PLOS ONE

RESEARCH ARTICLE

Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance

Keyan Abdul-Aziz Mutlaq[1,2], Vincent Omollo Nyangaresi[3], Mohd Adib Omar[1]*, Zaid Ameen Abduljabbar[4], Iman Qays Abduljaleel[5], Junchao Ma[6], Mustafa A. Al Sibahee[7,8]*

1 School of Computer Sciences, Universiti Sains Malaysia, USM, Gelugor, Penang, Malaysia, **2** IT and Communications Center, University of Basrah, Basrah, Iraq, **3** Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya, **4** Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq, **5** Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq, **6** College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China, **7** National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen, China, **8** Computer Technology Engineering Department, Iraq University College, Basrah, Iraq

* adib@usm.my (MAO); mustafaalsibahee@szu.edu.cn (MAAS)

Citation: Mutlaq KA-A, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, et al. (2024) Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. PLoS ONE 19(1): e0296781. https://doi.org/10.1371/journal.pone.0296781

Editor: Pandi Vijayakumar, University College of Engineering Tindivanam, INDIA

Received: August 19, 2023

Accepted: December 19, 2023

Published: January 23, 2024

Data Availability Statement: All relevant data are within the manuscript and its Supporting information files.

Funding: This work is supported by Natural Science Foundation of Top Talent of SZTU (grant No. 20211061010016). This work is partially supported by National Natural Science Foundation of China (61972263, 62073225), and the Stable Support Plan for Higher Education Institutions in Shenzhen (20200810113310001). The funders had no role in study design, data collection and

Abstract

The incorporation of information and communication technologies in the power grids has greatly enhanced efficiency in the management of demand-responses. In addition, smart grids have seen considerable minimization in energy consumption and enhancement in power supply quality. However, the transmission of control and consumption information over open public communication channels renders the transmitted messages vulnerable to numerous security and privacy violations. Although many authentication and key agreement protocols have been developed to counter these issues, the achievement of ideal security and privacy levels at optimal performance still remains an uphill task. In this paper, we leverage on Hamming distance, elliptic curve cryptography, smart cards and biometrics to develop an authentication protocol. It is formally analyzed using the Burrows-Abadi-Needham (BAN) logic, which shows strong mutual authentication and session key negotiation. Its semantic security analysis demonstrates its robustness under all the assumptions of the Dolev-Yao (DY) and Canetti- Krawczyk (CK) threat models. From the performance perspective, it is shown to incur communication, storage and computation complexities compared with other related state of the art protocols.

1. Introduction

Electrical grids comprise of networks that perform power generation, transmission as well as distribution. In this environment, there is need for communication and coordination with the power control centers so as to control and monitor the grid. To boost power supply quality,