TECHNISCHE UNIVERSITÄT
CHEMNITZ

Fakultät für Informatik
Professur Technische Informatik
Prof. Dr. Dr. h. c. Wolfram Hardt

Master's Thesis Topic (max. 12 words)
Simulation-Based Evaluation of Secure Communication Algorithms with Global Awareness in Game Engine Environments

Keywords (min. 4 words)
Global Awareness, Algorithm evaluation, Autonomous Vehicles Communication, Real-World Scenario Emulation

Introduction

As society's reliance on secure communication escalates within diverse domains such as autonomous vehicles, Internet of Things (IoT), and military applications, the imperative for robust and efficient communication algorithms becomes paramount. This thesis endeavors to conceive, validate, and appraise secure communication algorithms within simulated environments, leveraging specialized tools like game engines such as Carla. The core investigation centers on the integration of global awareness into these algorithms, endowing them with the capacity to dynamically acclimate to intricate and variable network circumstances.

Fig. 1: Car2X Real-time communication

Research Area/State of the Art

The literature review will take a deep dive into the world of secure communication algorithms that are currently in use. This will involve shining a light on both their strong points and the areas where they might fall short. Moreover, the review will venture into the progress made in simulation methods, particularly those involving game engines, which mimic real-life situations. In addition to this, the exploration will touch on the hurdles faced when trying to infuse global understanding into communication algorithms. This will involve considering things like shifts in network layouts, differences in data speeds, and potential threats from adversaries.

Problem Statement

How can secure communication algorithms be designed and integrated with global awareness in a simulated environment, using game engines like Carla, to address the challenges of dynamic network conditions, topology changes, varying data rates, and potential adversaries, ultimately ensuring effective and adaptive secure communication?

Solution approach

The envisaged solution entails formulating and implementing secure communication algorithms augmented with global awareness within a simulated framework. This will be achieved by constructing a comprehensive simulation environment utilizing game engines like Carla, which mimics real-world settings. These algorithms will not only ensure robust data security but will also exhibit the flexibility needed to navigate dynamically evolving network conditions. The crux of the solution lies in integrating a mechanism for global awareness, empowering communication nodes to gather and share real-time network information, encompassing changes in topology, data rates, and potential security threats. Through integration into the simulation environment, the algorithms' performance will be rigorously assessed under diverse conditions, encompassing abrupt network disruptions, fluctuating data rates, and deliberate malicious interventions. The overarching goal of this solution is to establish a proof-of-concept for the secure communication algorithms imbued with global awareness, with the simulation-based appraisal poised to validate their competence in surmounting the challenges presented by dynamic network landscapes while ensuring effective, secure, and adaptive communication.

Criteria for Evaluation

1. Security Assurance Metrics:

    - Data Confidentiality
    - Data Integrity
    - Authentication and Authorization Effectiveness
    - Resistance against Eavesdropping and Attacks

2. Adaptability and Robustness Metrics:

    - Response Time to Network Changes
    - Stability under Varying Network Conditions
    - Ability to Recover from Network Disruptions
    - Resistance against Network Congestion

3. Efficiency Metrics:

    - Computational Overhead
    - Memory Utilization
    - Bandwidth Consumption
    - Processing Time for Communication Tasks

4. Global Awareness Metrics:

    - Accuracy of Shared Network Information
    - Timeliness of Information Sharing
    - Effectiveness of Adaptation Based on Shared Information

5. Communication Performance Metrics:

    - Throughput of Data Transmission
    - Latency in Data Delivery
    - Jitter in Data Transmission

6. Resilience Metrics:

    - Behavior in the Presence of Malicious Adversaries
    - Ability to Detect and Mitigate Attacks
    - Recovery Time after Security Breaches

Expected Results

At the conclusion of this thesis, the expected results encompass the following key outcomes:

1. **Proof-of-Concept Validation:** A validated proof-of-concept showcasing the successful integration of secure communication algorithms with global awareness within a simulated environment using game engines. This substantiates the feasibility of adapting communication algorithms to dynamic network conditions while ensuring data security.
2. **Quantitative Performance Metrics:** A comprehensive set of quantitative metrics, demonstrating the algorithms' performance across various aspects such as security assurance, adaptability, efficiency, and global awareness. This will offer a clear assessment of their efficacy in addressing the defined challenges.
3. **Comparative Analysis:** A comparative analysis against existing secure communication methods that lack global awareness, highlighting the strengths and advantages of the proposed approach. This comparison will underscore the significance of global awareness in enhancing communication algorithms' performance.

Earliest Starting Time
WS23/24

Literature/Links

[1] Ma, L., Yang, S., & Kim, H. (2018). Security and Privacy in Smart Cities: A Review. IEEE Access, 6, 18059-18077.

[2] Wang, Q., Atiquzzaman, M., & Seet, B. (2019). Secure Communication Protocols for Internet of Things: A Survey. IEEE Internet of Things Journal, 6(6), 10001-10020.

[3] C. Team, “CARLA,” CARLA Simulator. https://carla.org/