Machine Learning-Enhanced Secure Voting-Based Aggregated Signatures Protocol for Authentication and Revocation in 5G-V2X Communication

Shimaa A. Abdel Hakeem [a,b], HyungWon Kim [a*]

[a]School of Electronics Engineering, Chungbuk National University, Korea.

[b]Computers and Systems Department, Electronics Research Institute, Giza, Egypt

shimaakotb@cbnu.ac.kr, hwkim@cbnu.ac.kr*

Abstract

With the rapid advancement of 5G technology and its integration into vehicular communication systems (V2X), ensuring secure and efficient authentication and revocation mechanisms has become critical. This paper presents a novel protocol leveraging voting-based aggregated signatures and machine-learning techniques for authentication, key management, and revocation in 5G-V2X communication. The proposed method enhances security, reduces computational overhead, and ensures reliable vehicular communication.

Ⅰ. Introduction

The evolution of 5G networks has paved the way for advanced vehicular communication systems, known as V2X (Vehicle-to-Everything). These systems require secure and efficient authentication mechanisms to ensure data integrity, confidentiality, and availability. Traditional authentication methods often fail to address the unique challenges posed by 5G-V2X environments, such as high mobility, low latency, and massive device connectivity [1].

Ⅱ. Method

We introduce a secure voting-based aggregated signatures (VBAS) protocol explicitly designed for 5G-V2X communication. This protocol utilizes a voting mechanism where multiple entities collaboratively authenticate a vehicle,

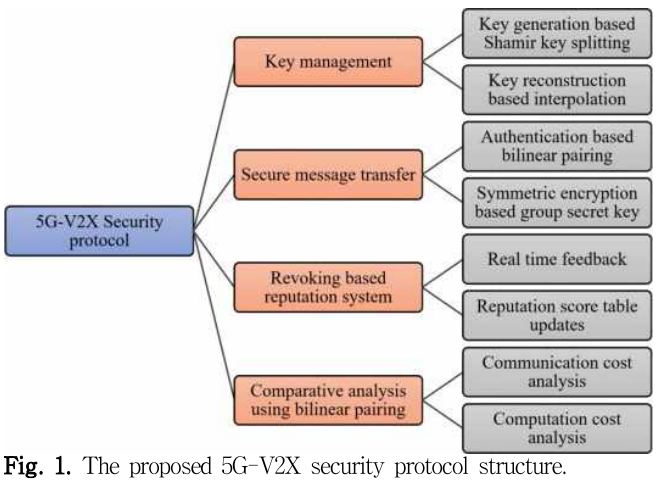

Fig. 1. The proposed 5G-V2X security protocol structure.

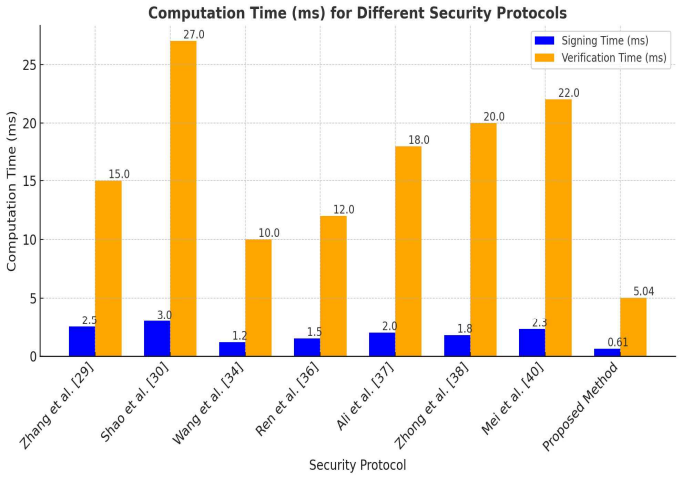

Fig. 2. Computation time (MS) for different security protocols using bilinear pairing security.

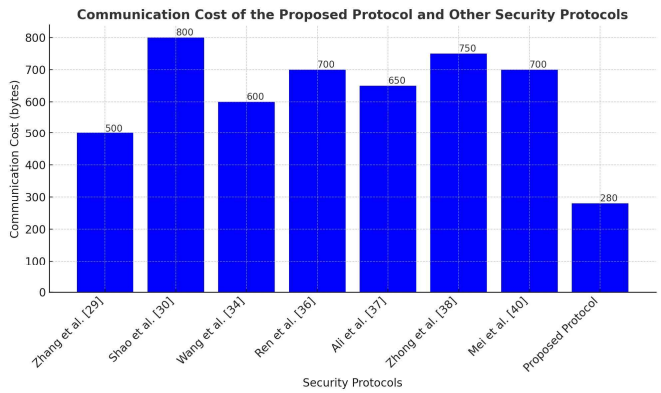

Fig. 3. Communication cost of the proposed protocol and other security protocols using bilinear pairing security.

enhancing security and resilience against attacks. Aggregated signatures reduce the communication overhead and computational load, making the protocol suitable for real-time applications in 5G-V2X scenarios [2-4]. The key features of the protocol are as follows:

Voting-Based Authentication: Multiple trusted entities

participate in the authentication process, ensuring higher security and mitigating the risk of single points of failure.

Aggregated Signatures: Aggregated signatures minimize the communication overhead and computational burden, allowing for efficient authentication even in high-density vehicular environments.

Revocation Mechanism: The protocol includes a robust revocation process to remove compromised or unauthorized vehicles from the network securely.

Scalability: The VBAS protocol is designed to handle the large scale of 5G-V2X networks, supporting many devices with minimal latency.

Ⅲ. Machine Learning Techniques for Key Management

Our protocol incorporates machine learning techniques in the key management system to enhance security and efficiency. These techniques include:

Anomaly Detection: Machine learning algorithms detect anomalies in key usage patterns, helping identify potentially compromised keys and preventing unauthorized access.

Predictive Analysis: Predictive models analyze historical data to forecast key usage trends and optimize key distribution, ensuring efficient and secure key management.

Classification: Machine learning classifiers categorize entities based on their behavior and key usage, enabling more targeted and effective key distribution and revocation strategies.

IV. Key Management Process

Secret Splitting-Based Key Generation: Key generation utilizes a Secret Splitting-based approach, distributing partial keys to vehicles within the same group, ensuring secure future communication.

Secure Key Distribution: Machine learning techniques optimize the distribution of partial keys, ensuring they are securely and efficiently allocated to authorized vehicles.

Dynamic Key Revocation: The revocation process leverages machine learning to detect and report misbehaving entities, ensuring timely revocation of compromised keys.

V. Performance Evaluation

The protocol's performance is evaluated in terms of communication and computation efficiency. Our protocol costs only 280 bytes per message, the lowest among evaluated protocols. It also demonstrates competitive computation efficiency, with a signing time of 0.614 ms per message and a verification time of 5.035 ms per signature. The innovative revocation method ensures timely detection and reporting of misbehaving entities, with an average detection time of 2.3 seconds and an average. The proposed secure voting-based aggregated signatures authentication and revocation protocol, enhanced with machine learning techniques for key management, offers a robust and efficient solution for 5G-V2X communication. By leveraging voting mechanisms, aggregated signatures, and machine learning, the protocol addresses the unique security and performance challenges of 5G vehicular networks, paving the way for safer and more reliable V2X communication revocation time of 1.8 seconds.

ACKNOWLEDGMENT

This Work was supported by Regional Leading Research Center (RLRC) of the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No.2022R1A5A8026986) and supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-01304, Development of Self-Learnable Mobile Recursive Neural Network Processor Technology). It was also supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Communication Technology Research Center support program (IITP-2024-2020-0-01462) supervised by the IITP (Institute or Information & communications Technology Planning & Evaluation).

REFERENCES

[1] Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2020). 5G-V2X: Standardization, architecture, use cases, network-slicing, and edge-computing. Wireless Networks, 26(8), 6015-6041. https://doi.org/10.1007/s11276-020-02264-1

[2] Hakeem, S. A. A., Hussein, H. H., & Kim, H. (2022). Vision and research directions of 6G technologies and applications. Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2022.04.004

[3] Abdel Hakeem, S. A., & Kim, H. (2022). Centralized threshold key generation protocol based on Shamir secret sharing and HMAC authentication. Sensors, 22(1), 331. https://doi.org/10.3390/s22010331