electronics

MDPI

Article

A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles

Vincent Omollo Nyangaresi [1], Hend Muslim Jasim [2], Keyan Abdul-Aziz Mutlaq [3], Zaid Ameen Abduljabbar [2,4,5,*], Junchao Ma [6,*], Iman Qays Abduljaleel [7] and Dhafer G. Honi [2]

1 Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya
2 Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
3 IT and Communication Center, University of Basrah, Basrah 61004, Iraq
4 Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
5 Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China
6 College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
7 Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
* Correspondence: zaid.ameen@uobasrah.edu.iq (Z.A.A.); majunchao@sztu.edu.cn (J.M.)

Abstract: Unmanned aerial vehicles have found applications in fields such as environmental monitoring and the military. Although the collected data in some of these application domains are sensitive, public channels are deployed during the communication process. Therefore, many protocols have been presented to preserve the confidentiality and integrity of the exchanged messages. However, numerous security and performance challenges have been noted in the majority of these protocols. In this paper, an elliptic curve cryptography (ECC) and symmetric key-based protocol is presented. The choice of ECC was informed by its relatively shorter key sizes compared to other asymmetric encryption algorithms such as the Rivest–Shamir–Adleman (RSA) algorithm. Security analysis showed that this protocol provides mutual authentication, session key agreement, untraceability, anonymity, forward key secrecy, backward key secrecy, and biometric privacy. In addition, it is robust against smart card loss, password guessing, known secret session temporary information (KSSTI), privileged insider, side-channeling, impersonation, denial-of-service (DoS), and man-in-the-middle (MitM) attacks. The comparative performance evaluation showed that it has relatively low computation, storage, and communication complexities.

Keywords: UAV; authentication; security; privacy; attacks

Citation: Nyangaresi, V.O.; Jasim, H.M.; Mutlaq, K.A.-A.; Abduljabbar, Z.A.; Ma, J.; Abduljaleel, I.Q.; Honi, D.G. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. *Electronics* **2023**, *12*, 3688. https://doi.org/10.3390/electronics12173688

Academic Editor: Dimitra I. Kaklamani

Received: 4 July 2023
Revised: 1 August 2023
Accepted: 25 August 2023
Published: 31 August 2023

1. Introduction

Unmanned aerial vehicles (UAVs), popularly known as drones, are smart machines with Internet of Things (IoT) connections that fly over certain regions to provide numerous real-time services [1]. For instance, they have been extensively deployed in areas such as intelligent transportation systems (ITSs), the detection and collection of environmental data, emergency rescue, autonomous driving, the creation of high-definition maps in real-time, and military applications [2,3]. In UAV-enabled ITSs, car sharing, real-time map creation, and autonomous driving can be facilitated [4]. In the military, surveillance, reconnaissance, intelligence collection, ground strikes, and fire guidance are enabled. As explained in [5,6], UAVs can also be applied in civil aviation, industrial setups, and areas that are dangerous or difficult for humans to reach, such as during earthquake searches and gas leak detection. In some cases, these drones can serve as relay nodes in mobile and wireless sensor network (WSN) communications. The authors of [7] pointed out that UAVs can be considered as extensions of Internet of Vehicle (IoV) communication that can offer aerial interfaces for