

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> .

This book is copyright material and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the publishers, as allowed under the terms and conditions under which it was purchased or as strictly permitted by applicable copyright law. Any unauthorized distribution or use of this text may be a direct infringement of the author s and publisher s rights and those responsible may be liable in law accordingly.

Copyright © 2017 Diplomica Verlag GmbH
ISBN: 9783960676805

Azees Maria

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

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>

All rights reserved. This publication may not be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Bearbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und die Diplomica Verlag GmbH, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Alle Rechte vorbehalten

© Anchor Academic Publishing, Imprint der Diplomica Verlag GmbH
Hermannstal 119k, 22119 Hamburg
<http://www.diplomica-verlag.de>, Hamburg 2017
Printed in Germany

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.

ACKNOWLEDGEMENT

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.
	ABSTRACT	i
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF SYMBOLS AND ABBREVIATIONS	xii
1	INTRODUCTION	1
1.1	VANET OVERVIEW	2
1.1.1	VANET System Model	2
1.1.2	Dedicated Short Range Communication (DSRC)	5
1.1.3	VANET Characteristics	6
1.2	SECURITY ISSUES IN VANET	7
1.3	PROPOSED WORKS	9
1.4	OBJECTIVES OF THE RESEARCH WORK	10
1.5	ASSUMPTIONS	11
1.6	ORGANIZATION OF THE THESIS	11
2	LITERATURE SURVEY	13
2.1	INTRODUCTION	13
2.2	SECURITY SERVICES OF VANETS	13
2.3	AVAILABILITY IN VANETS	14
2.3.1	Threats and Attacks on Availability	15
2.3.2	Works on Availability	17
2.4	CONFIDENTIALITY IN VANETS	18
2.4.1	Threats and Attacks on Confidentiality	19

CHAPTER NO.	TITLE	PAGE NO.
	2.4.2 Works on Confidentiality	20
2.5	AUTHENTICATION IN VANETS	21
	2.5.1 Threats and Attacks on Authentication	21
	2.5.2 Requirements for Authentication	23
	2.5.3 Works on Authentication with Privacy Preservation	24
	2.5.4 Computational Cost for Various Authentication Schemes	32
2.6	DATA INTEGRITY IN VANETS	34
	2.6.1 Threats and Attacks on Data Integrity	34
	2.6.2 Works on Data Integrity	36
2.7	NON-REPUDIATION IN VANETS	37
	2.7.1 Attack on Non-repudiation	37
	2.7.2 Works on Non-repudiation	37
2.8	COUNTER MEASURES ON VARIOUS SECURITY ATTACKS	38
2.9	WORKS ON KEY MANAGEMENT	41
2.10	LITERATURE SURVEY GAPS	42
2.11	PROPOSED WORK	43
2.12	CONCLUSIONS	43
3	SYSTEM ARCHITECTURE	45
4	DUAL AUTHENTICATION AND DUAL KEY MANAGEMENT FOR GROUP COMMUNICATION	48
	4.1 INTRODUCTION	48
	4.2 PROPOSED DUAL AUTHENTICATION TECHNIQUE	50

CHAPTER NO.	TITLE	PAGE NO.
4.2.1	Registration through Offline Mode	52
4.2.2	Vehicle's Authentication Process	53
4.2.3	Trusted Authority's Authentication Process and the Provision of Authentication Code (AC)	54
4.3	PROPOSED DUAL KEY MANAGEMENT FOR GROUP COMMUNICATION	58
4.3.1	TA Initial Set up	60
4.3.2	Group Key Computation	61
4.3.3	Secure Data Transmission in VANETs	63
4.3.4	Key Updating	65
4.4	SECURITY ANALYSIS	68
4.4.1	Resistance to Replay Attack	68
4.4.2	Masquerade and Sybil Attacks	68
4.4.3	Message Tampering /Fabrication/ Alteration Attack	69
4.4.4	Backward Secrecy	69
4.4.5	Forward Secrecy	70
4.4.6	Collusion Attack	71
4.5	PERFORMANCE ANALYSIS	72
4.6	CONCLUSIONS	76
5	CPAV: COMPUTATIONALLY EFFICIENT PRIVACY PRESERVING ANONYMOUS AUTHENTICATION FOR A VEHICLE USER IN VANETS	78
5.1	INTRODUCTION	78
5.2	SECURITY REQUIREMENTS	78

CHAPTER NO.	TITLE	PAGE NO.
5.3	BILINEAR PAIRING	79
5.4	PROPOSED CPAV SCHEME	80
5.4.1	System Initialization	80
5.4.2	Registration	81
5.4.3	Secure Activation Key Distribution	81
5.4.4	CPAV Secure Anonymous Mutual Authentication	82
5.5	SECURITY ANALYSIS	85
5.5.1	Message Integrity and Source Authentication	85
5.5.2	Conditional Privacy Preservation	86
5.5.3	Anonymity	86
5.6	PERFORMANCE ANALYSIS	87
5.7	CONCLUSIONS	91
6	EFFICIENT ANONYMOUS AUTHENTICATION OF AN RSU	92
6.1	INTRODUCTION	92
6.2	ANONYMOUS AUTHENTICATION	93
6.2.1	System Initialization	93
6.2.2	Anonymous Authentication of an RSU	94
6.3	SECURITY ANALYSIS	98
6.4	PERFORMANCE ANALYSIS	99
6.4.1	RSU Serving Capability	100
6.5	CONCLUSIONS	102

CHAPTER NO.	TITLE	PAGE NO.
7	CEKD: COMPUTATIONALLY EFFICIENT KEY DISTRIBUTION	103
7.1	INTRODUCTION	103
7.2	CEKD SCHEME	104
	7.2.1 System Initialization	104
	7.2.2 VANET License Issuing	104
	7.2.3 CEKD Scheme	105
7.3	SECURITY ANALYSIS	107
7.4	PERFORMANCE ANALYSIS	108
7.5	CONCLUSIONS	110
8	CONCLUSIONS AND FUTURE WORKS	111
8.1	DUAL AUTHENTICATION AND DUAL KEY MANAGEMENT FOR GROUP COMMUNICATION	111
8.2	CPAV: COMPUTATIONALLY EFFICIENT PRIVACY PRESERVING ANONYMOUS AUTHENTICATION	112
8.3	EFFICIENT ANONYMOUS AUTHENTICATION OF AN RSU	112
8.4	CEKD: COMPUTATIONALLY EFFICIENT KEY DISTRIBUTION	113
8.5	FUTURE WORKS	113
	REFERENCES	114