Chapter 16
SEBAKE-6G Secure Batch Authentication and Key Exchange for 6G-Enabled ITS

Praneetha Surapaneni
https://orcid.org/0000-0003-3822-7270
SRM University, India

Sailaja Chigurupati
https://orcid.org/0009-0009-5253-5799
KL University, India

Sriramulu Bojjagani
https://orcid.org/0000-0002-8801-4292
SRM University, India

ABSTRACT

As the cyber theft is increases, information safety and confidentiality are the major issues in wireless communications. 6G technology overcomes these difficulties to build a secured intelligent transportation system (ITS). Conventional transportation system faces high computation cost when road side unit (RSU) process each authentication vehicle request. In this chapter, to address this issue we introduced batch authentication and key exchange to secure user privacy and prevent attacks. To ensure message integrity, this system provides location-based information safely from RSU to vehicle without any changes. This system reduces the communication and computational costs. Simulation is performed using simulation of urban mobility (SUMO) simulator.

DOI: 10.4018/979-8-3693-8029-1.ch016

INTRODUCTION

VANETs are expected to be a fortunate technological advancement that will enhance the driving effectiveness and safety of roadway transportation systems as intelligent transportation systems advance (Al-Heety et al., 2020). Since all vehicles in VANETs have an on-board unit (OBU) which permits them to lialise with dispersed RSUs and other intelligent vehicles, all vehicles are regarded as intelligent vehicles (Tan and Chung., 2021).

The 6G era leverages widely available mobile broadband to improve network capacity in order to enable infotainment services and deliver high-quality OBU communications. Intelligent vehicles have the ability to broadcast information about traffic conditions and road conditions, such as accidents and congestion, to surrounding vehicles (Guerrero-Ibanez et al., 2018). This way, any receiver car that is nearby may become more aware of the driving conditions and adjust their route as needed. Likewise, upon entering their coverage territory, the RSUs disseminated location-based alerts to all VANET users (Tan and Chung., 2021). It is required for all VANET consumers and RSUs to enrol with the trusted authority (TA) using their authentic login credentials. The information shared via the VANET should be protected from different security threats by the suggested security services since V2V and V2R connections are conducted wirelessly (Vasudev et al., 2020). Because vehicles in VANETs move at the fastest possible speeds, 6G supports a mobility rate of 1000 km/h, while 5G only supports 500 km/h (Jiang et al., 2021).

As VANETs have grown, other new risks, such as privacy and security issues, have also emerged. Before using value-added services on VANETs, safe communication with regard to authentication, integrity, and secrecy must essentially be ensured. Furthermore, protecting user privacy with regard to location and identification is crucial (Zhang et al., 2022). Even though a number of authentication-based solutions have been created to deal with these problems, alot of them are limited to area-based services and do not apply to value-added services. It's obvious that appealing infotainment services have a big impact on users' capacity to engage in active VANET participation. Furthermore, it seems like there is not much time required for V2V and V2I communications given that the speed range of vehicles in VANET is 60 - 160 kilometres/hour (Guerrero-Ibanez et al., 2013). According to the DSRC standard, a vehicle sends location-based signals to the RSU and other adjacent vehicles every 150–300 ms, this means that if there are 200 or more vehicles in the RSU's coverage area, an RSU must confirm around 650 location-based messages (Ansari., 2021). The anticipated 6G data throughput is 1Gbps, which is very compatible with infotainment services on high-mobility 5G networks (Imoize et al., 2021). Consequently, a high-level computational load on RSUs should result from the individual verification of location-based signals. Once more, in the event