Enhancing Security for Robot-Assisted Surgery through Advanced Authentication Mechanisms Over 5G Networks

Shaman Bhat and Ashwin Kavasseri

Abstract — The adoption of robotic surgical procedures over wireless 5G networks has increased rapidly in recent years, providing improved precision and patient outcomes. However, the security and reliability of the end-to-end information between the surgeon's control console and the robotic system are critical concerns. This paper proposes a solution to enhance the security and reliability of the authentication process in robot-assisted surgery by enhancing existing authentication mechanisms. The proposed solution builds upon the existing Transport Layer Security (TLS) protocol, and introduces additional security measures, including biometric authentication and multi-factor authentication while minimizing latency and delay in transmission. The effectiveness of the proposed solution is evaluated through simulation and testing, demonstrating its ability to provide enhanced security for robot-assisted surgery. The proposed solution has the potential to provide an additional layer of security while staying in realistic bounds of latency and delay in data transmission.

Keywords — Latency, Reliability, Robot-Surgery, Security, Transport Layer Security, 5G.

I. INTRODUCTION

Robot-assisted surgery has become increasingly popular in recent years, thanks to its ability to provide better patient outcomes and improved precision. However, one of the key challenges facing the field of robot-assisted surgery is the need for high-speed, reliable communication between the surgeon and the surgical robot [1], [2]. This is particularly important for remote surgeries, where the surgeon may be located hundreds or even thousands of miles away from the patient.

The advent of communication networks offers a promising solution to this challenge. We have recently seen a large uptick in robot surgeries carried out over 5G networks which are ideally suited for supporting robot-assisted surgery given the requirements of high speed, low latency and transmission delay.

However, the security of the communication channels between the surgeon's control console and the robotic system is a significant concern that needs to be addressed. Any vulnerability in the authentication process can lead to unauthorized access, which can compromise patient safety and privacy. [3]

In this paper we build on the Transport Layer Security (TLS) protocol which provides a strong foundation for securing the communication over the 5G network channel between the remote surgeon control console and the robotic surgery system. The proposed solution introduces additional security measures, including biometric authentication and multi-factor authentication.

The remainder of the paper is organized as follows. Section II provides an overview of the TLS protocol used in robot-assisted surgery and its limitations. Section III presents the proposed solution and its implementation details. Section IV discusses the methodology of the implementation for the proposed solution. Section V evaluates the performance of the proposed solution through simulation and testing. Section 6 concludes the paper, highlighting the importance of utilizing advanced authentication mechanisms to enhance the security of critical applications such as robot-assisted surgery. Finally, Section VII discusses future work for this research.

II. TLS METHODOLOGY

TLS is a widely used security protocol that provides confidentiality, integrity, and authentication for data communication over the internet. In robot surgery over 5G, TLS can be used to encrypt the data exchanged between the surgical robot and the surgeon's device, which can include sensitive information such as images, video, and control commands. Here is a step-by-step explanation of how TLS would work in robot surgery [4] conducted over a 5G network:

![Fig. 1. Remote Surgery Over 5G.](image-url)
1. The surgical robot and the surgeon's device establish a 5G network connection using the 5G communication protocol.

2. The surgical robot and the surgeon's device negotiate using the TLS handshake protocol designed to establish a secure TLS connection.

3. During the TLS handshake, the surgical robot and the surgeon's device exchange their TLS versions, cipher suites, and other parameters. They also exchange their digital certificates, which contain their public keys.

4. The surgical robot and the surgeon's device verify each other's certificates to ensure that they are valid and issued by a trusted Certificate Authority (CA).

5. Once the certificates are verified, the surgical robot and the surgeon's device use their public keys to exchange a symmetric encryption key. This key is used to encrypt and decrypt the data exchanged between the devices.

6. The surgical robot and the surgeon's device use the symmetric encryption key to encrypt and decrypt the data exchanged between them. This ensures that the data is kept confidential.

7. The surgical robot and the surgeon's device also use the TLS protocol to provide integrity checks. This ensures that the data exchanged between the devices has not been tampered with during transmission.

8. The surgical robot and the surgeon's device continue to exchange data over the TLS connection until the surgery is completed. When the surgery is finished, they terminate the TLS connection.

### A. Drawbacks

TLS has quite a few drawbacks such as high cost of setup and resource requirements. With respect to the security, TLS has major drawbacks that can compromise the privacy of the communication channel [5]. The protection offered is transient in the sense that the information is only protected in the channel but not when transmitted/received by the endpoints. Given that TLS is implemented in the channel there are a wide range of possible security holes at the endpoint. Most notably at the endpoint gateway [6]. Hence, it is not an end to end solution but a point-to-point solution.

This calls for more advanced authentication schemes that will be discussed in the following sections.

### III. PROPOSED SOLUTION

The proposed solution builds upon the existing TLS protocol and introduces additional security measures, including biometric authentication, multi-factor authentication, and digital certificates.

![Fig. 2. TLS procedure for remote surgery authentication.](image)

![Fig. 3. Enhanced security measures for authentication of robot surgery.](image)
The proposed solution consists of the following 3 components:

1. TLS Protocol: The TLS protocol is a security mechanism used to secure communication channels. The proposed solution will be built on the foundation of the TLS protocol.

2. Biometric Authentication: The proposed solution utilizes biometric authentication to verify the identity of the surgeon. Biometric authentication uses physical characteristics, such as fingerprints or facial recognition, to authenticate the user. The proposed solution integrates biometric authentication on top of the TLS protocol to provide an additional layer of security.

3. Multi-factor Authentication (MFA): This solution combines two or more authentication mechanisms, such as biometric authentication and smart card authentication, to provide stronger security.

The implementation of the proposed solution involves the following steps:

1) User enrollment

The user, in this case, the surgeon, is enrolled in the system using simple login without any protection.

2) Authentication

When the surgeon attempts to access the control console, the proposed solution initiates the authentication process. The surgeon inserts their smart card into the card reader and provides their biometric data, which is verified against the stored data base. If the biometric authentication is successful, the proposed solution prompts the surgeon to enter a one-time password generated by the smart card, which provides an additional layer of security.

Once the authentication is secured on both the surgeon and the patient side, the TLS protocol takes effect to secure the communication channel.

The next section will evaluate the performance of the proposed solution through simulation and testing.

IV. ENHANCED METHODOLOGY

Step-by-step procedure for testing the proposed solution under various scenarios:

1. Set up the testing environment with a robotic surgery system and a 5G network.
2. Implement the proposed solution, including the biometric authentication mechanism and multi-factor authentication.
3. Create test scenarios that simulate replay attacks. Here we manually capture the traffic by intercepting it while it's in transit and then replay it later as if it was sent by the surgeon. This type of attack is particularly effective against systems that use weak or no authentication mechanisms [7] and hence used in our experiment.

4. For each test scenario, measure the following parameters:
   a) Authentication time: measure the time taken for the authentication process to complete. This is measured by a programmatic timer that starts and stops around the authentication function event.
   b) Authentication success rate: measure the rate of successful authentications. This is measured by dividing the total number of successful authentication attempts divided by the total number of authentication attempts.
   c) Network latency: measure the delay in network response times. This is measured by the total round trip time of a data packet between the robot surgeon to the remote patient console and back.

5. Below are the tools and software we used for testing the different scenarios based on the literature survey of existing experiments that were carried out.
   - Network simulation software: NS-3 was used to simulate the network environment and test the performance of the proposed solution under different network loads and conditions [8].
   - Attack simulation tools: Metasploit was used to simulate network attacks. Here we use replay attack [9].
   - Biometric sensor testing tools: BioAPI was used to test the accuracy and reliability of the biometric authentication mechanism [10].
   - Smart card testing tools: GlobalPlatform Test Suite was used to test the functionality and operability of the smart card component of the proposed solution [11].
   - The robot surgeon and the patient console are represented as two User Equipments (UEs) in the ns3 simulation tool. There is no concept of ‘distance’ between the robot surgeon UE and the patient console UE.
   - Total number of authentication attempts: 100.
   - TLS: mTLS (micro TLS) module in the ns3 tool.

V. RESULTS AND DISCUSSIONS

The simulation results showed that the proposed solution provides a robust and reliable authentication process that ensures the integrity and confidentiality of the data transmitted between the surgeon’s control console and the robotic system. We also measured the authentication time and authentication success rate using the proposed solution and compared it with the baseline solution that uses only the TLS protocol. The results showed that the proposed solution provides a significant improvement in the authentication success rate which comes at a cost of high authentication time.

From the simulation experiments where no additional security measure was employed, we see we have success rates >98%.

<table>
<thead>
<tr>
<th>Trial #</th>
<th>Authentication Time (ms)</th>
<th>Authentication Success Rate (%)</th>
<th>Latency (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>3.1</td>
<td>98.7</td>
<td>27.8</td>
</tr>
<tr>
<td>2.</td>
<td>4.2</td>
<td>99.1</td>
<td>28.8</td>
</tr>
<tr>
<td>3.</td>
<td>3.3</td>
<td>98.6</td>
<td>30.1</td>
</tr>
</tbody>
</table>

TABLE I: RESULTS WITHOUT ANY ADDITIONAL SECURITY MEASURES

DOI: http://dx.doi.org/10.24018/ejeeng.2023.8.4.3064

Vol 8 | Issue 4 | July 2023 3
VI. CONCLUSION

With added security measures, the authentication time increased in the order of 10x which is still significantly lower than 1s. The overall impact to latency is negligible. This is because the added security measures were outside the communication channel between the robot surgeon and patient console. The latency recorded seems to vary across both sets of results and have no correlation to the authentication mechanism. We believe this is a good improvement to the existing single authentication scheme of the TLS protocol. In conclusion, our proposed solution enhances the security of the authentication process in robot-assisted surgery by utilizing advanced authentication mechanisms with 5G technology. The simulation results showed that the proposed solution provides a robust and reliable authentication process that can effectively prevent security threats such as replay attacks.

VII. FUTURE WORK

The proposed solution has demonstrated the potential to enhance the security of robot-assisted surgery over 5G networks. However, there is still room for further research and improvements in this area. Some possible future work includes:

1. Conducting additional experiments to evaluate the effectiveness of the proposed solution under different scenarios and network conditions. For instance, the solution can be tested under various levels of network congestion or in the presence of different types of attacks to validate its robustness.
2. There was no concept of distance between the robot surgeon and the patient console in our experimentation. Incorporating that would add more validity to the results in terms of replication real world usage.
3. Investigating the impact of the proposed solution on the performance of the system, including latency, throughput, and energy consumption. The solution can be optimized to minimize the impact on system performance while still maintaining a high level of security.
4. Exploring the integration of artificial intelligence and machine learning techniques to enhance the security of the system. For example, machine learning algorithms can be used to detect anomalies in the network traffic and identify potential attacks.

CONFLICT OF INTEREST

Authors declare that they do not have any conflict of interest.

REFERENCES


TABLE II: RESULTS WITH ADDITIONAL SECURITY MEASURES IMPLEMENTED

<table>
<thead>
<tr>
<th>Trial #</th>
<th>Authentication Time (ms)</th>
<th>Authentication Success Rate (%)</th>
<th>Latency (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>301</td>
<td>99.73</td>
<td>29.4</td>
</tr>
<tr>
<td>2</td>
<td>322</td>
<td>99.13</td>
<td>30.8</td>
</tr>
<tr>
<td>3</td>
<td>330</td>
<td>99.84</td>
<td>29.1</td>
</tr>
</tbody>
</table>