

Enhanced Security and Safety in Telerobotic Systems

Existing telerobotics systems are vulnerable to security threats that create hostile operating environments that can be time sensitive. This technology offers a specialized coprocessor in telerobotic systems, specifically in surgical systems that guarantee information security using authentication and monitoring algorithms.

What is the Problem?

Advances in robotics, embedded and information systems are enabling a rapid development of tele-operated robotic systems. 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 tele-operated robotic systems are used for inspection, repair and manipulation, such as in telerobotic surgery systems.

What is the Solution?

The invention is the addition and use of a specialized coprocessor in telerobotic systems, and more particularly for telerobotic surgical systems, for purposes of security. This will be done on the surgical manipulator side of the system (at the patient location, rather than the surgeon location). It will be used to implement security methods and algorithms. These security algorithms include: encryption algorithms; session initiation and authentication methods and monitoring and anomaly detection algorithms. These are used to guarantee information security requirements for telesurgical systems. With this approach security methods are implemented and run in parallel with regular surgical robotic manipulator and sensor processing computations. Thus, security methods do not use regular computation resources and therefore do not increase communication delay or overall latency of the telesurgical system.

What Differentiates it from Solutions Available Today?

Currently, open and unpredictable communication media, hostile operating environments and time-criticality of surgical procedures render existing telerobotics systems vulnerable to security threats, including eavesdropping, message modification, and denial-of-service. There is limited

Technology ID

BDP 8675

Category

Software/Security

Selection of Available

Technologies

Authors

Howard Chizeck

Learn more



existing work involving security of telesurgical robotic systems. This system will enable higher security for telerobotic surgical systems, while not causing a communication delay or increasing the latency of the system. This will increase the effectiveness and reliability of these telerobotic surgical systems.

Patent Information:

[US9736167B2](#)