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

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

List of Figures