Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks

Mustafa A. Al Sibahee, Vincent Omollo Nyangaresi, Zaid Ameen Abduljabbar, Chengwen Luo, Jin Zhang, and Junchao Ma, *Member, IEEE*

***Abstract*—Internet of Vehicles (IoV) has greatly improved safety and quality of services in intelligent transportation system (ITS). However, the deployed dedicated short-range communication (DSRC) protocol broadcasts messages after every 100–300 ms. This presents some challenges in message validation within this short duration. As such, most of the current authentication schemes which incur heavy computation and communication overheads are not suitable in this environment. In this article, an efficient authentication scheme is presented based on lightweight cryptographic primitives, such as collision-resistant one-way hashing functions and exclusive OR (XOR) operations. In our protocol, two-factor authentication is attained using physically unclonable function (PUF) generated identities and random nonces, as well as passwords. Extensive formal security verification using the Real or Random (RoR) model shows that it is provably secure. In addition, elaborate semantic security analysis shows that it offers anonymity, untraceability, and key secrecy as well as resilience against numerous IoV attack vectors. In terms of performance, comparative evaluations demonstrate that it reduces computation and energy consumptions by 42.31%. Moreover, it increases the supported security features by 26.67%.**

***Index Terms*—Authentication, Internet of Vehicle (IoV), key agreement, performance, privacy, security, vehicular ad hoc networks (VANETs).**

I. Introduction

THE RECENT past has seen the rise in the development of intelligent transportation system (ITS) for efficient traffic management. The continued need to improve the Quality of Service (QoS) in ITS has led to the development of Internet of Vehicles (IoV). Basically, IoV amalgamates Internet of Things (IoT) and vehicular ad hoc networks (VANETs) to offer homogeneous communication, such as vehicle-to-roadside (V2R) units and vehicle to vehicle (V2V), as well as heterogeneous communication, such as vehicle to cloud (V2C) and vehicle to sensors (V2S) [1]. In an ITS environment, VANETs deploy ad hoc wireless communication technologies to offer safety and comfort to passengers and drivers. This enhances efficiency in road traffic management systems. To facilitate this, onboard units (OBUs) are installed in each vehicle so as to exchange messages with other vehicles, operators, and roadside units (RSUs). This communication is accomplished via the deployed dedicated short-range communication (DSRC) protocol. According to [2], the design of a typical VANET architecture involves a minimal range of networks that are characterized by limited computation and communication abilities. The VANETs' dynamic network topology renders them inadequate in the provision of stable and uninterrupted services. Therefore, IoV have been introduced to make VANETs smarter as well as provide safety and convenience during the communication process. This effectively enhances driving comfort, safety, and real-time road traffic management.

Due to their ability to process high volumes of data during the interaction among vehicles and other entities, IoV have been deployed in numerous novel intelligent areas such as smart cities and ITS to offer information services and intelligent control [3]. As explained in [4], multiple moving vehicles in IoV may communicate with other associated edge facilities to collaborate and share data. This helps them acquire vital information such as their own driving status and real-time traffic situations. The low-cost data sharing and flexible networking has rendered IoV a core component in ITS, which improves driving experience and traffic safety in the face of rapid developments in communication and computation technologies [5], [6]. As vehicles continue being more autonomous and intelligent, IoV have become interconnected infrastructures that facilitate vehicle information and resource exchange among pedestrians, RSUs, and vehicles [7].

In spite of the convenience and traffic management improvements occasioned by IoV, numerous issues remain unresolved in this environment. For instance, open wireless public channels are deployed for wireless access in vehicular environment (WAVE) and DSRC protocols to exchange messages between vehicles and other IoV components. As such, malicious nodes

Manuscript received 3 September 2023; revised 13 November 2023; accepted 4 December 2023. Date of publication 7 December 2023; date of current version 9 April 2024. This work was supported in part by the National Key R&D Program of China under Grant 2023YFB4704900, and in part by NSFC under Grant 61972263. *(Corresponding author: Chengwen Luo.)*

Mustafa A. Al Sibahee is with the National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen 518060, China, and also with the Computer Technology Engineering Department, Iraq University College, Basrah 61004, Iraq (e-mail: mustafaalsibahee@szu.edu.cn).

Vincent Omollo Nyangaresi is with the Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya (e-mail: vnyangaresi@jooust.ac.ke).

Zaid Ameen Abduljabbar is with the Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq (e-mail: zaid.ameen@uobasrah.edu.iq).

Chengwen Luo and Jin Zhang are with the National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen 518060, China (e-mail: chengwen@szu.edu.cn; jin.zhang@szu.edu.cn).

Junchao Ma is with the College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China (e-mail: majunchao@sztu.edu.cn).

Digital Object Identifier 10.1109/JIOT.2023.3340259