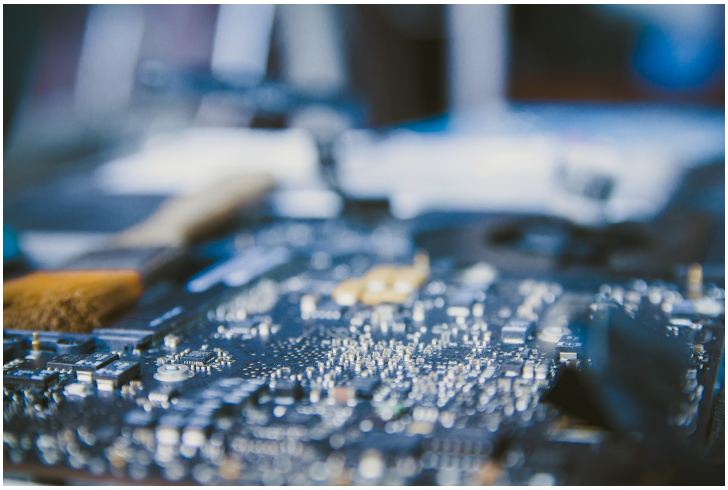
INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

Methods and Systems to Protect MEMS Sensors from Intentional Acoustic Interference

TECHNOLOGY NUMBER: 7092



OVERVIEW

Protecting MEMS gyroscopes and accelerometers from malicious acoustic attacks

- Prevents erratic behavior by using innovative signal sampling
- Applicable to drones, IoT devices, automotive systems, industrial automation

BACKGROUND

MicroElectroMechanical Systems (MEMS) sensors like accelerometers and gyroscopes measure motion and angular momentum and are integral to many modern technologies, including drones, automotive systems, and various Internet of Things (IoT) devices. Historically, these sensors have been used to enable precise motion detection and control. However, recent studies have uncovered a vulnerability wherein acoustic waves at resonant frequencies can maliciously manipulate the sensor outputs, leading to unstable system behavior or even complete failure. Traditional approaches, such as signal filtering and physical shielding, have proven inadequate in fully safeguarding these sensors from such sophisticated attacks. Given the increasing reliance on MEMS sensors for mission-critical applications, a need exists for robust methods to protect against these vulnerabilities and ensure reliable system

Technology ID

7092

Category

Hardware

Engineering & Physical Sciences

Inventor

Kevin Fu
Ofir Weisse
Peter Honeyman
Timothy Trippel

Further information

Joohee Kim
jooheek@umich.edu

Learn more

performance.

INNOVATION

Researchers have developed innovative sampling strategies to neutralize the impact of malicious acoustic attacks on MEMS sensors. By dynamically varying the sampling rates and patterns, the system can disrupt the predictable interference patterns produced by acoustic waves, thereby preventing them from creating consistent or semi-consistent effects on the sensor outputs. This approach significantly enhances the resilience of systems that depend on MEMS sensors, such as drones, automotive safety features, and various IoT devices. The potential applications are broad and impactful; this technology can prevent dangerous malfunctions in critical environments like self-driving cars, industrial automation, and even medical devices, ensuring both safety and reliability in the face of evolving cyber-physical threats.