Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges

Vincent Omollo Nyangaresi
Faculty of Biological & Physical Sciences
Tom Mboya University College, Homabay, Kenya.
vnyangaresi@tmuc.ac.ke

Zaid Ameen Abduljabbar
Computer Science Department
College of Education for Pure Sciences,
University of Basrah, Basrah, Iraq.
Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
Shenzhen Insitute of Huazhong University of Science & Technology,
Shenzhen, China.
zaid.ameen@uobasrah.edu.iq

Mustafa A. Al Sibahee
Department of Computer Technology Engineering,
Iraq University College, Basrah, Iraq.
College of Big Data and Internet,
Shenzhen Technology University, Shenzhen, China.
mustafa@sztu.edu.cn

Ayad Ibrahim
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
ayad.abdulsada@uobasrah.edu.iq

Mohammed Abdulridha Hussain
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
mohammed.abdulridha@uobasrah.edu.iq

Zaid Alaa Hussien
Information Technology Department, Management Technical College, Southern Technical University, Basrah, Iraq
zaid.alaa@stu.edu.iq

Mudhafar Jalil Jassim Ghrabat
Ashur University College, Pharmacy Department, Baghdad, Iraq
mudhafar.jalil@au.edu.iq

2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) | 978-1-6654-4231-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICECET52533.2021.9698744

***Abstract*— Unmanned Aerial Vehicles (UAVs) convey secret data that belongs to the military, individual or organizations. As such, privacy and security protection of this data is critical. To accomplish this, many protocols have been presented based on techniques such as dynamic keys, Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), public key cryptosystems, bilinear pairing, certificate-less group keys and Radio Frequency Identification (RFID). However, some of these schemes have long session keys and hence high computational and communication complexities, while others fail to address most pertinent attack vectors in UAV networks. In this paper, a provably secure session key agreement protocol is developed. The security analysis shows that it offers backward and forward key secrecy, strong anonymity, and can withstand impersonation, replay, privileged insider and side-channeling attacks. In terms of bandwidth requirements, the proposed protocol has the least bandwidth requirements among other related protocols. On the other hand, it requires average execution time during the key agreement and authentication phases.**

***Keywords*— Anonymity, attacks, authentication, privacy, protocol, security, UAV.**

I. INTRODUCTION

Unmanned Aerial Vehicle (UAV) generally refers to remote controlled unmanned aircrafts [1] that have some inbuilt control mechanisms. As explained in [2], the UAV network comprises of internet of drones communicating with each other. UAVs have salient features such as wider coverage and sensing capabilities [3] that has endeared them to applications such as military reconnaissance and disaster monitoring. Despite their wider application domains, the leakage of sensitive data conveyed in UAV networks is a major concern [4]. In military, it is critical to ensure that UAVs entering some secure airspace are properly authenticated, as some of them may be adversary-operated. As pointed out in [5], the deployment of UAV is normally curtailed by security fears. Although there are many security solutions for distributed network scenario, these schemes are inapplicable in a UAV communication environment [6] due to its dynamic topology which requires continuous authentication.

In addition, efficient resource usage in UAV network is critical due to post-disaster high traffic demands [7], and hence UAV security solutions need to be lightweight. In the absence of sufficient security and privacy protection, attackers can modify, delete, replay, monitor and eavesdrop the exchanged UAV intelligence [8]. Other attacks in this environment include man-in-the-middle (MITM), forgery, denial of service (DoS) and message replays [2], [4]. This is attributed to the transmission of packets among UAVs and the Ground Control Stations (GCSs) over insecure wireless channels [9]. On the other hand, the deployment of UAVs in unattended environments has been heighted in [5] as being the reason for physical capture and cloning attacks.

Before being allowed to operate within a particular secure airspace, UAVs must be authenticated [10]. However, the sensors that form part of the UAV network have limited computing power [3], and hence cannot handle computationally intensive cryptographic operations such as those ones of Public Key Infrastructure (PKI). Identity based authentication can be executed in a UAV network to verify the authenticity of each communicating entity. For instance, upon topological changes, new UAVs may join the network. These new entrants must be identity-authenticated prior to exchanging messages with other existing UAVs [2]. As explained in [11], encryption protocols can also be applied to preserve the integrity of transmitted message. However, with the ever-increasing computing power, it is possible to decipher the deployed passwords. As such, majority of the security protocols are not effective in the prevention of UAV attacks [12] as they have either performance or security challenges. For instance, identity-based schemes may inadvertently lead to leakage of authenticating entities' real identities [13].

978-1-6654-4231-2/21/$31.00 ©2021 IEEE