# Surgical Telerobotics Meets Information Security

Tamara Bonaci and Howard Jay Chizeck

***Abstract*—The next generation of surgical telerobotics systems, including portable telerobotics systems, are envisioned to provide a medical relief in the areas of natural disasters and battlefield environments. In such systems, one or more distant surgeons control a surgical manipulator through a communication network that may combine wired and wireless components. Due to an open nature of the wireless medium, hostile operating environments and time-criticality of surgical procedures, such telerobotics systems are vulnerable to a variety of security threats. In this paper, we analyze some the threats and discuss their impact.**

## I. Introduction

Recent developments in robotics and computer-aided systems have advanced the field of surgical robotics and enhanced the way health services are delivered to the patients. They have revolutionized minimally invasive surgical procedures, resulting in better outcomes and faster patient recovery [2].

Research and design of *portable* surgical telerobotics systems [6], where one or more surgeons operate a remote manipulator through either an existing communication infrastructure or a temporary wireless network, is recognized as the next step in surgical robotics. These portable (or mobile) telerobotics systems are envisioned to provide an immediate medical relief in the areas of natural disasters, and in the battlefield scenarios [1, 5].

Extreme battlefield environments impose, however, specific constraints on surgical telerobotics systems. They are expected to operate in situations lacking a basic infrastructure, often with limited power resources [5, 9]. Despite such harsh operating conditions, patients' safety must be established, maintained and guaranteed through the whole procedure.

To this end, the development of patient-safe portable surgical telerobotics systems and the analysis of their performance in extreme environments is an active research area. In recent years, several extreme environment research missions were conducted [1, 9], and the following network states were recognized as critical to system's performance [4]: (i) communication latency, (ii) jitters, (iii) packet delays and out-of-order arrivals, (iv) packet losses, and (v) devices failures.

In addition to these stochastic but benign network patterns, we recognize that surgeon-manipulator communication over publicly available, or even dedicated, wireless networks exposes mobile telerobotics systems to a novel set of problems, that were not present in wired, hospital settings. Due to the relatively open and uncontrollable nature of the wireless medium, it becomes easy for malicious entities (adversaries) to jam, disrupt, or even take over the communication between the surgeon and the manipulator, thus impacting surgical procedures. In battlefield environments, for example, adversaries may specifically target portable surgical systems in order to harm wounded soldiers and increase human casualties.

Thus, in order to develop *patient-safe* portable telerobotics surgical systems, it is necessary to ensure that these systems are *information secure*. The first step towards doing so is identifying possible security threats against such systems, and understanding their range and impact.

## II. Security Threats

Based on the exploited system property, we classify security threats against mobile surgical telerobotics systems into: i) attacks against the wireless communication, ii) attacks targeting surgeon-manipulator interaction, iii) attacks on the surgeon-side software (e.g., attacks exploiting development (engineering) interfaces), iv) attacks on the manipulator-side software (e.g., attacks on the programmable logical controllers (PLC)), and v) physical attacks. In the rest of this section, we focus is on the first two attack classes.

### *A. Attacks Against the Wireless Communication Medium*

Currently, the common communication paradigm in mobile surgical telerobotics systems is unencrypted, unauthenticated wireless communication. The messages between a surgeon and a manipulator are exchanged using the User Datagram Protocol (UDP) [4], a low-latency protocol. UDP is used because it is very fast, and commanded surgical tool motions are made in very small increments, so as to reduce the negative effects of lost packets. This protocol, however, does not provide a reliable service. Thus, even in benign environments messages may arrive out-of-order, may be duplicated or lost.

In hostile environment, however, an unencrytpted wireless channel renders mobile surgical telerobotic systems vulnerable to following attacks, mounted by the adversaries within the manipulator's communication range:

- **Eavesdropping**, where an adversary passively listens on the communication between one or more surgeon(s) and the manipulator.
- **Jamming,** depicted in Figure 1, where an active adversary deliberately introduces noise into the channel, in order to increase the communication delay between the surgeon and the manipulator, or even completely disrupt message exchange, thus effectively disabling the surgical telerobotics system.
- **Message modification/False data injection,** where an adversary either modifies transmitted messages or injects false messages, in order to destabilize the manipulator. By spoofing surgeon control inputs, the adversary may cause the manipulator to move in an undesired and unsafe direction. Further, by modifying feedback messages, the adversary may cause the surgeon to generate incorrect

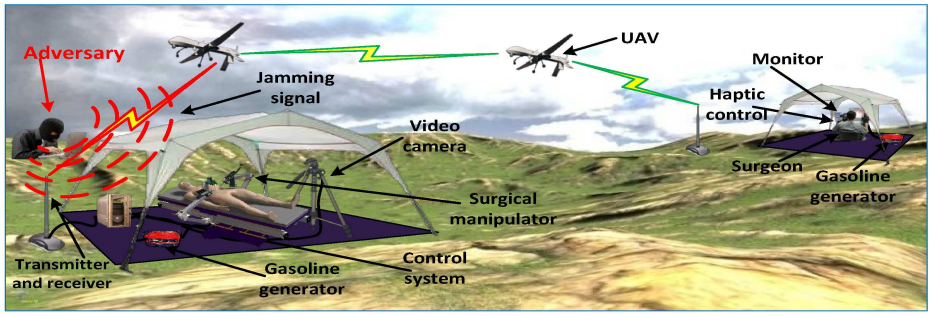


Fig. 1. An example of the jamming attack on a mobile surgery telerobotics system: an adversary constantly jams all control inputs. As a result, the manipulator is unable to determine its next position, and the remote surgical procedure is interrupted.

control inputs, thus driving the manipulator to an undesired operating point. Both types of the attack may potentially harm the patient.

Additionally, in multi-hop wireless networks, the adversary may resort to using **corrupted intermediate nodes**. While the use of such nodes may not be feasible in systems using dedicated wireless networks, such as systems with UAV-enabled communication [1, 5], it allows the adversary to eavesdrop, modify, delay or drop control and feedback messages from a distance, thus keeping his identity and location hidden.

### *B. Attacks Targeting Surgeon-Manipulator Interaction*

In the network security literature (e.g., [3, 8]), attacks on the wireless medium, such as eavesdropping and message modification, are typically mitigated using encryption algorithms. However, even if a surgeon and a manipulator communicate through an encrypted channel, the lack of an authentication mechanism between them renders a mobile surgical system vulnerable to a **man-in-the-middle** (MTIM) attack [7].

In this type of active attack, an adversary first blocks valid messages between the surgeon and the surgical manipulator, and then creates independent connections with both entities. By doing so, the adversary effectively gains control over the procedure, while making the surgeon and the manipulator believe they are talking directly over an encrypted channel.

MTIM attacks are especially malicious since the adversary may exploit different properties of the mobile telerobotics system to mount them. In order of increasing level of impact, we identify the following types of the MTIM attack as feasible:

- **Simple replay,** where an adversary receives messages and replays them to the recipient.
- **Delay attack,** where the adversary delays received messages for some chosen amount of time before forwarding them to the intended recipient.
- **Message dropping,** where the adversary simply drops some or all of the received messages.
- **Combined delay and drop attack,** where the adversary randomly delays some, and drops other messages, possibly in both directions.
- **Message modification and spoofing attack,** where an adversary modifies received messages, or creates false messages in order to render the procedure unsafe.

In the delay-MTIM attack, for example, the adversary may allow transmission of control messages, but delay feedback messages. The surgeon, upon concluding that the manipulator has not received the control input, repeats the same message. The manipulator, which has been correctly receiving control messages, simply drops this already-implemented messages and does nothing. The surgical system is now effectively in a dead-lock, and remains in this state until the adversary releases the delayed messages. Moreover, if the adversary decides to drop feedback messages, the surgical telerobotics systems remains in the dead-lock, as neither the surgeon nor the manipulator can recover from the current state.

## III. Conclusion

In this paper, we have classified security threats against mobile surgical telerobotics systems into five main groups, and analyzed the first two groups (the attacks against wireless communication and against surgeon-manipulator interaction). Communication networks security is an active research area and many existing mitigation strategies may be applicable to surgical telerobotics systems. Identifying those, as well as developing novel, specialized mitigation strategies, and analyzing their impact on system's performance, security and safety is an emerging research question.

## References

[1] B.M. Harnett, C.R. Doarn, J. Rosen, B. Hannaford, and T.J. Broderick. Evaluation of unmanned airborne vehicles and mobile robotic telesurgery in an extreme environment. *Telemedicine and e-Health*, 14(6):539–544, 2008.

[2] J.C. Hu, X. Gu, S.R. Lipsitz, M.J. Barry, A.V. DAmico, A.C. Weinberg, and N.L. Keating. Comparative effectiveness of minimally invasive vs open radical prostatectomy. *The Journal of the American Medical Association*, 302(14):1557–1564, 2009.

[3] C. Kaufman, R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World*. Prentice Hall, 2002.

[4] H.H. King, K. Tadano, R. Donlin, D. Friedman, M.J.H. Lum, V. Asch, C. Wang, K. Kawashima, and B. Hannaford. Preliminary protocol for interoperable telesurgery. In *the Proc. of the International Conference on Advanced Robotics*, pages 1–6, 2009.

[5] J. Rosen and B. Hannaford. Doc at a distance. *IEEE Spectrum*, 43(10):34–39, 2006.

[6] G. Sankaranarayanan, H.I. King, S.Y. Ko, M.J.H. Lum, D.C.W. Friedman, J. Rosen, and B. Hannaford. Portable surgery master station for mobile robotic telesurgery. In *the Proc. of the 1st International Conference on Robot Communication and Coordination*, pages 20–28, 2007.

[7] D.N. Serpanos and R.J. Lipton. Defense against man-in-the-middle attack in client-server systems. In *the Proceedings of the 6th IEEE Symposium on Computers and Communications*, pages 9–14, 2001.

[8] W. Stallings. *Cryptography and network security*, volume 2. Prentice hall, 2003.

[9] A.C. Yoo, G. R. Gilbert, and T.J. Broderick. Military robotic combat casualty extraction and care. *Surgical Robotics: Systems Applications and Visions*, pages 13–32, 2010.