Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 205 (2022) 50–57

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Military Communications and Information Systems (ICMCIS 2022)

A Secure Real-time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain

Niccolò Cecchinato[a]*, Andrea Toma[a], Carlo Drioli[a], Giuseppe Oliva[a], Gianluigi Sechi[a], Gian Luca Foresti[a]

[a]*Department of Mathematics, Computer Science and Physics, University of Udine, via delle Scienze 206, Udine 33100, Italy*

Abstract

This article proposes a framework of application-level security, an HW-SW implementation of a low-cost solution for real-time multimodal data encryption and decryption for security applications in protected environments like espionage, situational awareness, monitoring, and counter-UAV. Data is captured from drones equipped with microphone arrays and cameras. This is performed by exploiting acoustic event analysis, video tracking, and recognition, performed on a ground station. All the communications are delivered in a secure data channel. Integrity and secrecy of the sensitive data acquired by drones must be guaranteed until the data is delivered in real-time from UAVs to the destination node. A possible data exploit may cause critical problems if the data is intercepted by malicious attackers. Being the drones equipped with low energy consuming devices with low computational power, like single-board-computers, a real-time lightweight application-level AES encryption, in addition to the MAC encryption of the wireless communication channel, has been considered. In the experiment, the encryption and decryption process has been optimized, even under adverse transmission conditions ensuring continuous data encryption even if some packets are lost or the connection is repeatedly dropped and reestablished.

© 2022 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the International Conference on Military Communications and Information Systems

Keywords - secure multimedia streaming, AES encryption, UAV network, UAV security, multimedia data encryption

* Corresponding author. Tel.: +39-320-8072274
E-mail address: niccolo.cecchinato@gmail.com.

1877-0509 © 2022 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the International Conference on Military Communications and Information Systems
10.1016/j.procs.2022.09.006

1. Introduction

Unmanned Aerial Vehicles (UAVs), or drones, are aircraft without an onboard pilot that are remotely controlled by a ground-based operator. Recently, this technology has been attracting growing attention in military applications from defense to armed strikes and employed by a growing number of states worldwide. UAVs were originally developed as test dummies for aircraft at the start of the 20th century and saw incidental use in target training and as decoys [1]. Their usage intensified in later years when UAVs were employed for Intelligence, Surveillance and Reconnaissance (ISR). Since the start of the 21st-century, they have been armed for striking targets. In this work, we basically focus on unarmed military UAVs for patrolling and defense operational military applications. In [2], the risks of military UAVs being subjected to cyber and electronic attacks are considered, especially high-profile incidents such as the interception of unencrypted multimedia data from UAVs, which imposes an indirect security and safety threat. Lack of security measures to protect UAVs greatly exposes them to cyber and electronic attacks, with the consequent likelihood of unauthorized use or interception of confidential data. Protection of military UAVs means defense against sophisticated cyber or electronic attacks, including data link interceptions and navigational spoofing. This requires offensive activity to counter adversary drone operations. In military operations, this is called cyber power.

The main application for which we conducted this work is counter-UAV [3] for anti-UAV monitoring strategies against illegal use of UAVs and external UAV attacks [4,5] even in hostile environments. We aim at designing a proactive counter-UAV system to protect army tanks and patrols from aerial attacks launched by UAVs in non-protected urban areas [1]. In this framework, monitoring and analysis of the acoustic and video scene by using microphone arrays and cameras is undoubtedly of fundamental importance.

In the literature, multimedia data streaming architectures have recently been investigated in multiple node scenarios. In [6], the authors propose a high-level architecture in a collaborative UAV system with autonomous drones equipped with onboard sensors and embedded processing and networking algorithms with applications to disaster assistance, search and rescue, or aerial monitoring. Experiments on data acquisition from remote sensors have been conducted in [7] where the authors introduce an aerial ad-hoc network for video streaming and both source and receiver nodes are mobile. In our work, we considered a distributed sensor network with flying remote nodes with the objective of collecting not only video data but also audio data from the environment to be monitored. In Figure 1 we customized a DJI MATRICE 100 equipping it with a multimedia sensor frame composed by a circular microphone array and a camera in order to detect and localize approaching entities in the surroundings [8, 9].

Figure 1 - MATRICE 100 drone with counter-UAV A/V sensors

Any intruded UAV can in this way be detected and recognized by analyzing both the captured video images of the UAV and audio recordings of its propeller's noise. For the purpose of this task, the multimedia data collected onboard is transmitted to a ground control unit, through a Wi-Fi communication network, that gathers the data from all the remote nodes and processes it. Only small-size microphone arrays, cameras and embedded computers are mounted on the acquisition UAVs, due to the payload constraints of the UAVs. An access point on the ground control station receives the streams. The 5 GHz band of the 802.11ac is used since it is suitable for real-time multimedia data streaming and guarantees a high data-rate with low packet loss. Precisely because of the broadcast nature of the wireless communications, the streaming process is extremely vulnerable to external cyber-attacks.

Reducing the risk of cyber-attacks is definitely essential, especially in the military domain. This is a fundamental point in the research community and largely considered in the literature as in [10-16]. Nowadays, securing multimedia data deserves particular attention.

The use of encryption in multimedia has become a necessary step in order to protect and guarantee the confidentiality of the data transmitted. Leong et al. in [17] created a UAV sensor network with three drones for urban surveillance, as illustrated in the first picture of their paper. In this network, there is both video and control data transmission through wireless connectivity. To ensure secure data communication, a cryptography algorithm can be applied to this scenario. In our work, for the specific case in use, a correct data encryption algorithm must be used according to the multimedia application of the drone system. A real-time audio and video encryption is considered where data is encrypted using the Advanced Encryption Standard (AES) symmetric encryption algorithm, which guarantees a fast encryption process suitable for real-time applications and embedded systems. The aim of this task was to find a method to send multimedia streams over the network in a protected and encrypted way, using a fast encryption algorithm that did not aggravate the computational process and that allowed immediate and real-time data transmission. In the literature, the AES cryptography technique is implemented in real-time systems for securing data in small scale networks like UAVs wireless communication systems [18]. In [19] a hybrid cryptographic security scheme based on AES-256 with simple computing but a high level of security is proposed. It is implemented on a Raspberry Pi device drone service. A security system based on FPGA implementation for multimedia applications is presented in [20] where the authors investigate methods to maintain a high level of data security with a low impact on WLAN system performance. Architecture for secure video transmission for UAV applications is proposed in [21] where the security encryption tasks are implemented on an onboard FPGA and the encryption algorithm is the AES. The authors in [22] presented a reliable algorithm for securing communications between UAV and ground station (GS) using the AES algorithm and a key generated from the operator's Electroencephalogram (EEG) signal for the Xbee wireless communication. They extend the protocol encryption scheme incorporating a message authentication code (MAC) generated from the shared 128-bit AES key. A Hardware Security Module based on the AES algorithm for UAV communication encryption is proposed in [23].

The main contribution introduced by our work is related to the design of an efficient, secure, fast and reliable streaming application for multimedia data captured by audio and video (A/V) sensors mounted on flying nodes. These UAVs are used for espionage, interceptions, patrolling tasks and to counter unauthorized approaching entities. The proposed algorithm suits lightweight, inexpensive embedded systems mounted on UAVs, that are poor in computational resources and with energy constraints and allow the secure transfer of confidential data.

The remaining part of this manuscript is organized as follows: a detailed description of multimodal data encryption with AES is provided in Sec. II; the experiments with the results are in Sec. III; finally, Sec. V concludes the manuscript with some ideas for future work.

2. Multimedia Data Encryption with AES

The goal of this work was to identify a technique to deliver multimedia streams over the network in a secure and encrypted mode, utilizing a fast encryption algorithm that did not slow down the computation of the drones' single-board computers and allowed for fast and real-time data transmission. The transmitting node acquires the multimedia

streams by peripherals, encodes and encrypts them, and then sends them via Transmission Control Protocol (TCP) sockets to the ground station. The GS receives the encrypted messages, decrypts them and plays them back. The encryption is done at application-level, which means that the data is transferred already encrypted across connections. The AES algorithm has various modes of operation. Due to the heterogeneity of sensors mounted on drones that produce a variable data length, this project required a mode that allowed dynamic data management, rather than a fixed one. The EAX mode (encrypt-then- authenticate-then-translate) has been employed. This method is also called nonce-based authenticated encryption with associated data (AEAD) and it is a pair of algorithms $\Pi = (E, D)$, where E is the encryption algorithm and D the decryption one. It is an online algorithm: it processes the data on-the-fly, not knowing a-priori the data length. Given a message M (of variable length), a nonce N (of any length, but typically 16byte in length) and a header H (of variable length, which can only be used once), the EAX mode protects the privacy of M and the authenticity of both M and H.

The mode uses $2\left\lceil\frac{|M|}{n}\right\rceil + \left\lceil\frac{|H|}{n}\right\rceil + \left\lceil\frac{|N|}{n}\right\rceil$ block-cipher calls, where n is the block length of the underlying block cipher (when these fields are nonempty). The block-cipher is $E: Key \times \{0,1\}^n \rightarrow \{0,1\}^n$, where *Key* is a finite, nonempty and $E_K(\cdot) = E(K, \cdot)$ is a permutation on $\{0,1\}^n$ [24].

The nonce is a fundamental element that is assigned to the payload of the data to be transmitted. This is a unique, pseudo-random value generated each time the algorithm is instantiated. It aims to prevent replay and dictionary attacks. For this project, to increase data security and authentication, a new nonce is generated after each sending of data from the network socket. This allows, at each socket send, to use every time a new pseudo-random value associated with the payload. This, even in the event of any disconnections or packet losses, allows decrypting subsequent packets independently once the connection is restored.

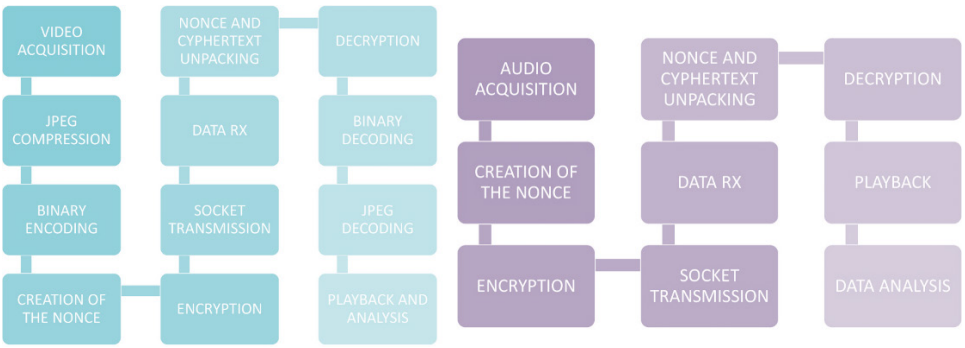

Figure 2. A/V Encryption processes

Figure 2 shows how the encryption and decryption processes work for both audio and video flows.

The elements that are needed for the encryption and decryption are: *i)* a key, that is chosen by the programmer and can be 128-192-256 bits long, *ii)* the header, *iii)* a nonce, *iv)* an authentication tag, also called the MAC, or integrity check value (ICV). It is generated during the final authentication of the message, thus when it is encrypted and digested and when the ciphertext is returned. All these elements generated by the sending node, must be sent to the ground station, together with the ciphertext. This will allow correct decryption of the multimedia flows. The GS at each received packet creates a new cipher using the nonce just received. In addition to the nonce, it also extracts from the network packets all the previously mentioned parameters and goes to decrypt the ciphertext using the same cipherkey of the drone. The GS also checks if the given MAC tag is legitimate. This controls if the message was encrypted with the correct key and no changes were made during the transmission. As soon as all these steps have been completed, the plain information is made available and sent to the next module of the application for playback.

3. Experiments and Results

In this part, a comparison between the encrypted data and the clear/decrypted data will be made, in order to verify and investigate the encryption algorithm's validity. The analyses were mainly performed on the audio, as it is easier to handle and visualize for results demonstrations. The effect that has been predicted on an encrypted audio stream was white noise, because Rijndael is a substitution and permutation network that assures the concept of diffusion and confusion. This, in the frequency domain, can be compared to a random signal having a constant spectral density. Therefore, during an audio stream two fragments of the same drone's microphone signal were recorded, before and after encryption. The generated, streamed and recorded audio was Pulse-code modulation (PCM) audio; therefore, two wave files were recorded. In Figure 3 it is possible to see the two spectrograms related to the decrypted and the encrypted signal; in particular, the latter can be compared to a white noise spectrogram. This makes it impossible to decrypt the signal both from a perceptual and computational point of view without having the cipher key and the other ciphering parameters. This technique prevents external attackers from sniffing packets and, consequently, extracting their payload with relevant and secret information.

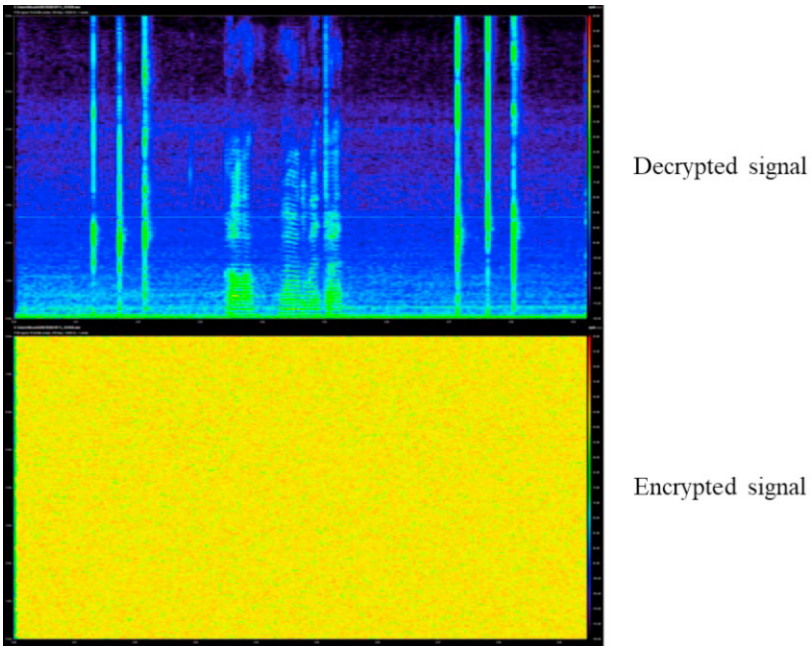

Figure 3. Spectrograms of the decrypted and encrypted transmitted audio feed

Regarding the video feed, being compressed in jpeg, it was impossible to properly view and reconstruct the encrypted frames as, undergoing repeated substitutions and permutations of the bits, the indexes of the jpeg markers have been lost, making the image undecodable.

The algorithm was tested also under adverse radio transmission conditions in a congested radio spectrum, with a weak radio signal and a low channel rate. The transmission was interrupted multiple times (Figure 4, points: from 1 to 3 and from 4 to 5) and the reception of the flows was regularly checked. The network software was developed so that when a disconnection occurs, the transmitter's TCP socket, not getting the confirmation ACK, waits for the transmission until the other node re-joins. During cryptography, the lack of data in the receiving ground station must be controlled effectively. Even if some packets are lost, or the connection is continuously broken and reestablished,

proper data management was adopted in order to always maintain continuous data encryption (Figure 4, points: from 3 to 5 and from 5 onwards). This was possible by generating and instantiating a new cipher with a new nonce and tag at each call of the while statement of the main sending loop. In doing so, each packet contains separate encrypted data allowing the GS to decrypt the subsequent packets correctly.

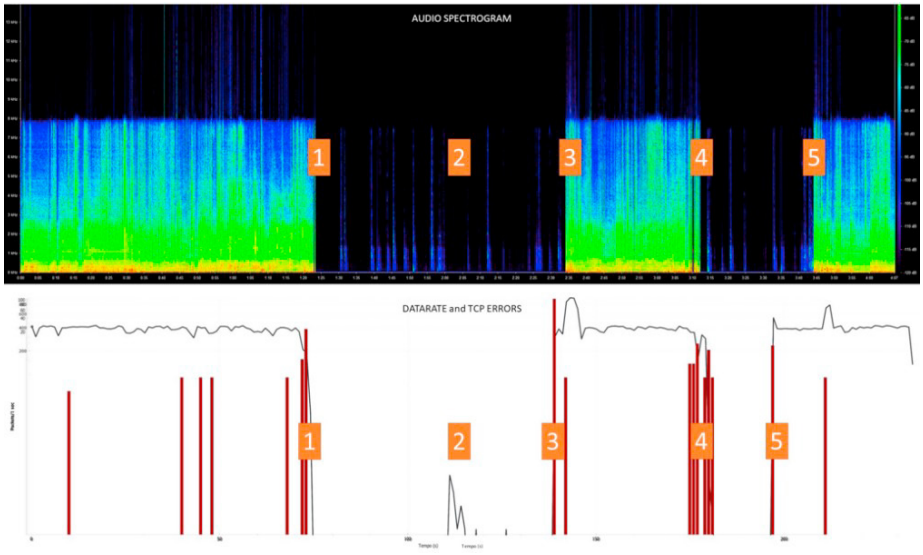

Figure 4. Audio and network analysis of the received flows under non-optimal transmission conditions.

The calculation of the execution times of the data encryption and decryption processes has been done, returning the results in Tab. 1. The times were calculated during a multi-channel (4-channel) audio streaming with the video feed.

Table 1. Execution times of the AES encryption/decryption processes

UAV Audio	UAV Video	GS Audio	GS Video
$1.759 \times 10^{-3} s$	$7.513 \times 10^{-3} s$	$4.223 \times 10^{-3} s$	$2.671 \times 10^{-3} s$

The obtained results showed how this algorithm, despite being performed at the application level, is light, fast, and suitable for low-power embedded devices mounted on drones. A higher execution value was found in the GS audio as the process for unpacking the payload and all parameters for decryption from the data string received from the socket requires some complexity.

4. Conclusions and Future Work

In this work, an application of securing multimedia data streaming from flying nodes in real-time is investigated using UAVs for security and surveillance tasks. The developed drones are equipped with A/V sensors as remote acquisition devices for ISR tasks and to counter unauthorized approaching entities. The proposed algorithm is based on AES cryptography and was implemented at application-level. It suits lightweight embedded systems mounted on UAVs that are not demanding in energy and computational resources. After introducing the general description of the usage of UAVs in military applications and the related multimedia data streaming, we focused on the securing of

multimedia data communications at the application-layer to protect the streaming system against attacks from unauthorized entities. Several experiments have been conducted to verify if the computing platforms mounted onboard the drones are able to guarantee a certain level of reliability and security. The results showed how high-quality multimedia data is efficiently encrypted and decrypted in real-time taking a small amount of time and also under adverse radio-link transmission conditions. The proposed algorithm is able to cipher data at each packet independently, so that even if the data is lost at some point, the subsequent chunks received can correctly be decrypted. As future work, a dynamic and coordinated keys management will be implemented.

Acknowledgements

This research was partially supported by Italian MoD project a2018-045 “A proactive counter-UAV system to protect army tanks and patrols in urban areas” (Proactive Counter UAV), and by the ONRG project N62909-20-1-2075 “Target Re-Association for Autonomous Agents” (TRAAA).

References

[1] H. Wang, H. Cheng, and H. Hao, "The Use of Unmanned Aerial Vehicle in Military Operations," In: Long S., Dhillon B.S. (eds) Man-Machine-Environment System Engineering, MMESE 2020, Lecture Notes in Electrical Engineering, vol 645, Springer, Singapore, https://doi.org/10.1007/978-981- 15-6978-4_108.

[2] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," In: 8th International Conference on Cyber Conflict (CyCon), 2016, pp. 205-221, doi: 10.1109/CYCON.2016.7529436.

[3] A. Toma, N. Cecchinato, C. Drioli, G.L. Foresti, G. Ferrin, "Towards drone recognition and localization from flying UAVs through processing of multi-channel acoustic and radio frequency signals: a deep learning approach," In: IST-190 Symposium on AI, ML and BD for Hybrid Military Operations (AI4HMO), 2021.

[4] Y. Kim, Y.G. Min, P.S. Hee, J. Wun-Cheol, S. Soonyong, and H. Tae-Wook, "The analysis of image acquisition method for anti-uav surveillance using cameras image," In: International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 549–554.

[5] H. Liu, Z. Wei, Y. Chen, J. Pan, L. Lin, and Y. Ren, "Drone detection based on an audio-assisted camera array," In: IEEE Third International Conference on Multimedia Big Data (BigMM), 2017, pp. 402–406.

[6] E. Yanmaz, S. Yahyanejad, B. Rinner, H. Hellwagner, C. Bettstetter, "Drone networks: Communications, coordination, and sensing," In: Ad Hoc Networks, 68, 1–15, 2018. https://doi.org/10.1016/j.adhoc.2017.09.001.

[7] R. Muzaffar, E. Yanmaz, C. Raffelsberger, C. Bettstetter, A. Cavallaro, "Live multicast video streaming from drones: an experimental study," In: Autonomous Robots, 44, 75–91, 2020.

[8] A. Toma, N. Cecchinato, C. Drioli, G.L. Foresti, G. Ferrin, "CNN-based processing of radio frequency signals for augmenting acoustic source localization and enhancement in UAV security applications," In: International Conference on Military Communication and Information Systems (ICMCIS), pp. 1–5, 2021, https://doi.org/10.1109/ICMCIS52405.2021.9486424.

[9] D. Salvati, C. Drioli, G. Ferrin, and G. L. Foresti, “Acoustic Source Localization From Multirotor UAVs,” In: IEEE Transactions on Industrial Electronics, vol. 67, no. 10, pp. 8618–8628, 2020, doi: 10.1109/TIE.2019.2949529.

[10] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," In: IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), 2017, pp. 194-199, doi: 10.1109/SSRR.2017.8088163.

[11] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," In: IEEE Conference on Technologies for Homeland Security (HST), 2012, pp. 585- 590, doi: 10.1109/THS.2012.6459914.

[12] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," In: Journal of Cyber Security Technology, 2021, 5:2, 120-137, DOI: 10.1080/23742917.2020.1846307.

[13] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," In: Internet of Things, vol. 11, 2020, https://doi.org/10.1016/j.iot.2020.100218.

[14] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," In: IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1773-1828, Secondquarter 2019, doi: 10.1109/COMST.2018.2878035.

[15] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis," 2022, In: ACM Comput. Surv., 55, 1, Article 21 (January 2023), 35 pages. DOI:https://doi.org/10.1145/3485272.

[16] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," In: Mobile Netw Appl, 25, 95–101 (2020). https://doi.org/10.1007/s11036-018-1193-x.
[17] W. L. Leong, N. Martinel, S. Huang, C. Micheloni, G. L. Foresti, and R. Teo, "Integrated Perception and Tactical Behaviours in an Auto-Organizing Aerial Sensor Network," In: 2020 International Conference on Unmanned Aircraft Systems (ICUAS), 2020, pp. 429-438, doi: 10.1109/ICUAS48674.2020.9214052.
[18] U. Arom-oon, "An AES cryptosystem for small scale network," In: Third Asian Conference on Defence Technology (ACDT), 2017, pp. 49-53, doi: 10.1109/ACDT.2017.7886156.
[19] F. Ronaldo, D. Pramadihanto, and A. Sudarsono, "Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network," In: International Electronics Symposium (IES), 2020, pp. 116- 122, doi: 10.1109/IES50839.2020.9231951.
[20] T. Hayajneh, S. Ullah, B. J. Mohd, and K. S. Balagani, "An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications," In: IEEE Systems Journal, vol. 11, no. 4, pp. 2536-2545, Dec. 2017, doi: 10.1109/JSYST.2015.2424702.
[21] D. Psilias, A. Milidonis, and I. Voyiatzis, "Secure Video Transmission System for UAV Applications," 2021, In: 25th Pan-Hellenic Conference on Informatics (PCI 2021). Association for Computing Machinery, New York, NY, USA, 318–322. DOI:https://doi.org/10.1145/3503823.3503882.
[22] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal," In: IEEE Access, vol. 6, pp. 22976-22986, 2018, doi: 10.1109/ACCESS.2018.2827362.
[23] K. Kim and Y. Kang, "Drone security module for UAV data encryption," In: International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 1672-1674, doi: 10.1109/ICTC49870.2020.9289387.
[24] M. Bellare, P. Rogaway, D. Wagner, "The EAX Mode of Operation," In: Roy B., Meier W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017, pp 389-407. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-25937-4_25.