VANET Secure Routing Simulation Using Python

Author: Farah Mae Sumajit

Introduction

Vehicular Ad Hoc Networks (VANETs) are crucial in intelligent transport systems where vehicles communicate wirelessly. However, securing communication in VANETs is a major challenge due to dynamic topologies and vulnerability to attacks like impersonation and replay. This project presents a Python-based simulation using hash functions to ensure message integrity and detect common VANET threats.

Simulation Overview

This project simulates secure routing by implementing SHA-256 hashing on each vehicle's broadcast message. Each vehicle moves randomly and exchanges messages with others. The simulation checks message integrity using individual cryptographic salts and detects impersonation by validating the sender identity against expected hashes.

Security Mechanisms Implemented

- SHA-256 based hashing for integrity

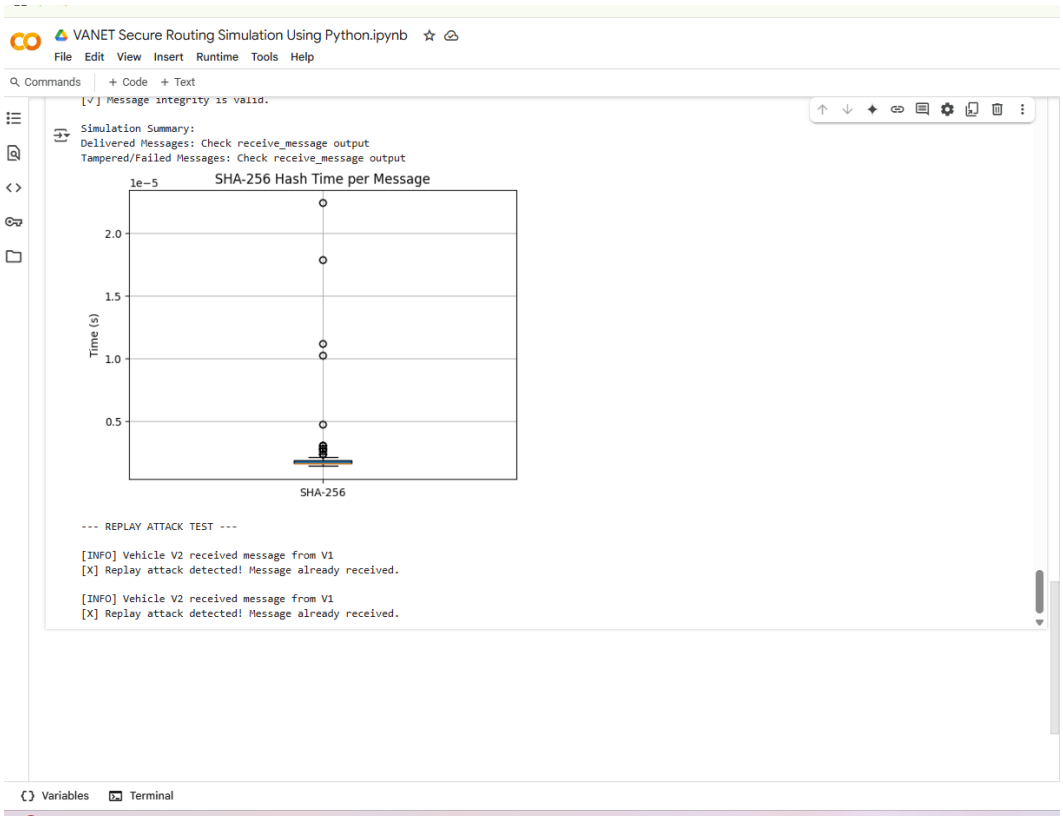
- Sender-specific salts to simulate private keys

- Replay attack detection using message hash memory

- Impersonation detection using mismatched hash validation

Simulation Results

The simulation was executed using Google Colab. The hash time performance was plotted, and replay attack detection worked successfully. Below is a sample output screenshot showing detection of replay attacks:



Conclusion

This simulation successfully demonstrates how message integrity, hashing, and basic sender verification can be used to secure VANET communications. Replay and impersonation attacks were effectively detected using lightweight cryptographic techniques suitable for real-time vehicular networks.