DMAV: Enhanced MAV Link Protocol Using Dynamic DNA Coding for Unmanned Aerial Vehicles

https://doi.org/10.3991/ijoe.v18i11.34085

Ghada Emad Kassim[1,2](✉), Soukaena Hassan Hashem[2]
[1] University of Information Technology and Communications, Baghdad, Iraq
[2] University of Technology, Baghdad, Iraq
ghada.emad@uoitc.edu.iq

Abstract—In the modern era, new and innovative ways of securing data and communications are continuously developing. One such recent development is using the concept of DNA as a means of data encryption. In this work, we propose a new approach to encrypt data and communications on the MAVLink protocol for unmanned aerial vehicles (UAVs) using a lightweight GIFT algorithm and dynamic DNA coding (with binary bits). MAVLink is a communication protocol for UAVs, which is currently unencrypted and can easily be intercepted by anyone. As such, a secure MAVLink protocol has long been needed in the UAV industry. We describe a novel secure communication protocol for UAVs using dynamic DNA coding to encrypt MAVLink packets, which we call DMAV. Experimental results show that this novel means of securing the MAVLink protocol performs better than the traditional method (i.e., using public and private key cryptography). Therefore, the proposed approach could potentially change the way secure communications are conducted between UAVs in the future.

Keywords—Mavlink, DNA coding, lightweight cryptography, UAV's, secure communication

1 Introduction

Unmanned aerial vehicles (UAVs; sometimes known as drones) have grown increasingly prevalent in recent years [1]. An unmanned aerial vehicle is an aircraft that is not flown by a person. This term is typically used to describe aerial vehicles that are not traditional airplanes [2]. Many people think of drones when they hear the term UAV, but UAVs also refer to UAS and SSTs, among others. UAS refers to a broader category of aircraft than just drones [3]. By widening their military capabilities to include civilian service, these aircraft are being exploited globally. UAVs can be flown remotely or autonomously, conduct a range of missions, and may be equipped with a variety of sensors [4]. They are generally much cheaper to operate than piloted aircraft. In the future, UAVs are likely to become even more common [5], with many companies using them to deliver packages and perform inspections [6]. Their ability to deliver products and services to hard-to-reach areas has led to an explosion in their civilian use. At present, a member of the public can order an unmanned aerial vehicle (UAV) from Amazon, watch YouTube videos of drones flying around, or even build their own from scratch. Despite their prevalence in popular culture and the mainstream, however, UAVs are still relatively new [7]. An unmanned aerial vehicle is part of an unmanned aerial system (UAS); a base station/ground control station (GCS), UAV, and communication system together constitute the unmanned aerial system [8]. MAVLink, UAVCan, and UranusLink are three widely used UAV-to-GCS communication protocols. As the most common and widely used communication protocol for UAVs and ground control stations, MAVLink is supported by many UAVs[9]. It was developed by Lorenz Meier in 2009 and released under a GPL license. MAVLink allows a GCS and UAV to communicate in both directions. Instructions and control messages are sent from the GCS to the UAV, while the UAV sends telemetry and other status information back to the GCS [10]. Unmanned aerial vehicles may also communicate with one another using the MAVLink protocol [10]. A number of unmanned aerial vehicles (UAVs) and autopilot systems, such as Ardupilot and PX4, can communicate through the MAVLink protocol. With the aid of these autopilot systems, unmanned aerial vehicles (UAVs) can fly and navigate on their own [11]. The MAVLink protocol is also used to communicate between UAVs and other devices, such as sensors [12]. UAVs use the MAVLink protocol to send flight data to other UAVs to help avoid crashes, and sensor data to other devices, which can be used to increase the effectiveness of a given mission. In summary, MAVLink is an open-source and cross-platform lightweight networking technology [13]. MAVLink 2.0 uses timestamped hash-based message authentication codes (HMACs) for message integrity and authentication[14]. It uses a Marshalling library, which implies that system status messages and the instructions necessary to execute in a particular binary format are serialized (as byte streams), regardless of the platform. Binary serialization allows for small messages to be sent through a variety of wireless networks, including Wi-Fi and even serial telemetry systems with low data rates [15]. These features have led to the widespread adoption of MAVLink as a communication protocol between autonomous vehicles and ground control stations (GCS). While MAVLink is the most durable and widely used protocol for UAV communications, it has security issues that leave it open to several types of assault, including distributed denial of service (DDoS), listening in, and man-in-the-middle (MITM) attacks [16]. These weaknesses arise because the MAVLink protocol does not encrypt messages in transit. As binary communications between the GCS and the UAV occur through an unencrypted channel, the latter is an obvious target for numerous security threats. For this reason, unmanned aerial vehicles are at risk of being compromised [17]. One of the most exciting areas in the world of information technology is the field of DNA cryptography [18]. DNA cryptography is a method that uses DNA as an information carrier to protect sensitive information. In biological science[19], DNA is the repository of genetic information that is passed from one generation to the next [20]. This genetic information is what makes each individual unique[20]. DNA cryptography is inspired by biological processes such as DNA [21] replication and transcription, which are used to carry out processes in living cells and are responsible for the propagation of genetic information from one generation to the next [22]. DNA is ideal for carrying and protecting information, due to its unique chemical composition, which makes it a very robust medium with which to store data. The structure of DNA is made up of a series of four possible nucleotides, which are joined together in a chain [23]. In this paper, a dynamic DNA-based GIFT technique is adopted to encrypt MAVLink packets and provide the user with protected, secure original data. The security requirements of confidentiality, integrity, availability, authentication, and confidentiality are all achieved through this novel approach. The main contribution of this paper is the identification of a new way of using dynamic DNA with MAVLink to secure direct communication between a UAV and a ground control system. The proposed scheme provides a robust and secure way to transfer data between a UAV and a ground control system with a high data rate, while the communication channel is designed such that only authorized parties can access it. The UAV is equipped with a genetic encoder that changes its genetic sequence at regular intervals. This paper presents the first use of DNA to construct molecular bonds between UAVs and ground control systems.

1. We propose the DMAV protocol to secure the communication channel between a UAV and a GCS.
2. We develop the lightweight D: GIF algorithm to encrypt a MAVLink payload, in order to ensure secure communications between a UAV and a GCS.

The remainder of this paper is structured as follows: Section 2 provides a more in-depth look at the MAVLink communication protocol. Section 3 discusses the MAVLink protocol's security flaws. Section 4 describes the use of DNA encryption methods to exploit security flaws and vulnerabilities. Section 5 proposes a way to secure the MAVLink communication protocol; our encryption method and security measures are also described in this section. Section 6 provides the experimental results regarding the performance of our proposed approach and efficiency benchmarking against the original MAVLink protocol. Finally, our conclusions are offered in Section 7.

2 MAVLink protocol

In the application layer, the MAVLink protocol specifies both the message composition and how messages are serialized. When a data structure or object state is serialized, it can be later saved or distributed in a different format. These serialized messages are then passed to the lower levels—namely, the transport layer and physical layer—for transmission through the network. A variety of transport layers are supported, due to the lightweight construction of MAVLink; for example, TCP/IP, Wi-Fi, or reduced serial sensor networks at 915 MHz are all options for transmitting the MAVLink protocol through sub-GHz frequencies [24]. To stream MAVLink communications across IP networks, the second alternative is to use a standard Wi-Fi or Ethernet network interface. Both UDP and TCP are accepted by the MAVLink autopilot at the transport layer, depending on the program settings [25]. Client-server communication is not required to run a program user–agent program Protocol (UDP)[26]. As a result, it may be unreliable when it comes to sending messages. Nevertheless, MAVLink provides a quick and lightweight option for real-time, loss-tolerant streaming communication [27]. TCP is a connection-oriented protocol, unlike

UDP, which ensures that it should be used in a network and can be used to verify that a request has been submitted and/or received. This signifies that the TCP protocol has been overtaken as a reliable communication tool. The user must select the best option, based on their own needs, when deciding between a TCP or UPD protocol. Binary serialized data are used for communications between a UAV and the ground station [28]. For bidirectional communication, serialization and deserialization of the message are required. The sender and recipient are responsible for these actions. When compared to alternative methods of serialization, fewer transmission messages are required when using MAVLink serialization. MAVLink, MAVLink 1.0, and MAVLink 2.0 [29] are the current versions of the protocol. However, there exists an alternative: sMAVLink, MAVLink's alias. To the best of our knowledge, sMAVLink has not yet been deployed [30].

3 MAVLink protocol security concerns

Even though the study and development of unmanned systems are still at an early stage, a great deal of effort is being put forward. This has been seen as a chance for hackers and attackers to simultaneously exploit new faults and jeopardize the security of these systems [30], with varying objectives. Numerous contributions have been made by researchers working to improve security. One of the limitations of these security solutions for unmanned systems is that they are still in the early stages of implementation or proposal [31]. Before a solution can be found, it is necessary to understand the weaknesses of the MAVLink protocol [32] leading to difficulty in securing the network. Security concerns for the MAVLink protocol are discussed in the following sections. Furthermore, security factors are grouped into two categories: (1) Security requirements and (2) security threats/attacks [14]. This is expected to be beneficial to practitioners and academics working towards the construction of unmanned vehicle security frameworks and aerial vehicle threat models in the future [22].

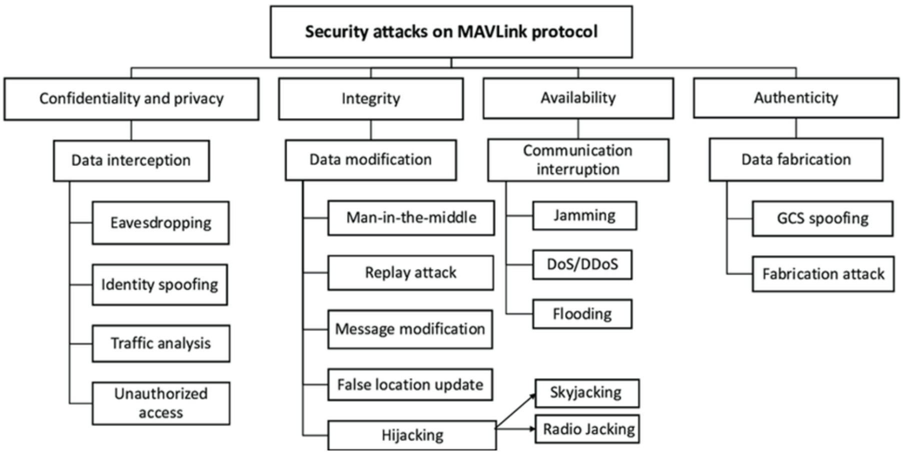

Fig. 1. MAVlink security attacks [31]

4 Security of drone communications

There is a considerable possibility of harm being caused to UAVs by flying objects; hence, UAV protection and safety concerns must be considered [32]. It is possible for hackers to quickly control a UAV, disrupting its ability to accomplish its mission or otherwise wreaking havoc. As a result, enhanced UAV security is an absolute necessity [33]. Vendors of drones currently focus on frequency hopping, spectrum dispersion, and key sharing as aggressive security measures. Only ISM bands (e.g., the 2.4 GHz band) and packet-based transfer methods (networking technologies) are legally permitted for service providers[34]. Protocols such as IPv4 share many similarities, but lack security measures, rendering them susceptible to known attacks [31]. Figure 2 depicts the connectivity within a UAV system.

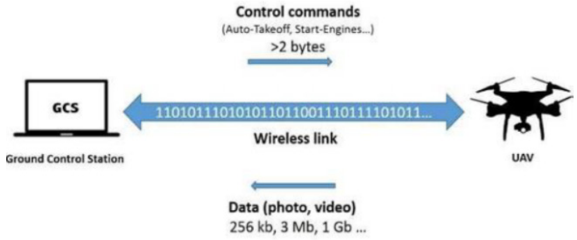

Fig. 2. UAV communication link [35]

The wireless networking technology called MAVLink (short for Micro Air Vehicle Link) enables entities to communicate with one another. Bidirectional communication between a ground control station and a drone is possible through the use of this technology [36]. The GCS instructs and controls the drone, while the drone feeds telemetry and status data back to the GCS. Lorenz Meier first published MAVLink for real-time applications in early 2009, under the terms of a Lesser General Public License [37]. Up to 255 aircraft can be supported by a single GCS using MAVLink. With a full payload, the MAVLink protocol has a maximum packet length of 263 bytes (i.e., no payload ACK). The MAVLink packet setup is depicted in Figure 3. The transfer of control and telemetry data necessitates a bidirectional link. The GCS receives data from the aerial vehicle and returns control information in the other direction n [15]. An error-correcting checksum is then sent through the contact channel, in the form of a byte-by-byte MAVLink message. If the checksums do not match, the message is deemed to be corrupt and is deleted from the system. The start of an encoded transmission is timed using a packet start sign (STX) in MAVLink [38]. The packet length (n) and checksum are checked after n bytes following the receipt of the packet start symbol. In this case, the decoded packet is processed, an ACK message is sent, and the process pauses until the next start sign is sent out. If the checksum is incorrect (e.g., due to tampered or missing message bytes), the packet is rejected, and the receiving system begins to look for the next start sign packet [39]. MAVLink assigns a sequence number (SEQ) to each packet as a security measure, in order to prevent packet loss. There is a limit to how far an unmanned aerial vehicle can fly if there is a high packet loss rate. Figure 3 [36]depicts the overall process.

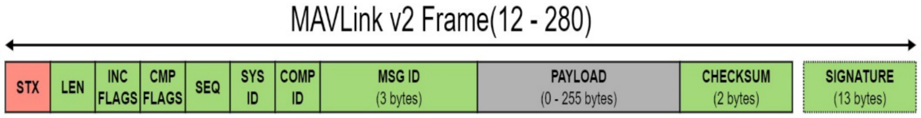

Fig. 3. MAVLink packet [31]

5 DMAV: Suggested protocol scheme

In this section, we discuss a method for ensuring the MAVLink protocol's security at runtime during a mission involving a UAV and a GCS. We suggest an entirely new approach, based on an existing cryptographic process. As depicted in Figure 4, a layer of security is added to the original MAVLink protocol. MAVLink packets cannot be restarted if they have been intercepted by any transmitter device, which means that the collected packets are of no value. The packets should be encrypted in such a way that, even if an intruder manages to capture one, they will not be able to decrypt the data within. A case study was considered to provide the findings described here. As previously mentioned, the experiment took place entirely online. Based on the use of drones for civilian purposes, we assumed that the mission would last more than 15 minutes and no more than 3 hours. The GCS and the UAV communicated by Wi-Fi. The suggested system presents a new way to construct a secure channel between drones and ground control stations, using dynamic DNA coding (with binary bits) in a lightweight algorithm. We propose the use of the lightweight DMAV protocol for encryption of the payload, in order to strengthen the security of the proposed authentication method (see Figure 4). Initially, the D: GIFT lightweight encryption method is used to encrypt and decode the data. Dynamic DNA coding utilizing binary bits is more sophisticated than available alternatives, able to provide superior encryption and more scrambling, conserves drone resources such as time and energy, and strengthens the security of the micro aerial vehicle (MAV) communication protocol used to communicate between the GCS and the drone. The D: GIFT encryption algorithm employs the substitution permutation network (SPN) approach in symmetric key cryptography. There are two types of D: GIFT: GIFT-64/128 (64-bit block and 128-bit key) and GIFT-128/128 (128-bit block and 128-bit key). Each round in the D: GIFT block cipher consists of five operations: Sbox, DNA Encoding, Permutation, AddRoundKey, and Constant XOR. Analysis of transmission characteristics, memory utilization, and other metrics was conducted for optimal construction of the encryption and decryption techniques for the proposed protocol, as well as reasonable comparisons with other known implementations. Additionally, we included the encryption approach in the Mission Planner, in order to enable a secure connection between the SITL UAV autopilot and the ground control station, decrypt the acquired packet, and extract the original MAVLink message. To carry out the encryption procedure, an algorithm was designed. The Python language was used to code the proposed system. The pseudo-code for the algorithms is provided below in four sections: Algorithm 1, Encrypting the MAVLink packet; Algorithm 2, D:GIFT

Encryption; Algorithm 3, Decrypting the MAVLink packet; and Algorithm 4, D:GIFT Decryption.

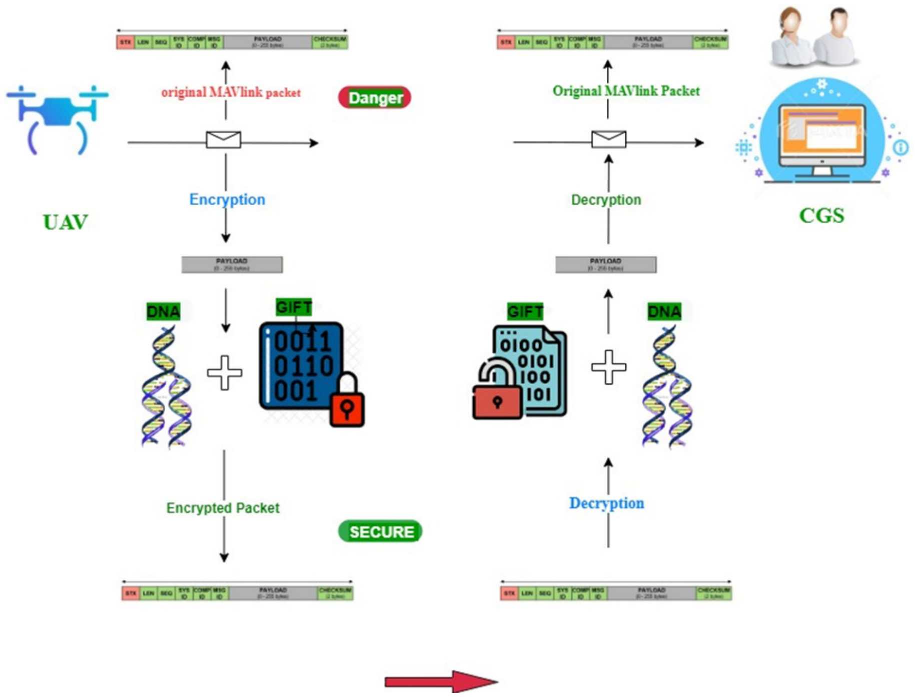

Fig. 4. Proposed DMAV protocol

```
Algorithm 1: mavlink_ packet_ Encrypting
Input: _Mavlink__Packets
Output: Encrypted_Mavlink_Packets
Procedure (Encryption_Mavlink)
 initialization DroneObject
 D0 = packet(data)
if (Packet_Count=RANGE)
 (Key = List)
 Pick← RandomIndex
 Key = Rand (Index)
 For (n = =char)
 if (Char= = Alphabet)
 D: GIFT_Encrypt (_ch)
 Else
 if (ch<= Num)
 D: GIFT_Encrypt (ch+2)
 Send Encrypted Packets
 End procedure
```

Algorithm 2: D: GIFT Encryption

```
Input: MAVlink Payload
   key bin 32bit
Output: Encryption payload
for each block do size 16bit
   Convert to hex for 4bit
   Change a bit from the key by using a Logistic map
   for each round do
      Sub Cells
      permute the bits
      permute DNA with a chaotic map
      Add Round Key
      Add constant
      key update
  end for
end for
```

Algorithm 3: Mavlink_ packet_ Decryption

```
Input: Encrypted _Mavlink_Packets
Output: _Encrypted_Mavlink_Packets
Procedure _(Encryption_Mavlink)
 initialization DroneObject
 D0 = packet(data)
if (Packet_Count=RANGE)
 (Key = List)
 Pick← RandomIndex
 Key = Rand (Index)
 For (n = ch)
 if (ch= Alphabet)
 DGIFT_decrypt (ch+2)
 Else
 if (ch ≤ Num)
 DGIFT_decrypt (char+2)
 Original MAVlink Packets
 End procedure
```

Algorithm 4: DGIFT Decryption

```
Input: input
    key bin
Output: Encryption image
Step1: compute and store the round keys
       For each R in rang(round)
         For each I in rang (32)
           Round key state[R][I] = key[i]
Step2: key update
       For each i in rang (32)
```

```
               Temp key[i] = key[(i+8) %32]
             For each I in rang (24)
               key[i] = Temp key[i]
      Step3: For each R in rang(round-1,0)
               Add Round Key
               key to key bits
               add round key
               add constant
               permute DNA with chaotic map
               Sub Cells
             End for
```

6 Performance evaluation

In this section, we present an evaluation of the MAVLink protocol in conjunction with our proposed encryption solution for protocol security. Furthermore, we assessed the results in terms of resource utilization (e.g., CPU processing speed and memory use). We compared our suggested protocol (DMAV) with the insecure original implementation in the MAVLink protocol. In comparison, our approach protected both the secrecy of communication between the UAV and the GCS, and the integrity of the data delivered. Thus, our technique securely encrypted the MAVLink packet without impairing its performance or efficacy. According to the results of the experiments, our technique transferred almost the same number of packets per second as the original; there was only a one or two packet difference between the two quantities. The number of packets sent per second with the original MAVLink protocol and with our method are shown in Figure 5.

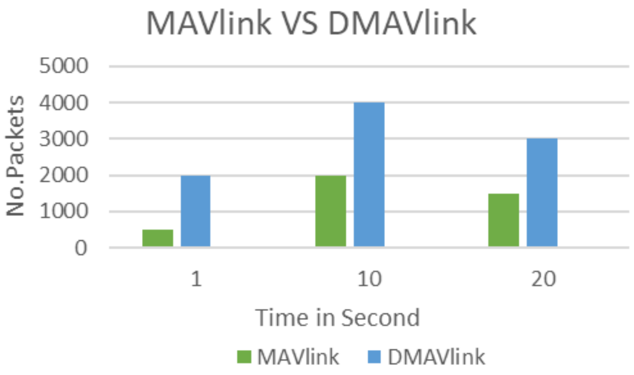

Fig. 5. MAVlink vs. proposed DMAV—number of packets over time

Another critical performance metric is memory utilization. The results indicated that the new approach consumed about the same amount of RAM as the original MAVLink, as shown in Figure 6.

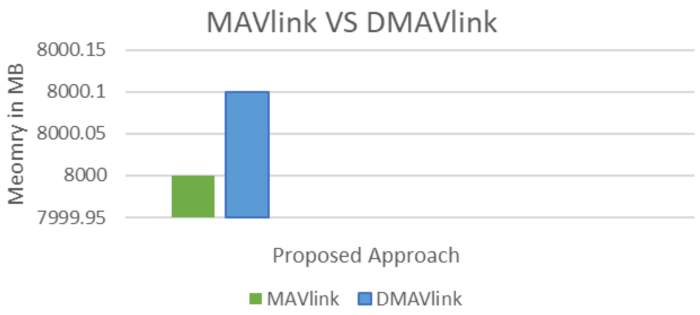

Fig. 6. MAVlink vs. DMAVlink—memory consumption

7 Conclusions

A new approach for protecting the MAVLink communication protocol was proposed in this paper. Dynamic DNA mapping and a lightweight cryptographic encryption technique served as the foundations of the proposed strategy. With this approach, an additional layer of security can be added to the MAVLink communication protocol, through encrypting the packet's payload. The MAVlink payload is encrypted utilizing DNA with binary bits and lightweight GIFT. A single pixel can be transformed into 8-bit binary bits, each of which may be encoded into a base using various rules controlled by a chaotic sequence. As the decoding process is the exact opposite of the encoding process, it is not addressed in this document. Ardupilot SITL, which uses the same autopilot as real planes and UAVs, was used to mimic the environment with a virtual UAV. The results demonstrated that our solution can protect communications without affecting the original protocol's performance or efficiency. Based on these findings, the proposed technique was compared to those in the existing literature (e.g., MAVsec) and benchmarked against the original insecure MAVLink protocol for validation. At present, it is best suited for missions ranging between 12 minutes and 2 hours in length. In future work, we intend to further develop the protocol in order to determine how much encryption to utilize, based on a mission's requirements.

8 References

[1] K. N. Qureshi, M. A. S. Sandila, I. T. Javed, T. Margaria, and L. Aslam, "Authentication scheme for Unmanned Aerial Vehicles based Internet of Vehicles networks," *Egypt. Informatics J.*, vol. 23, no. 1, pp. 83–93, 2022. https://doi.org/10.1016/j.eij.2021.07.001

[2] H. Noura *et al.*, "TRESC : Towards redesigning existing symmetric ciphers To cite this version : HAL Id : hal-03549341 TRESC : Towards Redesigning Existing Symmetric Ciphers," 2022. https://doi.org/10.1016/j.micpro.2020.103478

[3] A. Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, "A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook," *Ad Hoc Networks*, vol. 130, pp. 1–30, 2022. https://doi.org/10.1016/j.adhoc.2022.102790

[4] X. Gao, Y. Huo, Q. Gao, H. Zhao, and L. Ma, "Research Article A Secure Downlink Transmission Scheme for a UAV-Assisted Edge Network," vol. 2022, 2022. https://doi.org/10.1155/2022/5390771

[5] M. K. Abdul-Hussein, O. Strelnytskyi, I. Obod, I. Svyd, and H. T. S. ALRikabi, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare," *Int. J. online Biomed. Eng.*, vol. 18, no. 3, pp. 43–59, 2022. https://doi.org/10.3991/ijoe.v18i03.28015

[6] K. M. Ali Alheeti, M. S. Al-Ani, A. K. N. Al-Aloosy, A. Alzahrani, and D. A. S. Rukan, "Intelligent mobile detection of cracks in concrete utilising an unmanned aerial vehicle," *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 176–184, 2022. https://doi.org/10.11591/eei.v11i1.2987

[7] C. B. Le and D. T. Do, "Employing non-orthogonal multiple access scheme in uav-based wireless networks," *Bull. Electr. Eng. Informatics*, vol. 10, no. 1, pp. 241–248, 2021. https://doi.org/10.11591/eei.v10i1.2102

[8] B. Shang, "Unmanned Aerial Vehicles and Edge Computing in Wireless Networks," 2022.

[9] S. Samanth, P. K V, and M. Balachandra, "Security in Internet of Drones: A Comprehensive Review," *Cogent Eng.*, vol. 9, no. 1, 2022. https://doi.org/10.1080/23311916.2022.2029080

[10] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks," *Drones*, vol. 6, no. 1, pp. 1–19, 2022. https://doi.org/10.3390/drones6010010

[11] P. R. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES Int. J. Artif. Intell.*, vol. 11, no. 2, p. 504, 2022. https://doi.org/10.11591/ijai.v11.i2.pp504-515

[12] V. Simadiputra and N. Surantha, "Rasefiberry: Secure and efficient raspberry-pi based gateway for smarthome iot architecture," *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 1035–1045, 2021. https://doi.org/10.11591/eei.v10i2.2741

[13] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," *IEEE Access*, vol. 7, pp. 87658–87680, 2019. https://doi.org/10.1109/ACCESS.2019.2924410

[14] S. A. S. Alkadhim, "Communicating with Raspberry Pi via MAVLink," *SSRN Electron. J.*, 2019. https://doi.org/10.2139/ssrn.3318130

[15] A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 621–628. https://doi.org/10.1109/IWCMC.2019.8766667

[16] L. Chaari, S. Chahbani, and J. Rezgui, "MAV-DTLS toward Security Enhancement of the UAV-GCS Communication," *IEEE Veh. Technol. Conf.*, vol. 2020-Novem, pp. 0–4, 2020. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348584

[17] L. Chaari, S. Chahbani, and J. Rezgui, "Vulnerabilities assessment for unmanned aerial vehicles communication systems," *2020 Int. Symp. Networks, Comput. Commun. ISNCC 2020*, 2020. https://doi.org/10.1109/ISNCC49221.2020.9297293

[18] L. Muflikhah, M. A. Rahman, and A. Wahyu Widodo, "Profiling DNA Sequence of SARS-Cov-2 Virus Using Machine Learning Algorithm," *Bull. Electr. Eng. Informatics*, vol. 11, no. 2, pp. 1037–1046, 2022. https://doi.org/10.11591/eei.v11i2.3487

[19] N. Alseelawi, H. T. Hazim, and H. T. S. ALRikabi, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *Int. J. online Biomed. Eng.*, vol. 18, no. 3, pp. 114–133, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[20] S. A. Kadum, A. Y. Al-Sultan, and N. A. Hadie, "Data protection based neural cryptography and deoxyribonucleic acid," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 3, pp. 2756–2764, 2022. https://doi.org/10.11591/ijece.v12i3.pp2756-2764

[21] I. A. Aljazaery, H. T. S. ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *Int. J. online Biomed. Eng.*, vol. 18, no. 3, pp. 101–113, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[22] N. A. Hussein and M. I. Shujaa, "DNA computing based stream cipher for internet of things using MQTT protocol," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 1035–1042, 2020. https://doi.org/10.11591/ijece.v10i1.pp1035-1042

[23] A. Raj, "CRYPTOGRAPHY ALGORITHM USING," no. June, 2021.

[24] M. A. Husman *et al.*, "Unmanned aerial vehicles for crowd monitoring and analysis," *Electron.*, vol. 10, no. 23, pp. 1–18, 2021. https://doi.org/10.3390/electronics10232974

[25] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, A. A. Almazroi, and A. A. Almazroi, "A secure communication protocol for unmanned aerial vehicles," *Comput. Mater. Contin.*, vol. 70, no. 1, pp. 601–618, 2021. https://doi.org/10.32604/cmc.2022.019419

[26] R. Mitra and R. Ganiga, "A novel approach to sensor implementation for healthcare systems using internet of things," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5031–5045, 2019. https://doi.org/10.11591/ijece.v9i6.pp5031-5045

[27] H. G. Hamid and Z. T. Alisa, "Survey on IoT application layer protocols," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1663–1672, 2021. https://doi.org/10.11591/ijeecs.v21.i3.pp1663-1672

[28] P. Visconti, R. Velazquez, C. Del-Valle-Soto, and R. De Fazio, "FPGA based technical solutions for high throughput data processing and encryption for 5G communication: A review," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 4, pp. 1291–1306, 2021. https://doi.org/10.12928/telkomnika.v19i4.18400

[29] R. Jyothi and N. G. Cholli, "An efficient approach for secured communication in wireless sensor networks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 1641–1647, 2020. https://doi.org/10.11591/ijece.v10i2.pp1641-1647

[30] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, and A. Nayyar, *Emerging use of UAV's: secure communication protocol issues and challenges*, no. January. Elsevier Inc., 2020. https://doi.org/10.1016/B978-0-12-819972-5.00003-3

[31] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," *IEEE Access*, vol. 7, no. 8, pp. 87658–87680, 2019. https://doi.org/10.1109/ACCESS.2019.2924410

[32] M. Usman, "Lightweight Encryption for the Low Powered IoT Devices," 2020, [Online]. Available: http://arxiv.org/abs/2012.00193

[33] A. Hamza, U. Akram, A. Samad, S. N. Khosa, R. Fatima, and M. F. Mushtaq, "Unmaned Aerial Vehicles Threats and Defence Solutions," *Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020*, 2020. https://doi.org/10.1109/INMIC50486.2020.9318207

[34] J. N. Yasin, S. A. S. Mohamed, M. H. Haghbayan, J. Heikkonen, H. Tenhunen, and J. Plosila, "Unmanned Aerial Vehicles (UAVs): Collision Avoidance Systems and Approaches," *IEEE Access*, vol. 8, pp. 105139–105155, 2020. https://doi.org/10.1109/ACCESS.2020.3000064

[35] H. M. Ismael, Z. Tariq Mustafa Al-Ta, and A. Emails mordasshani, "Authentication and Encryption Drone Communication by Using HIGHT Lightweight Algorithm," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 11, pp. 5891–5908, 2021, [Online]. Available: https://www.turcomat.org/index.php/turkbilmat/article/view/6875

[36] J. Khan *et al.*, "Medical Image Encryption into Smart Healthcare IOT System," *2019 16th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. ICCWAMTIP 2019*, no.

September 2021, pp. 378–382, 2019. https://doi.org/10.1109/ICCWAMTIP47768.2019.9067592

[37] D. Popescu, F. Stoican, G. Stamatescu, O. Chenaru, and L. Ichim, "A survey of collaborative UAV-WSN systems for efficient monitoring," *Sensors (Switzerland)*, vol. 19, no. 21, pp. 1–40, 2019. https://doi.org/10.3390/s19214690

[38] S. Maitra and K. Yelamarthi, "Rapidly deployable IoT architecture with data security: Implementation and experimental evaluation," *Sensors (Switzerland)*, vol. 19, no. 11, 2019. https://doi.org/10.3390/s19112484

[39] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Networks*, vol. 86, no. November, pp. 72–82, 2019. https://doi.org/10.1016/j.adhoc.2018.11.010

9 Authors

Ghada Emad Kassim is with University of Information Technology and Communications, Baghdad, Iraq (email: ghademad@uoitc.edu.iq).

Soukaena Hassan Hashem is with University of Technology, Baghdad, Iraq.

Article submitted 2022-06-18. Resubmitted 2022-07-20. Final acceptance 2022-07-21. Final version published as submitted by the authors.