MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones

Zaid Ameen Abduljabbar[1,2], Vincent Omollo Nyangaresi[3], Junchao Ma[4(✉)], Mustafa A. Al Sibahee[4,5], Mustafa S. Khalefa[1], and Dhafer G. Honi[1]

[1] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
{zaid.ameen,mustafa.khalefa,dhafer.honi}@uobasrah.edu.iq
[2] Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen 518118, China
[3] Faculty of Biological and Physical Sciences, Tom Mboya University, Homabay 40300, Kenya
vnyangaresi@tmuc.ac.ke
[4] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
{majunchao,mustafa}@sztu.edu.cn
[5] Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
mustafa.alsibahee@iuc.edu.iq

Abstract. Unmanned aerial vehicles have been deployed for surveillance in highly sensitive domains such as in the military. As such, the data exchanged between the operators and these aerial vehicles must be protected as any malicious access may lead to leakages and adversarial control of the drones. To achieve this, many schemes have been developed based on techniques such as blockchains, elliptic curve cryptography, dynamic keys, physically unclonable function, asymmetric and symmetric cryptography among others. However, majority of these protocols have been shown to be inefficient for deployment in this environment, while others have security holes that be exploited by attackers to cause mayhem in these networks. In this paper, a protocol that leverages on quadratic residues and Chinese remainder theorem is developed. Its security analysis shows that it offers mutual authentication, non-repudiation, unlinkability, identity privacy and traceability for misbehaving drones. It is also resilient against impersonation, forgery and replay attacks. In terms of performance, this protocol has the least execution time and relatively lower bandwidth requirements.

Keywords: Authentication · Drones · Encryption · MAC · Protocol · Privacy · Symmetric · UAV

1 Introduction

Unmanned Aerial Vehicles (UAVs) consist of airborne sensors and drones that communicate through wireless channels [1]. They are normally managed via radio remote control techniques and some inbuilt program control devices [2]. Due to their wider coverage, UAVs have been applied in a wide range of domains such as in the military,

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2022, LNICST 445, pp. 16–36, 2022.
https://doi.org/10.1007/978-3-031-15101-9_2