2023 IEEE Conference on Standards for Communications and Networking (CSCN) | 979-8-3503-9538-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSCN60443.2023.10453140

A 5G-based Authentication Framework for V2X Communication

Diana Magalhães*, Vinicius C. Ferreira* (IEEE Member), Nelson Rodrigues*, João M. Fernandes†
*DTx - Digital Transformation CoLAB, Guimarães, Portugal
† Departamento de Informática, Centro ALGORITMI Universidade do Minho, Braga, Portugal
E-mail: {diana.magalhaes, vinicius.ferreira, ricardo.rodrigues}@dtx-colab.pt, jmf@di.uminho.pt

***Abstract*—The integration of Vehicle-to-everything (V2X) communication and Intelligent Transportation Systems (ITS) promises to revolutionize smart mobility. However, this technological advancement also exposes V2X networks to cybersecurity threats. To address these challenges, this work explores the critical security requirements for V2X communications, including User Equipment (UE) authorization, data integrity protection, and privacy support.**

***Index Terms*—V2X communication, 5G authentication, AKMA**

I. Introduction

Vehicle-to-everything (V2X) and Intelligent Transportation System (ITS) are driving the smart mobility revolution. ITS aims to reduce accidents, pollution, and congestion, ensuring timely services [1]. V2X establishes various critical connections, enhancing road safety, traffic flow, and real-time information sharing, ultimately improving urban life quality [2]. However, this ubiquitous connectivity also poses security challenges, with connected vehicles susceptible to cyber threats [2]. In this context, the security requirements for V2X communications, as outlined in [3], include UE authorization, integrity protection, and pseudonymity and privacy support. We propose the usage of 5G delegated authentication system to improve the security in V2X communications.

II. Authentication for V2X devices

Connected vehicle manufacturers are producing cellular-enabled vehicles, with embedded universal integrated circuit card (eUICC)[1]. It permits Communication Service Providers (CSPs) to provision embeded Subscriber Identity Module (eSIM) and create connectivity and subscriptions management needed within the automotive industry.

ITSs and other infotainment service providers in need of a secure channel with the vehicle can use the CSP as an identity Providers and delegate authentication systems. Authentication and key management for applications (AKMA) [4] is the new cellular-network-based delegated authentication system of 5G that enables Application Functions (AF) to request the user's Home Network (HN) to derive session keys.

After a 5G primary authentication, an AKMA Key ($\mathrm{K_{AKMA}}$) and its identifier (A-KID) are generated in the Vehicle and HN. When a vehicle wants to start a new session with a third-party application, it computes a session key, derived from its $\mathrm{K_{AKMA}}$ and the third-party ID (AF-ID). It requests a session, sending its A-KID to the third-party, represented as an AF. The AF requests the vehicle's HN to derive the session key, sending the vehicle's A-KID and its AF-ID. The HN computes the same session key, and sends it to the AF, that can start a secure session with the vehicle.

III. Discussion and Conclusion

The use of AKMA in V2X scenarios leverages the existing identity and authentication infrastructure deployed by mobile operators, allowing vehicles to achieve end-to-end secure sessions and benefit from strong 5G authentication. This study delves into vital security concerns at the intersection of V2X communications and Intelligent Transportation Systems. Our proposal focuses on using the 5G delegated authentication system, AKMA, to strengthen the security framework for V2X communications. This approach encompasses UE authorization, data integrity, and privacy support, positioning our work to contribute to international projects, adapting mechanisms for dynamic urban environments due to the global nature of V2X security.

References

[1] T. Garg and G. Kaur, "A systematic review on intelligent transport systems," *Journal of Computational and Cognitive Engineering*, vol. 2, no. 3, pp. 175–188, 2023.

[2] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," *Computer Networks*, vol. 169, p. 107093, 2020.

[3] TSGS, "Ts 122 185 - v17.0.0 - lte; service requirements for v2x services (3gpp ts 22.185 version 17.0.0 release 17)," 2022. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[4] M. Khan, P. Ginzboorg, and V. Niemi, "Akma: delegated authentication system of 5g," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 56–61, 2021.

[1] https://trustedconnectivityalliance.org/wp-content/uploads/2020/01/eUICC-for-Connected-cars_FINAL.pdf

979-8-3503-9538-9/23/$31.00 ©2023 IEEE