_{n+1},$$

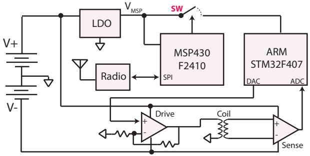
$$F_{n+1} = \frac{1}{\lambda_{1_n}} \left[F_n - \frac{F_n \phi_n \phi_n^T F_n}{\frac{\lambda_{1_n}}{\lambda_2} + \phi_n^T F_n \phi_n} \right]$$

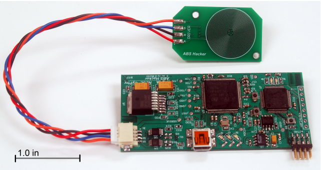
$$\lambda_{1_n} = \begin{cases} \lambda_0 \lambda_{1_{n-1}} + 1 - \lambda_0 & \text{if } \lambda_{1_n} > \lambda_{threshold} \\ \lambda_{threshold} & \text{otherwise} \end{cases}$$

From Theory to Practice

ABS Hacker Hardware

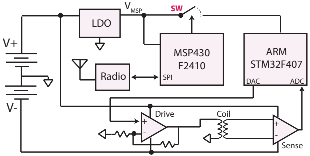
- **Actuator:**
  - Stack of 4-flat PCB coils driven by high current op-amp.
  - By increasing the number of internal layers, the number of coil turns increases and thus current decreases.
- **Sensor and filtering:**
  - Flat coil with differential output.
  - Two phase filters:
    - Amplification: using instrumentation amplifier with high common-mode rejection.
    - Noise rejection: elliptic curve low pass filter.
- Both sensor and actuator are designed to fit within the air-gap in the ABS sensor (final width = 0.95 mm).

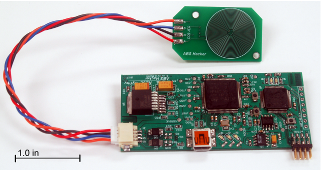




ABS Hacker Hardware

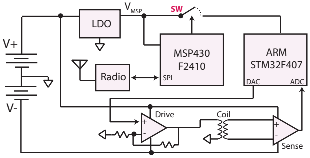
- **Actuator:**
  - Stack of 4-flat PCB coils driven by high current op-amp.
  - By increasing the number of internal layers, the number of coil turns increases and thus current decreases.
- **Sensor and filtering:**
  - Flat coil with differential output.
  - Two phase filters:
    - Amplification: using instrumentation amplifier with high common-mode rejection.
    - Noise rejection: elliptic curve low pass filter.
- Both sensor and actuator are designed to fit within the air-gap in the ABS sensor (final width = 0.95 mm).

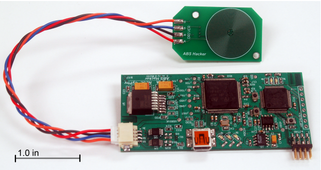




ABS Hacker Hardware

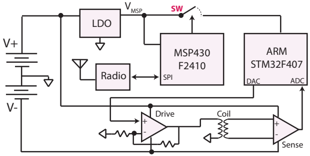
- **Actuator:**
  - Stack of 4-flat PCB coils driven by high current op-amp.
  - By increasing the number of internal layers, the number of coil turns increases and thus current decreases.
- **Sensor and filtering:**
  - Flat coil with differential output.
  - Two phase filters:
    - Amplification: using instrumentation amplifier with high common-mode rejection.
    - Noise rejection: elliptic curve low pass filter.
- Both sensor and actuator are designed to fit within the air-gap in the ABS sensor (final width = 0.95 mm).

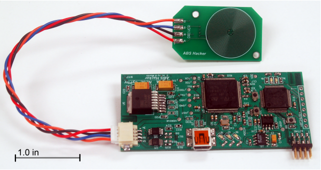




ABS Hacker Hardware

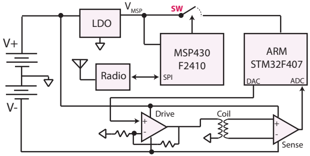
- **Low power MSP430F2410:**
  - Polls the radio interface until the attack command is received.
  - Boots up the powerful processor with its peripherals.
- **High power ARM Cortex M4 STM32F407:**
  - Powerful processor for DSP computations needed for active shielding (runs at 2.5 KHz).
- **Current consumption:**
  - 6.18 mA in idle mode which corresponds to 5.4 days.
  - 109 mA in attack mode which corresponds to 3 hour attack.

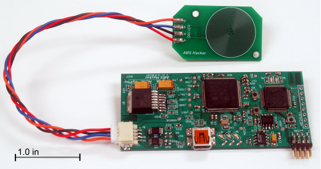




ABS Hacker Hardware

- **Low power MSP430F2410:**
  - Polls the radio interface until the attack command is received.
  - Boots up the powerful processor with its peripherals.
- **High power ARM Cortex M4 STM32F407:**
  - Powerful processor for DSP computations needed for active shielding (runs at 2.5 KHz).
- **Current consumption:**
  - 6.18 mA in idle mode which corresponds to 5.4 days.
  - 109 mA in attack mode which corresponds to 3 hour attack.

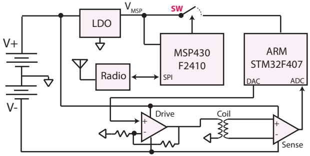


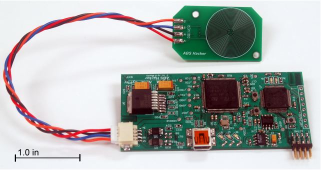


CyPhyLab NESL UCLA

ABS Hacker Hardware

- **Low power MSP430F2410:**
  - Polls the radio interface until the attack command is received.
  - Boots up the powerful processor with its peripherals.
- **High power ARM Cortex M4 STM32F407:**
  - Powerful processor for DSP computations needed for active shielding (runs at 2.5 KHz).
- **Current consumption:**
  - 6.18 mA in idle mode which corresponds to 5.4 days.
  - 109 mA in attack mode which corresponds to 3 hour attack.

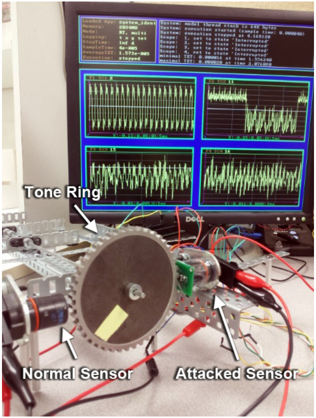




Implementation Results

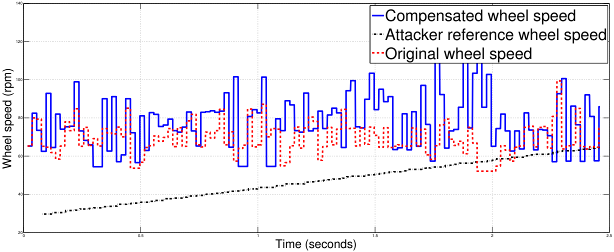
The used testbed includes:

- Two Mazda RX7 ABS sensors.
  - One provides the actual speed.
  - The other suffers the attack.
- Mounted on the same Mazda RX7 tone ring.
- MAX9926U ABS sensor interface evaluation kit.
- Tone ring is rotated using a DC motor controlled through Matlab xPC target.



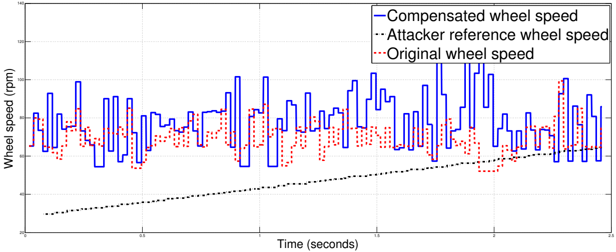
Implementation Results

Disruptive Attack:

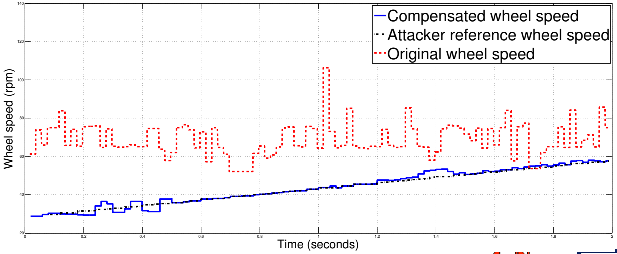


Implementation Results

Disruptive Attack:



Spoofing Attack:



Implementation Results

Conclusions

- Non-invasive attacks on cyber-physical systems pose considerable threats.
- Such attacks are harder to detect at the sensor level and thus require higher level detection mechanisms
- Small electronic module is designed and implemented to show the feasibility of the idea using ABS as an example.