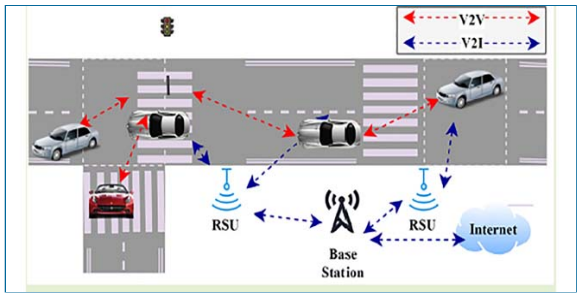
Authors' Reply

Publisher: IEEE

Cite This PDF

Tarak Nandy ; Mohd Yamani Idna Idris ; Rafidah Md Noor ; Ainuddin Wahid A… **All Authors**

Downl PDF



Abstract: Communication in vehicular ad hoc networks (VANETs) is significantly increased due to several services such as location-based service (LBS), traffic management, road safe... **View more**

▸ **Metadata**

Communication in vehicular ad hoc networks (VANETs) is significantly increased due to several services such as location-based service (LBS), traffic management, road safety, and vehicle privacy. Authentication is one of the

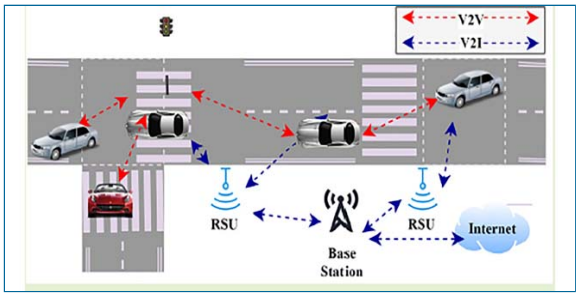
backbones for communication in the vehicular network to protect the whole system, and guarantee the unforgeability and effectiveness of various services. On this note, in the above article, Nandy *et al.* (2021) recently proposed a secure, privacy-preserving, and lightweight authentication scheme for VANET. Recently, Chaudhry (2022) comments on Nandy *et al.*'s article, discussing the private-public key pair, clogging attack, and the pseudo-identity uses. This note addresses the raised comment by the aforesaid author. Furthermore, the detailed clarification against all comments is discussed with the purpose of producing a clear understanding.

Published in: IEEE Sensors Journal (Volume: 22 , Issue: 13, 01 July 2022)

Page(s): 13767 - 13768 **DOI:** 10.1109/JSEN.2022.3175591

Date of Publication: 01 July 2022 **Publisher:** IEEE

ISSN Information:



Hide Full Abstract

Contents

The vehicular ad-hoc network acquires extensive attention from academics, industry, and research in recent decades. The interest in developing the security features in the VANET is outstanding. Every vehicle is equipped with an onboard unit (OBU), safe in a tampered proof device (TPD), to communicate to other vehicles via vehicle-to-vehicle (V2V) connections or other components such as roadside unit (RSU) through the vehicle-to-infrastructure (V2I) communication. On this note, a large-scale decentralized network can be formed and utilize dedicated short-range communication (DSRC) [3] to facilitate reliable communication and attain the characteristics of a mobile ad hoc network. The effectiveness of the VANET can be calculated based on road safety, security, vehicle navigation, and

communication patterns, the vehicular network is prone to malicious attacks [4]. On the other hand, information related to the vehicle such as vehicle ID, driver name, contact details, and

license plate [5]. Therefore, the research on the security and privacy of the vehicular network increased rapidly [6].

Authors

References

Keywords