Azees Maria

Efficient Anonymous Authentication and Key Management Techniques for Vehicular Ad-hoc Networks

Anchor Academic Publishing

disseminate knowledge

Bibliographic information published by the German National Library:

The German National Library lists this publication in the National Bibliography; detailed bibliographic data are available on the Internet at http://dnb.dnb.de .

ISBN: 9783960676805

Azees Maria

Efficient Anonymous Authentication and Key Management Techniques for Vehicular Ad-hoc Networks

Anchor Academic Publishing

Azees Maria

Efficient Anonymous Authentication and Key Management Techniques for Vehicular Ad-hoc Networks

Anchor Academic Publishing

disseminate knowledge

Maria, Azees: Efficient Anonymous Authentication and Key Management Techniques for Vehicular Ad-hoc Networks, Hamburg, Anchor Academic Publishing 2017

PDF-eBook-ISBN: 978-3-96067-680-5
Druck/Herstellung: Anchor Academic Publishing, Hamburg, 2017

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographical Information of the German National Library:
The German National Library lists this publication in the German National Bibliography. Detailed bibliographic data can be found at: http://dnb.d-nb.de

ABSTRACT

The Vehicular ad hoc network (VANET) is an important communication paradigm in modern-day transport system for exchanging live messages regarding traffic congestion, weather conditions, road conditions, and targeted location-based advertisements to improve the driving comfort. In such environments, authentication and privacy are two important challenges needed to be addressed.

There are many existing works to provide authentication and privacy in VANETs. However, most of the existing authentication schemes are suffered from high computational cost during authentication and high communicational cost during secure key distribution to a group of vehicles. Moreover, in many existing schemes, there is no conditional tracking mechanism is available to revoke the misbehaving vehicles from the VANET system. In order to overcome these issues, four new approaches have been developed in this research work.

Firstly, a dual authentication scheme is developed to provide a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANET. Moreover, a dual group key management scheme is developed to efficiently distribute a group key to a group of users and to update such group keys during the users' join and leave operations. The major advantage of the proposed dual key management is that adding/revoking users in the VANET group can be performed in a computationally efficient manner by updating a small amount of information. The results of the proposed dual authentication and key management scheme are computationally efficient compared with all other existing schemes discussed in literature, and the results are promising.

Secondly, in order to preserve the privacy of vehicle users, a computationally efficient privacy preserving anonymous authentication scheme (CPAV) is developed to anonymously authenticate the vehicle users based on the use of anonymous certificates and signatures. Even though there were many existing schemes to provide anonymous authentication based on anonymous certificates and signatures in VANETs, the existing schemes suffer from high computation cost in the certificate revocation list (CRL) checking process and in the certificate and the signature verification process. Therefore, a computationally efficient anonymous mutual authentication mechanism is proposed in this research work to preserve the privacy of the vehicle users and to guarantee the integrity of the transmitted messages. Moreover, a conditional tracking mechanism is introduced to trace the real identity of vehicles and revoke them from VANET in the case of dispute.

Thirdly, an efficient anonymous authentication scheme to preserve the privacy of RSUs is proposed in this research work. In this research work, each authenticated vehicle is required to authenticate the RSUs in an anonymous manner, before communicating with it. Because, each RSU provides the location based safety information (LBSI) to all authenticated vehicles when they are entered into its region. By doing this, each RSU provides the knowledge to vehicle users about the obstacles within its coverage area.

Finally, a computationally efficient group key distribution (CEKD) scheme for secure group communication is proposed in this research work based on bilinear pairing. In VANETs, secure and reliable group communication is an energetic area of research. Today, the most important research challenge is an efficient group key distribution for a secure group communication. Even though there are many group key distribution protocols, they have the security and performance weakness. The proposed CEKD

scheme provides better performance in comparison with most of the previously proposed key distribution schemes in terms of computation cost and hence it is suitable for secure group communication in VANETs.

ACKNOWLEGDEMENT

I, with great pleasure would like to express my heartfelt thanks to my esteemed research supervisor **Dr. P. Vijayakumar**, Assistant Professor, University College of Engineering Tindivanam, Tindivanam, for his persistent help, continued drive and timely motivation which has made this work possible. His illuminating comments and genuine suggestions enabled me to carry out this work fruitfully.

I am very much grateful to **Dr.D.Loganathan**, Professor, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, and to **Dr.K.Kulothungan**, Assistant Professor, Department of Information Sciences and Technology, CEG Campus, Anna University, Chennai, for acting as the doctoral committee members and to provide their valuable suggestions and encouragements throughout the period of my research.

I sincerely express my great sense of gratitude to **Dr. L. Jegatha Deborah**, Assistant Professor and Head i/c, Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam for the support rendered to me at all the stages of my research.

The whole task of acknowledging seems to be incomplete if I don't owe my indebtedness and gratitude to my parents **Mr. V. Maria John Francis** and **Mrs. G. Martinammal** and my brother **Mr. M. Abeens** for their invaluable moral support at every stage of my progress in this research work. Not to mention, my family is the greatest strength behind all my endeavors. Above all, I thank **God, the Almighty** for having blessed me with all physical and mental strength in executing my will successfully.

AZEES M

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.