applied sciences

MDPI

Review

A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions

Adnan Shahid Khan [1,*], Muhammad Ali Sattar [1], Kashif Nisar [2], Ag Asri Ag Ibrahim [3,*], Noralifah Binti Annuar [1], Johari bin Abdullah [1] and Shuaib Karim Memon [4]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2] Victorian Institute of Technology, Adelaide, SA 5000, Australia
[3] Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia
[4] Department of Computer Science, University of York, Deramore Lane, Heslington, York YO10 5GH, UK
* Correspondence: skadnan@unimas.my (A.S.K.); awgasri@ums.edu.my (A.A.A.I.)

Abstract: This paper demonstrates a broad exploration of existing authentication and secure communication of unmanned aerial vehicles (UAVs) in a '6G network'. We begin with an overview of existing surveys that deal with UAV authentication in 6G and beyond communications, standardization, applications and security. In order to highlight the impact of blockchain and UAV authentication in 'UAV networks' in future communication systems, we categorize the groups in this review into two comprehensive groups. The first group, named the Performance Group (PG), comprises the performance-related needs on data rates, latency, reliability and massive connectivity. Meanwhile, the second group, named the Specifications Group (SG), is included in the authentication-related needs on non-reputability, data integrity and audit ability. In the 6G network, with blockchain and UAV authentication, the network decentralization and resource sharing would minimize resource under-utilization thereby facilitating PG targets. Furthermore, through an appropriate selection of blockchain type and consensus algorithms, the SG's needs of UAV authentication in 6G network applications can also be readily addressed. In this study, the combination of blockchain and UAV authentication in 6G network emergence is reviewed as a detailed review for secure and universal future communication. Finally, we conclude on the critical identification of challenges and future research directions on the subject.

Keywords: 6G; unmanned aerial vehicles; network; security; topology; authentication; cryptography

Citation: Khan, A.S.; Sattar, M.A.; Nisar, K.; Ibrahim, A.A.A.; Annuar, N.B.; Abdullah, J.b.; Karim Memon, S. A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions. *Appl. Sci.* **2023**, *13*, 277. https://doi.org/10.3390/app13010277

Academic Editor: Dimitris Mourtzis

Received: 22 October 2022
Revised: 22 November 2022
Accepted: 23 November 2022
Published: 26 December 2022

1. Introduction

As 5G is heading closer to commercial status, prospects of UAV system integration with future 6G communication models are becoming a significant part of ongoing research in the field [1]. These papers identify a few key UAV systems in 6G flighty applications and administrations such as Human Bond Communication (HBC), Multi-sensory amplified Reality Applications (XR), Wearable Innovation-based Cutting edge Applications (WTech) and Large-scale associated independent frameworks (LS-CAS), and are more noteworthy for a few vertical spaces. All these applications show up in a combinational way beneath the space of the UAV system in 6G-based UAV communication. These applications have remarkably demanding information rates, inactivity and unwavering quality; thus, the nature of the information collected by a few UAV systems in 6G applications will be progressively delicate and fundamental. As 5G is entering the deployment phase, discussion on 6G networks is gradually gaining momentum [2]. The objective of 6G is to support faster connection. Hence, the performance of 6G will be degraded using an inefficient authentication scheme which also brings the possibility towards some security issues. The productive allocation of UAV frameworks in 6G-based UAV structures by the customers would thus require strict data security guarantees. Figure 1 illustrates the UAV paradigm in