Secured VANET Protocol with signature authentication (SVPSA)

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 182

Number 24

Year of Publication: 2018

Authors:

Sonia Lal, Anshika Goyal

10.5120/ijca2018917904

Abstract

Vehicular Area Network (VANET) plays an important role in today’s demand of smart roads where the traffic needs to be monitored for safe commuting along with it, the commuters should also be given facilities in case of an emergency or otherwise. Keeping in mind the challenging requirements of the present and the future, in this paper work first previous solutions were reviewed and a new Secured Protocol for VANET with Signature Verification has been proposed. Modified Hill cipher and RSA algorithms are used in sequence to secure the Vehicle’s information transmitted to the Road Side Unit (RSU). Signature verification has been taken care of using Baker’s map. MD5 hashing has been also used to ascertain that there was no intrusion. The device in the vehicle and the RSU communicates only when the signatures are verified. A comparative analysis has also been presented where it has been observed that the proposed algorithm performs better than simple RSA algorithm. The results obtained shows an improvement in Bandwidth by 16%, energy consumed is reduced by 14% and time reduced by 5%. The results indicate that the proposed method not only secures the privacy of the commuters but also uses lesser resources. It can be concluded that the proposed three tier
secured structure is more robust than the existing models.

References

6. Park, S., "Defense against sybil attack in vehicular ad hoc network based on roadside unit support", 2009, IEEE, MILCOM.
18. Bariah L., Shehada D., Salaha E., “Recent advances in VANET security: a survey”, 2015, 10.1109/VTCFall.2015.739111

23. Shikha Mathur, "Analysis & design of enhanced RSA algorithm to improve the security", 2017, ICCT 17029536

Index Terms

Computer Science  Security

Keywords

VANET, RSU, RSA, MD5, Hill Cipher, Signature verification