Secure Authentication Protocol Implementation for V2X Communication: a Simulation Study-Case

Emanuely Poncio do Amaral, Leonardo Passig Horstmann, Antônio Augusto Fröhlich
Software/Hardware Integration Lab, Federal University of Santa Catarina
Florianópolis, Santa Catarina, Brazil
{poncio*, horstmann, guto}@lisha.ufsc.br

***Abstract*—Secure Vehicle-to-Everything (V2X) communication is a key for the development of Intelligent Transportation Systems (ITS). Compromising the sensitive data exchanged by vehicles, pedestrians and the infrastructure can lead to critical safety and privacy risks. Nevertheless, implementing robust security protocols that respect the real-time requirements of such critical applications is challenging due to the significant computational overhead of traditional PKI and the strict latency constraints of safety messages. This work investigates the application of a secure IIoT authentication protocol, proposed in previous work by the group, in the context of V2X communication. The secure protocol is implemented on a V2X simulation environment built over the Artery framework (which integrates OMNeT++ and SUMO) and accounts for vehicles and Roadside Units communication. We evaluated the implementation in a 100-vehicle simulation in terms of latency and jitter, with a mean end-to-end authentication latency of 24.15 ms. The results corroborate the suitability of the secure IIoT protocol implemented here for V2X communication, demonstrating its ability to provide robust security without introducing prohibitive delays.**

***Index Terms*—security, V2X, simulation, protocol**

I. Introduction

Vehicle-to-Everything (V2X) communication is the backbone of Intelligent Transportation Systems (ITS), enabling continuous information exchange among vehicles, infrastructure, pedestrians, and networks. Robust security mechanisms are essential, since sensitive data is transmitted, used for decision-making, and thus has a direct impact on the system's safety. In fact, compromised data can lead to critical road-safety hazards and severe privacy breaches.

Nevertheless, the security mechanisms currently adopted in ITS solutions are largely derived from traditional Internet solutions, such as Public Key Infrastructure [5], which are known to introduce significant authentication delays. This challenge becomes even more complex as vehicles are increasingly interconnected to user devices and other services to promote comfort and improve user experience, opening potential attack vectors from within the vehicle itself.

In the context of safe communication for Industrial Internet of Things (IIoT) scenario, Fröhlich et al. [4] proposed a Secure Gateway solution for IIoT devices. The Secure Gateway acts as a central defense element within the V2X architecture. It functions as an encrypted traffic control and filtering point, validating identities, ensuring message integrity, and protecting against replay, spoofing, and man-in-the-middle attacks. At the same time, it must maintain real-time performance and guarantee interoperability across equipment manufacturers and communication protocols (e.g., IEEE 802.11p, LTE-V2X).

This work was partially supported by FUNDEP grants Rota 2030/Linha VI 29271.02.01/2022.01-00 and 29271.03.01/2023.04-00.

In this work, we implement the IIoT Gateway solution proposed by Fröhlich et al. [4] in a simulated V2X scenario. In the present work, Road-side Units (RSUs) act like the gateway in the architecture proposed by Fröhlich et al. and are responsible for vehicle authentication. Meanwhile, the vehicles are modeled as IIoT devices and are supposed to authenticate to the RSU to obtain the IIoT segment group key, which will allow them to participate in V2X communication. We implemented their protocol in a simulation environment for V2X and vehicle mobility. The evaluation of the protocol on the simulation scenario considered metrics for latency and jitter. Therefore, our main contribution is the assessment of the performance and scalability of the solution proposed by Fröhlich et al. on an automotive simulation scenario.

The remainder of this paper is organized as follows: Section II presents the basic concepts on the IIoT Gateway architecture proposed in [4]. Section III describes the System Model adopted to implement the original IIoT Gateway on a V2X scenario. Section IV describes the simulation environment and tools along with the evaluation metrics. Section V present the results collected in our simulations. Finally, Section VI ends this work with some final remarks.

II. IIoT Gateway Architecture

In this section, we describe our IIoT Secure Gateway Architecture proposed by Frohlich et al. [4]. In their work, the gateway is designed as an edge component between IIoT devices and the Internet. Any interaction between devices in the IIoT segment and the Internet is bridged by it. Furthermore, their architecture encompasses an External Security Agent (ESA) that continuously verifies the integrity of the gateways and gives support to additional security operations, including the authentication process. Finally, devices are Cyber-Physical Systems (CPS) that usually communicate using application-specific low-latency, time-triggered, cross-layer protocols.

In their solution, the authentication between devices and the gateway starts with a human operator responsible for storing the device information in the External Security Agent (ESA), triggering a message to the gateway that informs it of registered, valid IIoT devices and their authentication

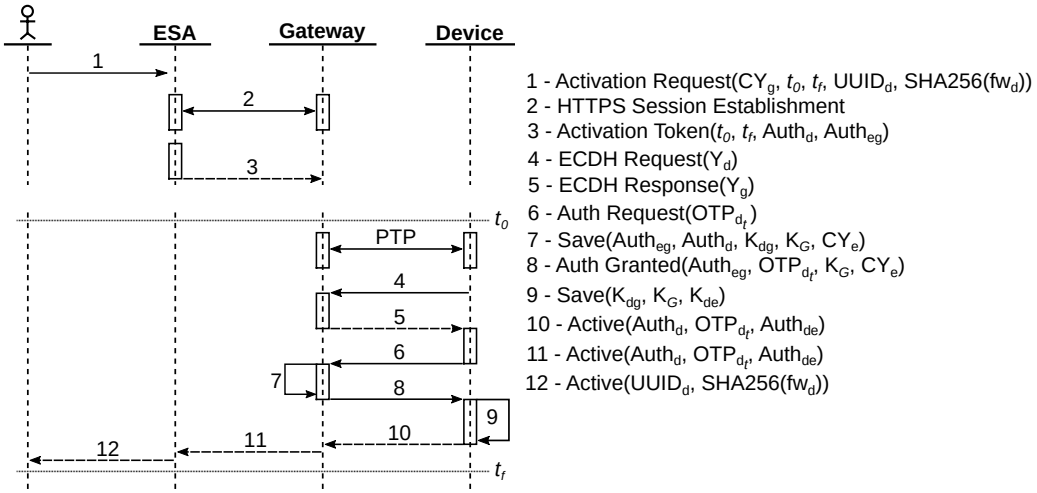

Fig. 1. Secure Bootstraping of IIoT Devices. Source: Fröhlich et al. [4]

window. This validity window (t_0, t_f) is defined by the ESA based on the vehicle's authorized operational schedule. The second part of the authentication process is initiated by the device that makes a PTP (Precision Time Protocol) request and synchronizes its time with the Gateway. . After that, the device and gateway establish a secure channel through Elliptic Curve Diffie-Hellman (ECDH) [9]. The authentication is then conducted using OTP that considers information that was previously provided to the gateway by the ESA. This process allows for verifying the identity of both the device and the gateway, once only valid nodes registered on the ESA would be able to produce such information.

Once devices successfully authenticate to the gateway, both the device and the gateway share a key for direct communication. Furthermore, the gateway also shares the group key for communicating with all local IIoT segment. Whenever a message produced by the device is meant to be exchanged on the IIoT segment, it should use the IIoT group key, guaranteeing that only registered devices can communicate. Finally, the authenticated device sends a confirmation message to the ESA and human operator for further checking on the gateway integrity. Figure 1, extracted from [4], depicts the whole authentication process.

Beyond the secure cryptography algorithms presented in their work, the IIoT Secure Gateway Architecture proposed by Fröhlich et al. [4] leverages a Trusted Execution Environment solution for managing secure operations and handling sensitive information (e.g., keys, plain-text, and variables used for authentication). Other than that, a Gateway Integrity Protocol [8] is envisioned to be adopted for enhancing the ability to verify the gateway's correct behavior. Other than that, their solution also comprises mechanisms for key revocation, gateway replacement, and reboot.

III. System Model

We assume a network model where vehicles and RSUs are devices on a IIoT. In this model each RSU behaves like the gateway modeled by Fröhlich et al. [4] in the sense it authenticates vehicles according to information obtained from an ESA. Meanwhile, vehicles should authenticate to a RSU as soon as they enter its region in order to guarantee access to the RSU services and being able to communicate to nearby vehicles. This section details the network components:

- **ESA**: The External Safety Agent is responsible for holding the information for valid registered vehicles and control admission process by informing the RSUs of trusted vehicles necessary information for network admission.
- **RSU**: Different from the approach described in [4], the admission control in our network model is handled by RSUs whenever vehicles enter their region, which is defined according to the range of its radio. In this sense, RSUs assume the role of a gateway in the IIoT architecture modeled in [4]. Upon receiving the request for authentication from a valid vehicle, a RSU is supposed to authenticate it and provide it with the group key for V2X communication within its respective region and also establish a key for direct communication to the vehicle. Whenever the authentication request comes from an unregistered vehicle, i.e., a vehicle whose id was not provided by a trusted ESA, the RSU should ignore the authentication request.
- **Vehicle**: Vehicles in our network model are equivalent to IIoT devices in [4]. In this way, whenever entering the region of a RSU the vehicle will try to authenticate itself with the RSU. This process begins with a PTP stage followed by establishing a secure channel for communication with ECDH. Once the secure channel is established, the vehicle and RSU authenticate each other using information provided by the ESA. Once authenticated, the vehicle will receive both a key for communicating with the gateway and a group key for group V2X communication.

IV. Evaluation Scenario

The simulation environment adopted for this implementation is built around Artery [12], an open-source vehicular

network simulation framework that integrates the network and traffic simulators Omnet++ [2] and Simulation of Urban MObility (SUMO) [7], with Vanetza, which implements the ETSI Cooperative ITS (C-ITS) protocol suite. In this framework, vehicles exchange Cooperative Awareness Message (CAM) messages, providing a realistic network traffic profile for the protocol to be evaluated. In this section, we describe the configurations and detail the operation of the protocol.

First, security messages are assigned a higher priority. Following the description of the Secure IIoT Protocol in Section II, the vehicle authentication considers time, the public parts of the RSU's certificate, their own certificate, and their firmware and UUID. The simulation environment was specifically configured to isolate the performance of the protocol, focusing solely on authentication and V2V communication latency. Therefore, a single RSU was deployed in the center of the simulated urban grid. Using a single RSU simplifies the mobility model for the evaluation of latency and jitter, as we also ensured that all simulated vehicles remained within the RSU's communication range during the simulation. This methodology allowed the analysis to focus purely on cryptographic and network contention overhead without the need to model dynamic handover procedures or cross-RSU transitions, which were out of the scope for this work.

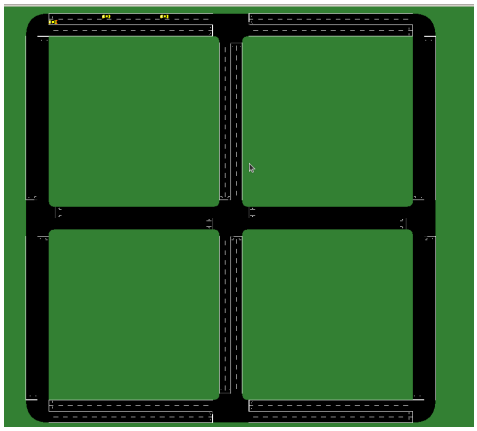

Fig. 2. SUMO network with RSU and devices

As described in Section II and depicted in Figure 1, prior to engaging in secure communication, vehicles must complete a four-phase protocol to obtain authorization. The first phase consists of synchronizing the vehicle's internal clock with the gateway using the Precision Time Protocol (PTP) [1], a crucial step for subsequent cryptographic operations. Following the successful synchronization, the vehicle and RSU perform an ECDH key exchange to derive a shared master secret key, denoted as K_{dh}, and establish a secure channel. This key is subsequently employed to compute a One-Time Password (OTP), depicted as OTP_{d_t} in step 6 of Figure 1. More details on the security algorithms and the process of generating each key and token can be found in [4].

The third phase, Authentication, is initiated when the vehicle sends an Auth Request message to the RSU, with the computed OTP_{d_t} and the synchronized timestamp t (step 6 of Figure 1). After this, the RSU uses the shared secret derived in Phase 2 to compute the expected OTP and compares it with the received value. To validate the process, we used the HMAC-SHA256 [11] implementation from TinyCrypt library [6] to verify the integrity and authenticity of the request.

In case the OTP is successfully validated, the protocol enters the fourth phase, Authorization. Since the RSU functions as the trusted Key Distribution Center in this centralized group key management model, it distributes the symmetric Group Key K_g to the device inside an encrypted AuthGranted message. The Gateway encrypts K_g using AES-128 [10] in Cipher Block Chaining (CBC) mode. The device, upon receiving and decrypting this message, is able to engage in secure Vehicle-to-Vehicle (V2V) communication using K_g.

All subsequent V2V messages are encrypted using AES-128, ensuring confidentiality and integrity within the authorized group. Any authorized recipient vehicle within the group can successfully decrypt and validate the message using the same group key.

The security of the protocol proposed by Fröhlich et al. [4] is reviewed against Dolev-Yao's Threat Model [3]. Nevertheless, the present work validates the implementation of the security aspects by inserting an impostor vehicle in the simulation. This impostor vehicle, not registered with the ESA, will attempt to perform the authentication protocol and to communicate with nearby vehicles.

Finally, the evaluation of the protocol considered metrics for performance and security that were captured in the simulation to fully assess the protocol's suitability for safety-critical Intelligent Transportation Systems (ITS).

Performance Metrics include:

- **Authentication Latency**: The end-to-end time required for a vehicle to complete the four-phase protocol (PTP to authorization).
- **Group Key Distribution Latency**: The time taken for the Gateway to distribute the symmetric Group Key.
- **V2V Message Latency**: The time taken for the Gateway to distribute the symmetric Group Key.
- **Packet Delivery Ratio:** : The end-to-end time required for a vehicle to complete the four-phase protocol (PTP to authorization).

Security Metrics include:

- **Security Validation:**: General assessment of the protocol's access control efficacy.

V. Results

This section presents the results obtained from the simulation scenarios detailed in the previous Section. The analysis is twofold: first, we verify whether the RSU was able to guarantee only registered vehicles would be able to authenticate; second, we conduct a performance evaluation considering metrics like latency and jitter in order to extract insights on the protocol scalability.

The security validation scenario confirmed the protocol's effectiveness in enforcing access control. The experiment,

TABLE I
STATISTICAL SUMMARY OF LATENCY METRICS FOR THE 100-VEHICLE SCENARIO

Metric	Mean (ms)	Std. Dev. (ms)	Min (ms)	Max (ms)	Samples
Authentication Latency	24.15	4.58	18.92	35.41	100
Group Key Latency	1.85	0.62	0.98	3.12	100
V2V Latency	25.73	8.15	15.45	42.88	N/A
ECDH Latency	0.152	0.02	0.11	0.21	100
OTP Latency	0.004	0.001	0.003	0.009	100
AES Encrypt Latency	0.006	0.002	0.004	0.011	N/A
AES Decrypt Latency	0.008	0.002	0.005	0.014	N/A

conducted with two legitimate vehicles and one impostor, demonstrated that the two legitimate vehicles successfully completed the full authentication process and received the group key for V2V communication. Nevertheless, the impostor was consistently rejected by the RSU, as its identifier was not present in the list of trusted vehicles provided by the ESA

To evaluate scalability, one scenario, featuring 100 vehicles, was executed to measure the performance overhead of the RSU. Seven latency metrics were collected for each successful authentication and V2V message exchange. The aggregated statistical results are summarized in Table I.

The mean end-to-end authentication latency was found to be 24.15ms. This result indicates that the secure protocol does, in fact, not introduce prohibitive delays. The latency of the final authorization stage, averaging 1.85ms, further demonstrates the high responsiveness of the Gateway when processing valid authentication requests The total latency for a secure V2V message, which encompasses all cryptographic and network delays, averaged 25.73ms. The low values corroborate the protocol's suitability for exchanging time-sensitive safety messages, such as collision warnings or dangerous location alerts, where the timely and secure delivery of information is necessary. Furthermore, the analysis of the computational overhead metrics reveals the efficiency of the chosen cryptographic primitives. The results show that the cryptographic operations themselves contribute only a small fraction of the total end-to-end latency, with average values in the sub-millisecond range.

VI. FINAL REMARKS

This work presented an implementation of the secure IIoT Gateway protocol proposed by Fröhlich et al. [4] in a simulated V2X scenario. In the present work, we modeled RSUs to handle the authentication process managed by the gateways in the architecture proposed by Fröhlich et al., and the vehicles were modeled as IIoT devices.

We evaluated the implementation on a simulation setup including network simulation tools like Artery [12], Veins, and OMNet++, and mobility simulation with SUMO. The evaluation considered latency and jitter and indicates the suitability of the proposed solution for V2X applications.

While the protocol demonstrated good performance in the 100-vehicle scenario, it is important to consider scalability implications as the number of connected vehicles increases, a factor that can deteriorate both the channel and the RSU performance. But the present simulation did not evaluate maximum stress conditions (i.e., testing the maximum number of vehicles that may connect concurrently).

In addition, it should be noted that the simulated vehicle routes in this study were intentionally kept simple. This design choice ensured that all vehicles remained within the coverage area of a single RSU, therefore isolating the analysis to authentication and V2V latency. However, in more complex mobility patterns or in larger urban scenarios, vehicles may move out of the RSU's communication range. Since the scope of this work was not to investigate RSU handover mechanisms, route variations, and cross-RSU transitions were not modeled. Future work should therefore extend the analysis to scenarios involving multiple RSUs and dynamic handover procedures, as these factors will directly influence latency, reliability, and scalability in practical deployments.

REFERENCES

[1] IEEE standard for a precision clock synchronization protocol for networked measurement and control systems.

[2] Daniel J. Bernstein. An overview of the omnet++ simulation environment. pages 32–49, Paris, France, march 2008.

[3] D. Dolev and A. C. Yao. On the security of public key protocols. In *22nd Annual Symposium on Foundations of Computer Science (sfcs 1981)*, pages 350–357. IEEE, October 1981.

[4] Antônio Augusto Fröhlich, Leonardo Passig Horstmann, and José Luis Conradi Hoffmann. A secure iiot gateway architecture based on trusted execution environments. *Journal of Network and Systems Management*, 31(2), February 2023.

[5] Farah Haidar, Arnaud Kaiser, and Brigitte Lonc. On the performance evaluation of vehicular pki protocol for v2x communications security. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, page 1–5. IEEE, September 2017.

[6] Intel Corporation. TinyCrypt Cryptographic Library. Accessed November 21, 2025.

[7] Pablo Alvarez Lopez, Evamarie Wiessner, Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, Yun-Pang Flotterod, Robert Hilbrich, Leonhard Lucken, Johannes Rummel, and Peter Wagner. Microscopic traffic simulation using sumo. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, page 2575–2582. IEEE, November 2018.

[8] Mateus Lucena, Roberto Milton Scheffel, and Antônio Augusto Fröhlich. Iot gateway integrity checking protocol. In *2019 IX Brazilian Symposium on Computing Systems Engineering (SBESC)*, pages 1–8, 2019.

[9] NSA. The case for elliptic curve cryptography, January 2009.

[10] National Institute of Standards and Technology. Advanced encryption standard (AES), November 2001.

[11] National Institute of Standards and Technology. Secure hash standard, July 2015.

[12] Raphael Riebl, Christina Obermaier, and Hendrik-Jörn Günther. *Artery: Large Scale Simulation Environment for ITS Applications*, page 365–406. Springer International Publishing, 2019.