

Design security architecture for unmanned aerial vehicles by 5G cloud network based implementation of SDN with NFV and AI

Ahssan Ahmed Mohammed Lehmoud¹, Nawfal Turki Obeis², Ahmed Fakhir Mutar^{1,3}

¹Babylon Education Directorate, Babylon, Iraq

²Department of Information Network, College of Information Technology, University of Babylon, Babylon, Iraq

³Department of Computer Technology Engineering, Al-Mustaqbal University College, Babylon, Iraq

Article Info

Article history:

Received Jun 12, 2022

Revised Sep 5, 2022

Accepted Sep 28, 2022

Keywords:

Authentication

Network

Software defined networking security

Unmanned aerial vehicle

ABSTRACT

A recent progression of unmanned aerial vehicles (UAV) augmentation its employments for different applications. It's also vulnerable to being, stolen, lost, stray, or destroyed at status of a security infringements for the UAV network. The proposed strategy is defending against of different attacks through using artificial intelligence by implements five steps: RGSK, GCSCS, SEDC, HSSC, and FVNF. UAV authentication is happened in the first step through the Curve448. We performance deep reinforcement learning to run with GCS for packet assignment as it implemented for switch current state identification before updating. In our work we ability to alleviate for attack of flow table overloading by assigned of packets as an under loaded or idle switches. Then, selected the least loaded switch by applied 5 tuples. Hence, we divided SDN to SEDCs and HSSC forms. First in the SEDC we using Shannon entropy to achieve classified of input packet in to regular and suspicious packets. Last will forwarded regular packets to cloud layer. By growing multiple self-organizing maps for maintained in NFV that used to classify suspicious packets as classes normal or malicious packet. The proposed performance work evaluates using NS3.26 show up the better strategy to secure UAV for different attacks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ahssan Ahmed Mohammed Lehmoud

Babylon Education Directorate

86 Mahaweel, Babylon, Iraq

Email: ahssan_ahsan@bab.epedu.gov.iq

1. INTRODUCTION

The unmanned aerial vehicle (UAV) is a major drivers of the smart society that is produces of different cost efficient services such as surveillance, search operations, inspection, policing, traffic management, involve rescue, and package delivery [1]–[3]. In fact, an UAV is aircraft flying without human pilot on board as well as it controls autonomously based on operator or the onboard computer systems during flight [4]–[6]. Through information technology with computer developments, the UAV communication and miniaturization therefore included of other flying objects quadcopters, balloons could, and gliders be also included in UAV. The first UAV was designed and used through second world war for military operations after that was used in the civil applications. So, the UAV is used in different environments everywhere in the globe depending to them respective laws of country with regulations [7], [8].

Wireless communication is one of the critical enabling technologies for UAV. The network functions (NFs) like switching, routing, bandwidth allocations, and even load balancing that associated within network devices together. So, for any UAV with processor and memory for help it by taken dynamic network related decisions [9]–[11]. The control of UAV network and maintain is very difficult based for

UAV system developers because of many challenging like fitful connectivity, high mobility, high operational expenditures cost, and dynamic network topology that were associated with software integrated devices as well as, reduce reliability of the UAV network system's [12].

So, by implement of network softwarization (NS) technique via the UAV network will be possible to aforementioned issues associated and eliminated. It provides and decouples the softwarization of NFs that are accomplished via the devices of network and UAVs. The recent fifth generation technologies (5G) like network function virtualizations (NFV) and software defined networking (SDN), which the enablers to softwarization [13], [14]. Over dividing user plane from control plane in SDN as forwarding plane by network programmability utilizing the open source interfaces like OpenDaylight [15] OpenFlow [16] through southbound application programming interfaces. At the data plane for manage of switching and routing for data packets of UAV by populates of the flow table in centralized control plane. Nevertheless, without any additional hardware costs, the NFV permits to a NFs for virtualization, which share a physical resource like storage and compute with networking to expand of networks services based on UAVs systems. Multiple instances of NFs are creating by helps of containers at a NFV systems based on a network demand during single virtual machine [17]–[21].

According to a discussions raised, networks softwarization provides number of supports to the UAV network like NS authorizes system developers without making the entire network shutdown to regulate the NFs of UAV with policies via a centralized programming controls, NS is logically centralize of UAV networks intelligence within programmable NFs, NS increment of end user quality of services with quality of experiences [22], NS preserves for the UAV specific dynamic path information like to accomplish the mission timely from source to destination, and last NS allows flexible and cost efficient solutions (NFV without implement of any additional device) of UAV that is useful to mission criticals application [23]. The benefits of the UAV mentioned in the above paragraphs help for increase the acceptability with number of organizations in the world. Nevertheless UAV security continue the common agenda. UAV security will extreme importance because of vastly used in different mission critical applications. The vital information can affect the entire UAV network if compromised of any UAV can disclose through intruders.

The 5G mobile network helps with SDN/NFV for implement a UAV networks management for make it a robust with easy through separating of control from the data plane or forwarding plane for a UAVs. Therefore when implement of SDN will allows take real-time dynamic decisions of the programming performance of UAV NFs in the control layer in efficiently. Also will increases the UAV network of it scalability. For the best communication by intended of a SDN, NFV with cloud and 5G network to be more of rate with less data latency as a goal of our proposed work.

Many of work based for security of UAV in last few years, some of them will be the focus of related work in our paper like Fichera *et al.* [24] introduces an OPERETTA system to mitigate synchronous (SYN) flooding attack by implemented in the controller. Presented a system lengthy delays as it first proves the transmission control protocol (TCP) source then implement the forwarding rules [25], [26]. Among the previous studies, it wasin implanted an identity based of cryptography structure between data and control planes of SDN for secure communication [27]. In the same field implement the SLICOTS system, at SDN based of combat attack of SYN flooding. Beneath different attacks scenarios they have performed a SLICOTS system with decrease the time of response up to 50% as an expansion of the ODL controller as compared within a existent states of the art system [24].

In this way also introduce effectively information used on UAV networks for manage and analyze by monitoring platform was implement based for SDN controller, also introduce a balancing algorithm to maintain a desirable network service. The SDN framework based on towards knowledge centric networking [28], [29]. Additionally, introduce a SDN based to secure structure for preserve UAV against a particular attack like a distributed denial of service, wormhole, and blackhole attacks [30]. Moreover, implement of new kind of UAV network called SUV depened on SDN structure with blockchain technology to physically distributed control plane for the configuration management as well as routing calculation to UAV network [31]–[34].

The aforementioned security solutions for SDN with NFV may be suffer from different issues such as lead astray of UAVs from their legitimate ways when prospect of distributed denial of service attack in SDN controller. The attack of man in the middle may be spoofed for communication via data and control planes, the UAV data privacy may be could compromise because of various policies are being implemented through much trusted third party (TTP) system of software compatibility issues, and may be the UAV network functionalities put down entire when compromised was happen for controller. The proposed work is a viable solution implemented to mitigate of security problem associated to the UAV network softwarization. The rest of proposed work in this paper is marshaled by: i) introduce the work on proposed design system for security UAV based by SDN with FNV and AI; ii) method of simulation environment of this paper. Then provide of security of our proposed for design work; iii) result for proposed work and discussion based on attacks; and v) at the latest, we state our concluding remarks.

2. METHOD

In this section, we will explain the proposed design system to detected as well as prevent various security attacks. The propose work will be managing a network of UAV in both cases based on data communication as UAV-to-UAV by switch and between UAV-to-ground stations. Where we will use 5 steps to provide adequate flexibility and protection that is shown in the Figure 1. The proposed security work is divided into 5 steps, namely:

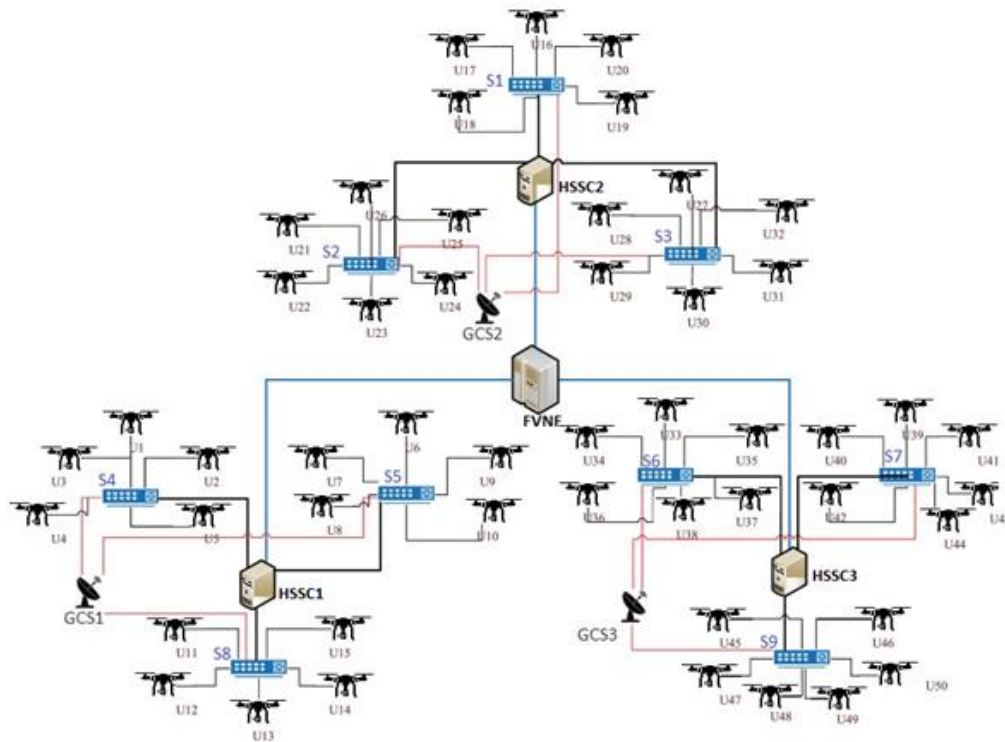


Figure 1. Main structure of proposed UAV system

2.1. Register and generated secret key

First step in our proposed system is register and generated secret key (RGSK), any UAV that requests access to the system, the TTP will register its data from device ID, IP address, password, and the media access control (MAC) address. The TTP generates a secret key and gives it reliability if the registration information is correct. The secret key is generated by using the (Curve448) key generation algorithm.

Curve448 is elliptic curve algorithm with possibility to providing 224bits of security. Curve448 introduce for utilize with the elliptic curve Diffie Hellman (ECDH) means ECDH for key agreement scheme for cryptography. Curve448 permits quick execution when compared via other curves algorithm by comparable security [35]. Hamburg select the Solinas trinomial major rule $H_p=2,448-2,224-1$. Solinas trinomial calling a "Goldilocks" major" based on defines a golden ratio $\phi=2,224$ ". Prime feature of the golden ratio major is quick Karatsuba multiplication [36], [37]. The curve Hamburg utilize is a not twisted Edwards curve $E_d: A^2+B^2=1-39081B^2A^2$. The constant $d_s=-39,081$ was selected as a little absolute number, which had the needed mathematical properties, thus a nothing up my sleeve value [38], [39].

TTP will provide the generated secret key for UAV to the ground control station (GCS) as a step for mitigate spoofing attack of IP. The UAV IP address assigned will remains stable as long as the connection is continuous and is changed in some cases and a new IP is taken, such as turning off, restate or exiting the UAV from GCS. So, the GCS generates a pseudorandom number for UAV registration by xor function between secret key and UAV IP. The UAV should be return pseudorandom number from GCS by used secret key. The authentication process occurs for GCS depending to the pseudorandom number because of a name is various as well as valid for specific time [40], [41].

Open the document you would like to format and import the styles. How this works depends very much on the version of Ms Word that you use. The styles' names to be used for online-journals.org are preceded by a "0_" which makes them appear first in the styles list and therefore easier to be found. Now just place the cursor in the paragraph you would like to format and click on the corresponding style in the styles window (or ribbon).

2.2. Ground control station classified switches

In the second step in our proposed system will processing UAV requested flow by selected the perfect switch through the GCS. The GCS classified switches based on 5 tuples of switch for 3 types as an overloaded, states under loaded and idle according. The characteristics of switch are packet forward rate, packet drop rate, packet received rate, duplicate packet rate, and packet time interval. The switch that is an under loaded will be selected by UAV based on the flow table usage to prevent overloading attack from switch by address the flow table. Therefore, will used deep reinforcement learning in our work to interact and learns via a real world environment as well as to extreme reward for environment in the current state. Deep reinforcement learning is depend on finite Markov decision process through entities that is following: i) step 1 X means a set of state and Y means set of action; ii) step 2 the probability of transition state is $Z(X' | x, y)$ means for action y of a state x the probability distribution function is calculated of state space; iii) step 3 r means a discount factor that has a range between 0 to 1; iv) step 4 the reward $\gamma(X*y)$ will calculated by use a state with action (set of a real number); and v) step 5 use finite Markov decision process when X and Y are finite variables.

When given X and Y in the environment we can compute of a probability distribution function to the follows reward r by (1):

$$Z(x', r|x, y) = zr(XT + 1 = X'. yt + 1 = r|XT = x. YT = y) \quad (1)$$

Also, according to the rewar function we can compute the state of transition probability z (2):

$$Z(X'|X, y) = \sum_{r \in Y} Z(x', r|x, y) \quad (2)$$

For compute the expected reward of x and y as (3):

$$r(X, y) = E[yt + 1|XT = x, YT = y] \sum_{r \in Y} r \sum_{x' \in X} z(x', r|x, y) \quad (3)$$

Two metrics will have updated for switch stage when applied deep reinforcement learning algorithm are packet inter arrival time and flow duration. The arrival time of the inter packet is a time variance via 2 succeeding data packets. And between the first and last packet for flow duration. The following fig will illustrate the switch update by deep reinforcement learning algorithm. Variables that enter of every switch as well as current state are gated in deep neural networks (DNN). Through, input variables will be calculating a weight value for a hidden layer and then locate the current state. also we compute the switch' s state for any request from UAV in our proposed work.

Based on packet inter arrival time with flow duration metrics we compute the objective. The GCS has 2 targets, the first one is specify the benign packet within a message to be switch as well as based for the network will be prohibit as a result to eliminate the malicious packet within message as second target. Therefore, will minimize the attack traffic percentage.

2.3. Shannon entropy for domain controlle

SEDC is the third step in our work, depending in packet features will classified and processed the packets in this step. So, by Shannon entropy function will classified the packets into 2 types as suspicious packets and regular packets that is computed by (4):

$$S(E) = -\sum_{j=1}^m p(E_j) \log_2(p(E_j)) \quad (4)$$

The Shannon entropy is $S(E)$ as well as the feature probability is $p(E_j)$ for E_j . Shannon entropy shall build based to learning average with its dynamic. Average of a Shannon entropy is beneficial characterizing each specific attack in the work, so, an incorrect decision will happen when the threshold as default setting on packet classification. For Shannon entropy in our work, we have assigned a threshold dynamically established as well as we computed the error based on multiple samples. Then will forwarded to the cloud for regular package through a smart controller.

2.4. Hierarchical structure of smart controller

Through HSSC will manage multiple controllers that connected with it as deploy in the domain controllers step in hierarchical structure to be presentation the performance of proposed work through an attack of a control plane saturation. The smart controller acts as second secret key that generator, to generate and schedule a secret applied key at whole of switches spreader for an environment. The smart controller used same algorithm for generating secret keys. Actually, authentication process of switches based on switch ID with

location and even history of packet by investigated with maintained at a smart controller and databases of domain controller. At smart controller, UAV attack of hijacking is alleviated through following: MAC with IP address of UAV and path of location for ID (UAV communicated with switch). For updated of this information specific to smart controller as well as reflected in the domain controller and GCS for attack alleviation.

2.5. Forwarded virtual network function

In this step will forwarded the questionable packets to the virtual network function for confirmation classification as malicious packets or regular packets utilizing the growing multiple self-organizing map. Growing multiple self-organizing map is proposed to discover the attack of distributed denial of service, so, it's adaptive and dynamic as well as has characteristic of unsupervised learning and supervised learning algorithms. Wherefore multiple virtual network functions are chosen in the cloud for classification the deployed for the current load. Questionable flow classification in virtual network functions is depend at a sequencing: i) source of IP UAV address; ii) destination of IP UAV address; iii) flow duration of UAV; iv) service kind; v) UAV length of a packet; vi) current timestamp; vii) UAV sequence number; viii) UAV action; ix) UAV unique identifier (pseudorandom number); and x) source UAVs locations (based on X-axis, Y-axis position or longitude with latitude).

After process of a flow request of regular packets depend at a python scripts then the system will have removed malignant packets from the network. Three entities will take in considered are success of packet average, loss of packet average and error of packet average when classification the packets. A questionable packet within height success of packet average within low for both of loss and error average of packet is considered as regular packet. The threshold in growing multiple self-organizing map is dynamic as well as should be miscellaneous for various packets. Therefore, the system will be possible to efficacious determine the malignant packets from its header.

3. RESULTS AND DISCUSSION

In this section, it is explained the results of our proposed work and at the same time is given the comprehensive discussion. The proposed work was simulated is implemented by using network simulator (NS3), that is real time separated happening with open source NS. We used C++ as a programming language for simulation code as well as Python for commitment of programming. Also, we associated OpenFlow 1.0 for network simulator. Through our work, we used a 5 functions which is a get, set, update topologies with set flow table, and last is get flow status. Then using NetAnim programming to assistance of emulation with two modes consists of a real time scheduler. So, by GNU GPLv2 platform implemented we can simulation visualized as well as testbeds from the simulation (dynamic moving) with supported of live system. We implement the software-defined networking/network functions virtualization of 5G testbed for the simulation our work that is illustrate in following figure. Our work structure consists of completely connected, that is implemented of 50 UAVs as (U1,U50), nine of switches as (S1,S9), three of controllers as (HSSC1, HSSC3), and three of GCS (GCS1,GSC3). The proposed system was process in a Linux OS by Ubuntu 14.04 with allocated of single CPU core i7 and RAM of 6 GB. Our proposed work is executing a simulation in 5 minute with environment length of 1k*1k as well as buffer capacity is 10. Also 2 seconds as a packet interval with 100 mbps as data average some of work comparated with other works [39]–[41] our proposed work is a best strategy to secure UAV for different security attacks.

Based on the information provided by security of our proposed work, the transmission evaluation of confirmed better security and efficient authentication within various UAVs in the wireless medium that's shown by the following Table 1. Based on the Table 1, the following figure depict growing UAVs numbers in network, then spontaneous security communication with more in the proposed strategy in the same time will low floss based on bit transmission as shown in Figure 2. The ratio of throughput transmission through network for different UAVs are represented in the following Table 2. Based on the Table 2, the throughput result of proposed work gives preferable performs via transmitted among UAVs as well as shown in the following Figure 3. Through real testbeds, in this section we see the analysis of our proposed work to defend against different types of attacks like IP spoofing, distributed denial of service, flow table overloading, host hijacking and control plane saturation.

Table 1. Transmission evaluation

Number of UAVs	RGSK (bits)	GCSCS (bits)	SEDC (bits)	HSSC (bits)	FVNF (bits)
50	8,480	12,640	13,750	15,135	16,825
100	8,765	11,700	13,200	14,700	16,090
150	8,670	10,515	12,300	13,590	15,435
200	9,320	11,700	12,650	13,650	14,550
250	8,960	10,500	11,780	12,535	14,170

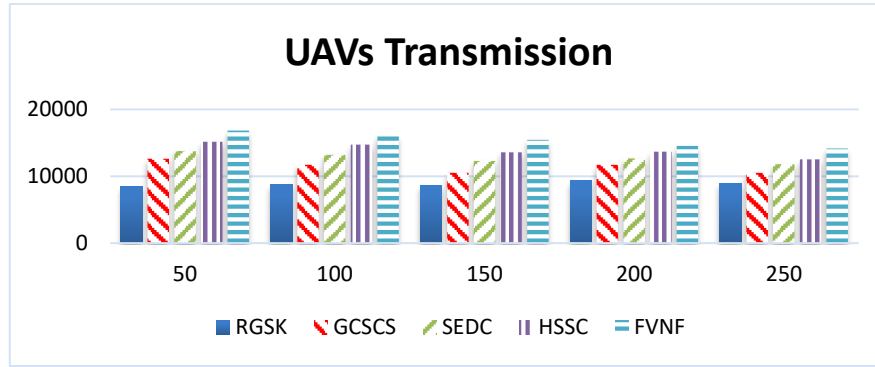


Figure 2. Show the transmission evaluation

Table 2. Throughput transmission

Number of UAVs	RGSK (bits)	GCSCS (bits)	SEDC (bits)	HSSC (bits)	FVNF (bits)
50	752	1,574	1,340	1,216	1,065
100	893	1,336	1,074	1,034	994
150	846	1,071	1,233	1,311	1,416
200	961	1,187	1,214	1,334	1,397
250	795	1,121	964	934	863

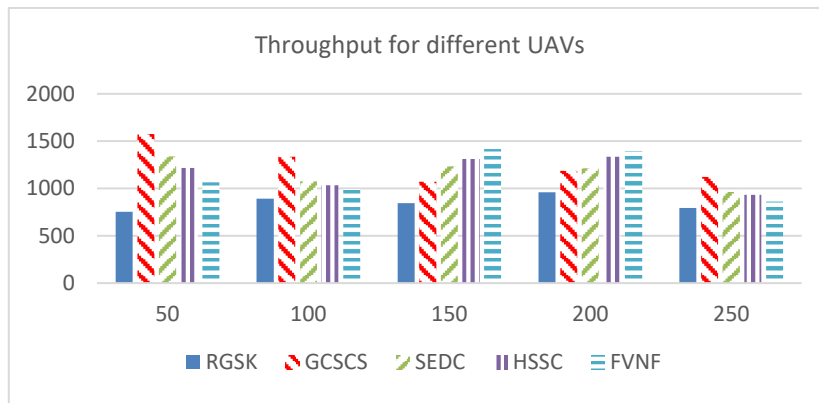


Figure 3. Throughput of different UAVs

4. CONCLUSION

In particular, for mitigate vulnerabilities and various security threats we proposed a strategy to achieve secure of UAV based on 5G cloud network with SDN/NFV programming. The main determination of this work to alleviate of attacks that infects UAV networks as: FlowTable overloading, distributed denial of service (DDos), IP_spoofing, host location hijacking, and control plane saturation attacks. To alleviate of IP spoofing attack, we used Curve448 algorithm with pseudorandom number generation for UAV device authenticated based on process held in TTP to be best achievement more than traditional ECC algorithm. For data plane, we authorized packets of UAV are performed using GCS that serves as middle via UAV and switches as well as for detect process and preventing it of interventions at a SDN/NFV for a packet of 5G networks. We performance deep reinforcement learning algorithm to run with GCS for packet assignment as it implemented at switch identification of current state before update process. In our proposed work we ability to alleviate for attack of flow table overloading by assigned of packets as an under loaded or idle switches. Then, selected the least loaded switch by applied 5 tuples. Hence, we divided SDN controllers to SEDCs and HSSC forms. first in the SEDC we using Shannon entropy to achieved classified of input packet in to regular and suspicious packets. last in the HSSC will forwarded regular packets to cloud layer. By growing multiple self-organizing map for maintained in NFV that used to classify suspicious packets as classes normal or malicious packet. therefore, through evaluate our proposed work performance it is the better strategy to secure UAV for different security attacks.

ACKNOWLEDGEMENTS

The authors thank Al-Mustaqbal University College as well as the dean of the Al-Mustaqbal university college for their financial and moral support for work.





REFERENCES

- [1] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Aug. 2019, pp. 1–5, doi: 10.1109/CITS.2019.8862127.
- [2] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, Oct. 2019, doi: 10.1109/MWC.001.1900028.
- [3] M. M. Jasim, H. K. AL-Qaysi, and Y. Allbadi, "Reliability-based routing metric for UAVs networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1771–1783, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1771-1783.
- [4] A. S. Hou and C. E. Lin, "UAS delivery multi-rotor autopilot based on ardu-pilot framework using s-bus protocol," in *2022 Integrated Communication, Navigation and Surveillance Conference*, 2022, pp. 1–10, doi: 10.1109/ICNS54818.2022.9771505.
- [5] Z. Jin, L. Nie, D. Li, Z. Tu, and J. Xiang, "An autonomous control framework of unmanned helicopter operations for low-altitude flight in mountainous terrains," *Drones*, vol. 6, no. 6, p. 150, Jun. 2022, doi: 10.3390/drones6060150.
- [6] J. Sakakeeny, H. R. Idris, D. Jack, and V. Bulusu, "A framework for dynamic architecture and functional allocations for increasing airspace autonomy," in *AIAA AVIATION 2022 Forum*, Jun. 2022, p. 3702, doi: 10.2514/6.2022-3702.
- [7] A. Takacs and T. Haidegger, "Infrastructural requirements and regulatory challenges of a sustainable urban air mobility ecosystem," *Buildings*, vol. 12, no. 6, p. 747, May 2022, doi: 10.3390/buildings12060747.
- [8] L. J. Prinzel *et al.*, "Human interfaces and management of information (HIMI) challenges for 'in-time' aviation safety management systems," *International Conference on Human-Computer Interaction*, 2022, pp. 367–387, doi: 10.1007/978-3-031-06509-5_26.
- [9] P. S. Ramesh and J. V. M. L. Jeyan, "Comparative analysis of the impact of operating parameters on military and civil applications of mini unmanned aerial vehicle (UAV)," in *AIP Conference Proceedings*, 2020, vol. 2311, pp. 1–10, doi: 10.1063/5.0033989.
- [10] D. Munera, D. P. Tobon V., J. Aguirre, and N. G. Gomez, "IoT-based air quality monitoring systems for smart cities: A systematic mapping study," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3470–3482, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3470-3482.
- [11] P. Manapongpun *et al.*, "DroneBox: A fully automated drone system for surveillance application," Mar. 2022, doi: 10.4043/31685-MS.
- [12] M. A. Massad, B. A. Alsaify, and A. Y. Alma'aitah, "Innovative unmanned aerial vehicle self-backhauling hybrid solution using RF/FSO system for 5G network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, p. 4483, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4483-4506.
- [13] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Computer Communications*, vol. 161, pp. 304–323, 2020, doi: 10.1016/j.comcom.2020.07.042.
- [14] S. Mahmoud, I. Jawhar, N. Mohamed, and Jie Wu, "UAV and WSN softwarization and collaboration using cloud computing," in *2016 3rd Smart Cloud Networks & Systems (SCNS)*, Dec. 2016, pp. 1–8, doi: 10.1109/SCNS.2016.7870554.
- [15] V. Sanchez-Aguero, F. Valera, B. Nogales, L. F. Gonzalez, and I. Vidal, "VENUE: Virtualized environment for multi-UAV network emulation," *IEEE Access*, vol. 7, pp. 154659–154671, 2019, doi: 10.1109/ACCESS.2019.2949119.
- [16] A. Wang, R. Liang, X. Liu, Y. Zhang, K. Chen, and J. Li, (2017, March). An inside look at IoT malware. In *International Conference on Industrial IoT Technologies and Applications*, Springer, Cham, March 2017, vol. 202, pp. 176–186, doi: 10.1007/978-3-319-60753-5_19.
- [17] M. Grari, I. Idrissi, M. Boukabous, O. Moussaoui, M. Azizi, and M. Moussaoui, "Early wildfire detection using machine learning model deployed in the fog/edge layers of IoT," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 2, pp. 1062–1073, 2022, doi: 10.11591/ijeecs.v27.i2.pp1062-1073.
- [18] T. S. Gunawan, W. A. Yahya, E. Sulaemen, M. Kartiwi, and Z. Janin, "Development of control system for quadrotor unmanned aerial vehicle using LoRa wireless and GPS tracking," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 5, pp. 2674–2681, Oct. 2020, doi: 10.12928/telkommika.v18i5.16716.
- [19] H. Cao, "Network function virtualization," in *Software Defined Internet of Everything*, Cham: Springer, 2022, pp. 135–143, doi: 10.1007/978-3-030-89328-6_8.
- [20] F. B. Sufi, J. D. D. Gazzano, F. R. Calle, and J. C. L. Lopez, "Multi-camera tracking system applications based on reconfigurable devices: A review," in *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, Jul. 2019, pp. 1–5, doi: 10.1109/IC4ME247184.2019.9036575.
- [21] A. Arulappan, G. Raja, K. Passi, and A. Mahanti, "Optimization of 5G/6G telecommunication infrastructure through an NFV-based element management system," *Symmetry*, vol. 14, no. 5, p. 978, May 2022, doi: 10.3390/sym14050978.
- [22] S. Badotra and S. N. Panda, "Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking," *Cluster Computing*, vol. 23, no. 2, pp. 1281–1291, 2020, doi: 10.1007/s10586-019-02996-0.
- [23] M. Wang, G. Simon, L. A. Neto, I. Amigo, L. Nuaymi, and P. Chanclou, "SDN East–West cooperation in a converged fixed-mobile optical access network: enabling 5G slicing capabilities," *Journal of Optical Communications and Networking*, vol. 14, no. 7, pp. 540–549, 2022, doi: 10.1364/JOCN.460300.
- [24] S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S. Palazzo, "OPERETTA: An openflow-based remedy to mitigate TCP SYN/FLOOD attacks against web servers," *Computer Networks*, vol. 92, pp. 89–100, Dec. 2015, doi: 10.1016/j.comnet.2015.08.038.
- [25] D. W. Djamari, M. R. Fikri, B. A. Budiman, and F. Triawan, "Formation control of non-identical multi-agent systems," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 2721–2732, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2721-2732.
- [26] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, 2020, doi: 10.1016/j.comnet.2019.106984.
- [27] I. Zacarias *et al.*, "Enhancing mobile military surveillance based on video streaming by employing software defined networks," *Wireless Communications and Mobile Computing*, pp. 1–12, Oct. 2018, doi: 10.1155/2018/2354603.
- [28] J. Lam, S.-G. Lee, H.-J. Lee, and Y. E. Oktian, "Securing SDN southbound and data plane communication with IBC," *Mobile Information Systems*, pp. 1–12, 2016, doi: 10.1155/2016/1708970.
- [29] S. K. Debnath *et al.*, "Flight cost calculation for unmanned air vehicle based on path length and heading angle change," *International Journal of Power Electronics and Drive Systems (IJPEDS)*, vol. 11, no. 1, pp. 382–389, Mar. 2020, doi: 10.11591/ijpeds.v11i1.pp382-389.
- [30] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 487–497, Jun. 2017, doi: 10.1109/TNSM.2017.2701549.





- [31] X. Zhang, H. Wang, and H. Zhao, "An SDN framework for UAV backbone network towards knowledge centric networking," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs)*, Apr. 2018, pp. 456–461, doi: 10.1109/INFCOMW.2018.8406959.
- [32] C. Guerber, N. Larriou, and M. Royer, "Software defined network based architecture to improve security in a swarm of drones," in *2019 International Conference on Unmanned Aircraft Systems*, Jun. 2019, pp. 51–60, doi: 10.1109/ICUAS.2019.8797834.
- [33] R. Sairam, S. S. Bhunia, V. Thangavelu, and M. Gurusamy, "NETRA: Enhancing IoT security using NFV-based edge traffic analysis," *IEEE Sensors Journal*, vol. 19, no. 12, pp. 4660–4671, Jun. 2019, doi: 10.1109/JSEN.2019.2900097.
- [34] T. Alladi, V. Chamola, N. Naren, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Computer Communications*, vol. 160, pp. 81–90, Jul. 2020, doi: 10.1016/j.comcom.2020.05.025.
- [35] N. Hu *et al.*, "Building agile and resilient UAV networks based on SDN and blockchain," *IEEE Network*, vol. 35, no. 1, pp. 57–63, Jan. 2021, doi: 10.1109/MNET.011.2000176.
- [36] M. Hamburg, "Ed448-Goldilocks, a new elliptic curve," *IACR Cryptology ePrint Archive*, vol. 2015, p. 625, 2015, [Online]. Available: <http://eprint.iacr.org/2015/625>
- [37] P. Sasdrich and T. Güneysu, "Cryptography for next generation tls: Implementing the rfc 7748 elliptic curve448 cryptosystem in hardware," in *Proceedings of the 54th Annual Design Automation Conference 2017*, Jun. 2017, pp. 1–6, doi: 10.1145/3061639.3062222.
- [38] A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "Towards a security reference architecture for NFV," *Sensors*, vol. 22, no. 10, p. 3750, May 2022, doi: 10.3390/s22103750.
- [39] M. M. Sajjad, D. Jayalath, Y.-C. Tian, and C. J. Bernardos, "ZSM-based management and orchestration of 3GPP network slicing: An architectural framework and deployment options," 2022, [Online]. Available: <http://arxiv.org/abs/2203.12775>
- [40] A. Sharma and P. K. Singh, "UAV-based framework for effective data analysis of forest fire detection using 5G networks: An effective approach towards smart cities solutions," *International Journal of Communication Systems*, pp. 1–23, Apr. 2021, doi: 10.1002/dac.4826.
- [41] Y. A. A. S. Aldeen and H. M. Abdulhadi, "Data communication for drone-enabled internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 1216–1222, May 2021, doi: 10.11591/ijeecs.v22.i2.pp1216-1222.

BIOGRAPHIES OF AUTHORS







Ahssan Ahmed Mohammed Lehmoud     received his BS in computer science from University of Babylon in Iraq 2006. From 2009 to 2011, he completed his master's study in Computer Science from the Department of Computer Science and Information Technology at Dr. BabaSahib Ambedkar Marthwada University, India. He received the Ph.D thesis in information technology from the Department of Software College of Information Technology University of Babylon, Iraq, in April 2018. He is lecturer in the Babylon Education Directorate since 2008 till now. His research interests include the information security, network security, cryptography, steganography, image processing, and data mining. He can be contacted at email: ahssan_ahsan@bab.edu.gov.iq.



Nawfal Turki Obeis     received his BS and MSc in computer science from University of Babylon in Iraq in 2005 and 2013, respectively. From 2005 to 2011, he worked as a lecturer in the Faculty of Sciences at the Department of Computer Science in the University of Babylon. In September 2014, he enrolled in the Faculty of Information Technology at the Department of Software, University of Babylon, Babylon, Iraq as a Ph.D student. At April 2019, he received his Ph.D. At 2019, he started working as a lecturer in the Faculty of Information Technology at the Department of Information Networks in the same university, in addition to participating in the discussion of many master's theses, as well as the administrative and scientific committees. His research interest includes information security and networking. He can be contacted at email: nawfal.aljumaili@uobabylon.edu.iq.



Ahmed Fakhir Mutar     received his BS and M.Sc in computer science from University of Babylon in Iraq in 2008 and M.Sc in computer science in Mustansiriyah University in Iraq in 2018, respectively. From 2018 to 2022, he worked as a lecturer in Department of Computer Technology Engineering in the AL-Mustaqbal College of Babylon. In February 2019, he started working as a lecturer a lecturer in the Babylon Education Directorate since 2009, in addition to participating in the administrative and scientific committees. His research interest includes information security and image processing, computer network. He can be contacted at email: ahmedfakhir.mo@bab.edu.gov.iq.