N. Mouzakitis[1]
Mathematician, Computer Engineer
Corfu, Greece
email: mzktsn@gmail.com

Enhanced Dynamic ID Generation Scheme with Signal Generation Algorithm for Secure Communication and Prevention of Masquerade and Replay Attacks on CAN Bus

1 Introduction

The Controller Area Network (CAN) Bus is a widely adopted communication protocol in automotive and industrial systems. However, it faces security challenges, such as masquerade and replay attacks, that can compromise the integrity and confidentiality of communication. In this article, we propose an enhanced Dynamic ID Generation (DIDG) scheme with the integration of a Signal Generation Algorithm (SGA) to address these security concerns and facilitate secure communication on the CAN Bus.

2 Dynamic ID Generation Scheme and ID Hopping

The DIDG scheme generates unique 11-bit message identifiers for secure nodes, incorporating fixed upper bits and encrypted lower bits. This scheme facilitates ID hopping between secure nodes, enhancing communication efficiency and minimizing the risk of collision and unauthorized access.

3 Signal Generation Algorithm (SGA) for Trustworthiness

To further enhance the trustworthiness of communication and prevent masquerade and replay attacks, we integrate the Signal Generation Algorithm (SGA). The SGA generates a unique and recognizable signal that secure nodes periodically transmit using the same ID derived from the DIDG scheme. This validation mechanism ensures that nodes have not been impersonated since the last periodic transmission, enhancing trust and preventing unauthorized access.

4 Prevention of Masquerade and Replay Attacks

We present techniques and countermeasures to prevent masquerade and replay attacks on the CAN Bus. These include secure key management, encrypted communication channels, timestamp-based validation, and message authentication protocols. The integration of the DIDG scheme and SGA adds an additional layer of protection against these attacks, ensuring the integrity and authenticity of transmitted data.

5 Implementation Details

We provide detailed guidelines for implementing the enhanced DIDG scheme with SGA, including the generation of encrypted lower bits, key management procedures, integration of the SGA, and deployment considerations. We discuss the necessary cryptographic techniques, algorithms, and protocols to ensure secure and robust communication on the CAN Bus.

6 Performance Evaluation

We evaluate the performance of the enhanced DIDG scheme with SGA in terms of security, efficiency, and resilience against masquerade and replay attacks. The evaluation includes measures such as identifier uniqueness, encryption strength, computational overhead, message transmission latency, prevention of unauthorized access, and detection of replayed messages. The results demonstrate the effectiveness of the scheme in providing secure and reliable communication while preventing masquerade and replay attacks on the CAN Bus.

7 Conclusion

In this article, we have proposed an enhanced Dynamic ID Generation scheme with the integration of a Signal Generation Algorithm for secure communication, prevention of masquerade and replay attacks, and ID hopping between secure nodes on the CAN Bus. The scheme provides robust security mechanisms, enhances trustworthiness, and ensures the integrity and confidentiality of data transmission. The experimental results validate the effectiveness of the scheme in providing secure and reliable communication on the CAN Bus while mitigating the risk of masquerade and replay attacks.

[1]Corresponding Author.
October 27, 2023

List of Figures

List of Tables