This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TGCN.2021.3111529, IEEE Transactions on Green Communications and Networking

Blockchain-based Data Dissemination Scheme for 5G-enabled Softwarized UAV Networks

Rajesh Gupta, *Student Member, IEEE*, Mohil Maheshkumar Patel, Sudeep Tanwar, *Senior Member, IEEE*, Neeraj Kumar, *Senior Member, IEEE*, Sherali Zeadally, *Senior Member, IEEE*

***Abstract*—Unmanned aerial vehicles (UAVs) are widely used in various applications such as surveillance, healthcare, rescue, and crowdsensing. However, the network management of these applications is quite challenging given the mobility of UAVs. In this scenario, network softwarization, which decouples the hardware from the network control functions, becomes essential. Moreover, the fifth generation (5G) communication network is used to disseminate the data from controller-to-UAV and UAV-to-Internet of things (IoT) enabled devices. However, handling the security and privacy of data against the eavesdropper is one of the challenging aspects that need to be resolved efficiently. Most of the solutions presented in the literature are based on a centralized architecture having a single point of failure and are also vulnerable to various security attacks such as controller hijacking and man-in-the-middle attack. Motivated by these facts, we present a blockchain-based secure data dissemination scheme for softwarized UAV networks. The proposed scheme can detect an eavesdropper, analyze malicious data, and mitigate various security attacks on the SDN controller. The performance analysis shows that the proposed scheme achieves superior results in detecting the eavesdropper and anomalous data before adding them into the blockchain compared to other state-of-the-art schemes.**

***Index Terms*—Blockchain, smart contract, software-defined network, softwarization, unmanned aerial vehicles, 5G.**

I. Introduction

In recent years, unmanned aerial vehicles (UAVs) have been used in numerous cyber-physical applications such as healthcare monitoring, intelligent transport systems, search & rescue, and video streaming. UAVs are high-mobile and cost-efficient flying devices, which can cover a wider area and can be deployed quickly in terrain environments wherever needed [1]. UAVs with traditional networks such as 4G LTE-A cannot meet the required quality of service (QoS) and quality of experience (QoE) due to high delay. The fifth-generation (5G) communication network with its characteristics of ultra-low latency ($< 1ms$) and ultra-high reliability (99.999%) meets the QoS and QoE of the cyber-physical applications [2]. Integrating 5G with UAVs provides real-time communication, dynamic topology, and universal coverage. The massive deployment of UAVs makes network management tedious and challenging. This is because the network functions such as firewall, routing, access control, bandwidth management, and path planning are tightly coupled with the network hardware devices, i.e., devices are capable of making dynamic decisions autonomously [3]. So, any modification in device network functions is a burden for the system developers because they need to shut down the entire system during maintenance activity that affects the system throughput and reliability [4]. This also raises the capital and operational expenditures associated with it.

Network softwarization can be employed to overcome the aforementioned UAV network management issues. 5G-enabled software-defined network (SDN) is the key enabler for softwarization, which separates the hardware control plane from the data plane and communicates using the OpenFlow protocol [5]. It is well suited for a highly mobile UAV network where the connectivity is intermittent. The other benefits of softwarization in the UAV network are (i) flexibility and versatile, (ii) cost-effective, and (iii) the upgrading of network services without shutting down the entire system. This employs massive deployment of UAVs, which motivates researchers to explore artificial intelligence (AI)-based solutions to increase network efficiency. AI algorithms are being increasingly adopted in various UAV areas such as channel modeling, autonomous path-planning, swarm intercommunication, UAV detection, and cooperative multi-UAV transmission.

Such a high utilization and deployment of softwarized UAVs opens up various security and privacy concerns such as unauthorized access to SDN controller, denial-of-service, eavesdropping, jamming, software vulnerabilities, and UAV hijacking [6], [7]. These security attacks can either harm the UAV or stop it from performing its intended task. This motivates the researchers to develop and design solutions to cope up with the aforementioned issues. Moreover, the adoption of ML and AI techniques provides intelligent solutions to these problems.

All SDN, AI, and power optimization-based solutions that many authors have proposed may suffer from various issues such as controller hijacking and detecting intelligent eavesdroppers [8]. To address the aforementioned issues, blockchain technology is a viable solution. Blockchain is a distributed ledger and is equipped with cryptographic techniques to ensure data security. The immutability characteristic of blockchain does not allow any modification of data once stored into the block of a blockchain. It eliminates the trusted third-party systems by incorporating the concept of smart contracts, which are self-executable and self-enforceable. This paper proposes

R. Gupta, M. Patel, S. Tanwar are with the Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India 382481, e-mail: (18ftvphde31@nirmauni.ac.in, 17bce062@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in).

N. Kumar is with Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India, and School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India, e-mail: (neeraj.kumar@thapar.edu).

S. Zeadally is with the College of Communication and Information, University of Kentucky, Lexington, KY 40506-0224, USA (szeadally@uky.edu).

2473-2400 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.