Using Supplemental Encrypted Signals to Mitigate Man-in-the-Middle Attacks on Teleoperated Systems

Teleoperated robotics need security systems to avoid misuse, tampering, and harmful security threats. This technology offers a mitigation system that protects against replay, spoofing, false data injection, and man-in-the-middle attacks using two independent detection systems. This multi-detector system uses encrypted signals to control inputs in the operators' remote devices' that will quickly and reliably detect malicious feedbacks.

What is the Problem?

Advances in robotics, embedded systems and information systems are enabling a rapid development of teleoperated robotic systems serving as extensions of people, such as those used in bomb disposal, remotely operated aircraft and underwater vehicles, search and rescue and robotic surgery. Human operators, often geographically distant, interact with robots through a communication channel. Natural and human-caused disaster circumstances impose specific constraints on teleoperated robotic systems. The systems are expected to operate with limited power resources, often lacking a basic infrastructure, and in challenging climates and environments. Some of the applications of such systems include handling radioactive material; operating unmanned vehicles for air (e.g., UAV, drone), space (e.g., near Earth's orbit or a manned platform or vehicle), land, and underwater (e.g., ROV) exploration; and telesurgery. With an increase in possible applications, however, the risk of such systems being misused, deliberately tampered with, or even compromised increases as well. These security threats are especially harmful if teleoperated robotic systems are used for inspection, repair and manipulation, such as in telerobotic surgery systems. There is a need to increase security in these systems.

What is the Solution?

This solution is a novel mitigation system designed to protect tele-operated systems against replay, spoofing, false data injection, and man-in-the-middle attacks. The invention consists of two or more detection systems, independently operating on both the operators' and the remote device sides. It utilizes encrypted signals, which are incorporated into the operators' control inputs and into the remote devices' feedback signals. These encrypted signals could be added, multiplied or otherwise combined with the control and feedback signals. These signals contain information about the operators' and the remote devices' unique identities, as well as about the content and time of transmitted messages.

Technology ID

BDP 8674

Category

Selection of Available Technologies

Hardware/Telecom/Wireless

Authors

Howard Chizeck

Learn more

What is the Competitive Advantage?

Current systems have limited security, which leaves many systems vulnerable to tampering and becoming compromised. This multi-detector system with supplemental encrypted signals will quickly and reliably detect any maliciously altered control and feedback messages, prevent any false control and input messages from being accepted and implemented, and can be used as a failure detection mechanism, in case of any benign failure.

Patent Information:

US9686306B2

References

1. Tamara Bonaci, Howard Jay Chizeck(45608) , https://ieeexplore.ieee.org/document/6523908, 2012 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)