MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FOR IMMEDIATE RELEASE **No. 3252**

Customer Inquiries

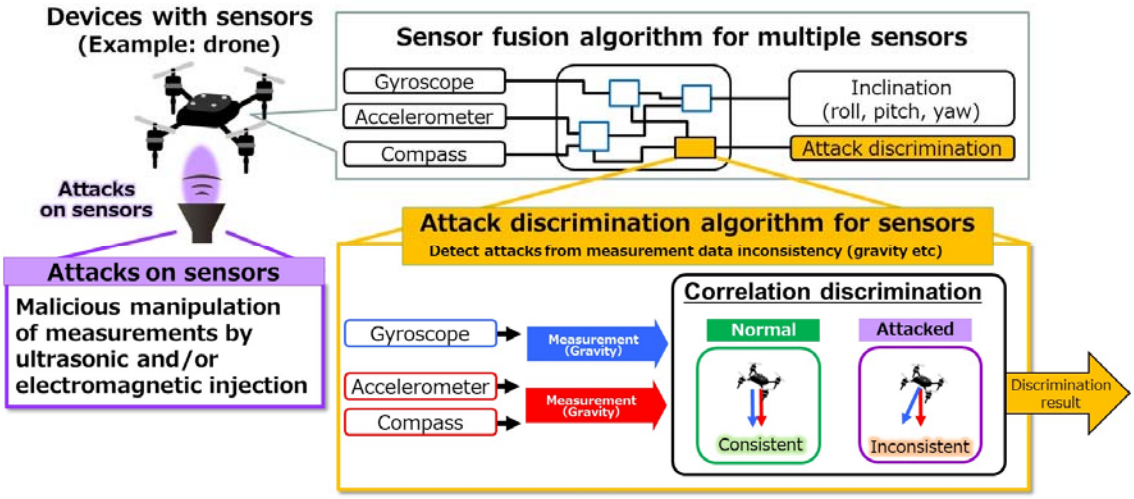
Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

Media Inquiries
Niels Meinke
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric Develops Security Technology to Detect Attacks on Equipment Sensors

World's first attack algorithm for sensors used in drones, cars, production equipment and more

TOKYO, February 7, 2019 – Mitsubishi Electric Corporation (TOKYO: 6503) announced today that it has developed what is believed to be the world's first sensor-security technology that detects measurement-data inconsistencies by embedding a proprietary algorithm in sensor fusion algorithms, which combine multiple sensors for measurements used in the automatic control of drones, in-vehicle devices, production equipment and more. Going forward, the company will continue development with the aim to commercialize the technology from the year 2020 onwards.



Application example using a drone

Key Features

Mitsubishi Electric's new algorithm detects malicious attacks based on more than 42 percent inconsistencies in measurement data. In the case of ultrasonic attacks on drones, for example, the Earth's magnetism or gravity is calculated in two ways using intermediate values in the sensor fusion algorithm, and any difference between the two results is treated as an inconsistency.

The new algorithm can be implemented at low cost as additional software in existing sensor signal processing circuits without the need to add or modify hardware. The accuracy of sensor measurements is not compromised.

Comparison

	Function	Disturbance correction (heat, magnetism, etc.)	Attack detection
Developed Technology	Sensor attack detection	Possible	Possible
Conventional Technology	Sensor fusion	Possible	Impossible

Background

Sensor-based automatic control is becoming increasingly common in everyday applications such as drones, in-vehicle devices and production facilities, raising the need for cybersecurity countermeasures. Sensor fusion algorithms, which combine multiple sensors for measurement, play a key role in automatic control, but their security performance was unproven.

In response, Mitsubishi Electric developed what is believed to be the world's first sensor-security technology that detects inconsistencies in sensor measurements during malicious attacks. The development was partially supported by business commissioned by the New Energy and Industrial Technology Development Organization (NEDO) under Japan's National Research and Development Agency.

Details

1) Attack detection algorithm for sensors

Until now, effective countermeasures have not existed for malicious attacks that apply abnormal signals to sensors. Sensor fusion algorithms, which combine multiple sensors for measurement, were thought to offer attack resistance as well as high-accuracy measurements, but due to the complexity of algorithms and the difficulty of creating an evaluation environment, it had not been proven that the algorithms were actually resistant to attacks nor under what conditions attacks could succeed relatively easily.

Mitsubishi Electric, recognizing the potential of using the internal calculations of sensor fusion algorithms, has exploited these calculations in a novel embeddable attack-detection algorithm. Malicious attacks are detected on the basis of inconsistencies between measurements from various sensors, such as compasses, gyros and/or accelerometers used for the automatic control of drones. The algorithm does not compromise computation speed because it exploits intermediate values calculated by the sensor fusion algorithm.

Mitsubishi Electric also created an advanced evaluation environment that applies abnormal signals individually to each sensor, such as a drone's compass, gyro and accelerometer, as well as simultaneously to multiple sensors. Using this environment, Mitsubishi Electric has confirmed significant differences between disturbances caused by natural physical phenomena and measurement inconsistencies caused by

malicious cyber-attacks.

2) Low-cost implementation in autonomous devices with sensors

The new sensor security technology can be added to devices such as drones at low cost because it can be implemented in existing sensor-signal processing circuits without having to modify the hardware or make any other addition.

Patents

Pending patents for the technologies announced in this news release number two in Japan and two outside of Japan.

###

About Mitsubishi Electric Corporation

With nearly 100 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 4,444.4 billion yen (in accordance with IFRS; US$ 41.9 billion*) in the fiscal year ended March 31, 2018. For more information visit:
www.MitsubishiElectric.com

*At an exchange rate of 106 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2018