

Ahmed Fraz Baig

**An Improved and Robust
Anonymous Authentication
Scheme for Roaming in
Global Mobility Networks**



Anchor Academic Publishing

disseminate knowledge

Baig, Ahmed Fraz: An Improved and Robust Anonymous Authentication Scheme for Roaming in Global Mobility Networks, Hamburg, Anchor Academic Publishing 2017

PDF-eBook-ISBN: 978-3-96067-647-8

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

Acknowledgments

I am very grateful to *ALLAH* the *ALMIGHTY* for without His grace and blessing this study would not have been possible.

Foremost, I would like to express my sincere gratitude to my supervisor *Dr. Shehzad Ashraf Chaudhry* for the continuous support of my MS study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my MS study.

I would also like to acknowledge my friends, and colleagues. All of them encouraged and provided logistic and technical help during this research.

I would like to admit that I owe all my achievements to my truly, sincere and most loving parents and friends who mean the most to me, and whose prayers have always been a source of determination for me.

Abstract

Global Mobility Networks(GLOMONET) plays very important role in wireless communication. Due to the rapid growth of technology in wireless communication different security challenges have been raised up in GLOMONET. A secure and threat-proof authentication protocol in wireless communication may overcome the security issues because it permits only a legitimate user to access the services. Recently, Karuppiah-Saravanan found Rahee et al's scheme suffers with various attacks and proposed a new scheme by using Diffie-Hellman key agreement protocol, Gope-Hwang pointed out that Wen et al. scheme suffers with many security problems and Islam et al. proposed new authentication Chaotic Maps based scheme. This thesis points out that Karuppiah-Saravanan's scheme is vulnerable to Impersonation attack, Replay attack and key guessing attacks and the Gope-Hwang's scheme cannot resist the replay attacks, Dos attacks and scheme does not verify the user and password locally. Whereas, Islam et al's scheme is failed to accomplish mutual authentication and user anonymity. Thus, this thesis introduced EEC based an improved and robust protocol to overcome all security flaws and to attain computational efficiency in Global Mobility Networks. The security analysis of proposed work is checked formally and informally. Further security and computational analysis reveals that our proposed authentication scheme can withstand all possible attacks in GLOMONET with the features of user anonymity, user friendliness and efficient computation cost.

Contents

1	Introduction	2
1.1	Authentication in GLOMONET	3
1.2	Preliminaries	3
1.2.1	Hash Function	3
1.2.2	Elliptic Curve Cryptography(ECC)	4
1.3	Objectives	4
1.4	Thesis outline	5
2	Literature Review	6
2.1	Literature Survey	6
2.2	Karuppiah-Saravanan’s scheme review	8
2.2.1	Initialization phase	9
2.2.2	Registration Phase	9
2.2.3	Login-Authentication Phase	9
2.2.4	Password Change Phase	11
2.2.5	Cryptanalysis and security weaknesses in Karuppiah-Saravanan’s Scheme	11
2.3	Gope-Hwang’s scheme review	13
2.3.1	Registration-reestablishment Phase	13
2.3.2	Mutual-Authentication Phase with key-agreement phase	14
2.3.3	Password Change Phase	15
2.3.4	Security weaknesses in Gope-Hwang’s Scheme	15
2.4	Islam et al.’s scheme review	18
2.4.1	Registration Phase	18
2.4.2	Login Phase	18
2.4.3	Authentication Phase	19
2.4.4	Password Change Phase	19
2.4.5	Revocation of lost SC Phase	20

2.4.6	Cryptanalysis of Islam et al's. scheme	22
2.5	Problem Statement	22
2.6	Chapter Summary	23
3	Proposed Scheme	24
3.1	Initialization Phase	24
3.2	Registration Phase	25
3.3	Login Phase	25
3.4	Authentication Phase	26
3.5	Password change Phase	28
3.6	Chapter Summary	30
4	Security Analysis and Computation Cost Analysis	31
4.1	Security Analysis	31
4.1.1	Security Analysis with BAN logic	31
4.1.2	Security Analysis with ProVerif	35
4.1.3	Informal Security Analysis	40
4.1.4	Security Requirements and Comparison	45
4.1.5	Security Requirements	46
4.2	Computation Cost Analysis	46
4.3	Chapter Summary	49
5	Conclusion and Future work	50

List of Figures

1.1	Global Mobility Networks Authentication	4
2.1	Karuppiah-Saravanan's Scheme	12
2.2	Gope-Hwang's proposed scheme	17
2.3	Islam et al. scheme	21
3.1	Proposed Registration phase	25
3.2	Proposed Scheme	29