Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack

Yucheng Li and Cong Pu
Department of Computer Sciences and Electrical Engineering
Marshall University, Huntington, WV 25755, USA
Email: {li160, puc}@marshall.edu

***Abstract*—Micro aerial vehicles, a.k.a. drones, have become an integral part of a variety of civilian and military application domains, including but not limited to aerial surveying and mapping, aerial surveillance and security, aerial inspection of infrastructure, and aerial delivery. Meanwhile, the security and privacy of drones are gaining significant attention due to both financial and strategic information and value involved in aerial applications. Due to the lack of security features in communication protocols, an adversary can easily interfere with on-going communications or even seize the control of drone. In this paper, we propose a lightweight digital signature protocol, also referred to as *DroneSig*, to protect drones from man-in-the-middle attack, where an adversary eavesdrops the communications between Ground Control Station (GCS) and drone, and impersonates the GCS and sends fake commands to terminate the ongoing mission or even take control over the drone. The basic idea of the DroneSig is that the drone will only execute the new command after validating the received digital signature from the GCS, proving that the new command message is coming from the authenticated GCS. If the validation of digital signature fails, the new command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position. We conduct extensive simulation experiments for performance evaluation and comparison with existing Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES). The simulation results show that the proposed DroneSig can achieve better performance in terms of energy consumption, computation time, CPU cycle, memory usage, and code size, indicating a viable and competitive approach defending drones against man-in-the-middle attack.**

***Index Terms*—Man-In-The-Middle Attack, Lightweight Digital Signature, Micro Aerial Vehicle, Drones, Internet of Drones**

I. Introduction

Micro aerial vehicles, a.k.a. drones, are flying robots endowed with the capabilities of sensing, computing, and wireless communicating, and becoming progressively popular in various civilian and military application areas, including but not limited to aerial surveying and mapping, aerial surveillance and security, aerial inspection of infrastructure, and aerial delivery [1], [2]. The global small drones market is projected to reach USD 40.31 billion by 2025, at a compound annual growth rate of 17.04% from 2018 to 2025 [3]. By 2026, commercial drones for both corporate and consumer applications will have an annual impact of $31 billion to $46 billion on the United States GDP [4]. As the drone-based civilian and military applications are proliferating, Internet of Drones (IoD), a layered aerial network management and control architecture, was proposed and has been demonstrated as an applicable architecture for coordinating the access of drones to controlled airspace and providing navigation services [5]. With the assistance of advanced communication technology as well as emerging computing infrastructure, we envision that drones will definitely find many new ways to improve the quality of our life in the near future [6].

Due to both financial and strategic information and value involved in aerial applications, however, drones look especially attractive to attackers and become an ideal target for various cyber attacks [7]. For example, in January 2016, Mexican drug traffickers used satellite navigation signal deception technology to send spoofed GPS signals to attack the U.S. border patrol drone in order to illegally cross the border. In December 2011, Iran successfully captured an U.S. Lockheed Martin RQ-170 Sentinel drone through spoofing the drone's GPS system. Nowadays, drones have started showing their impact in everyday life of ordinary people, and have been considered as a supplement of humans in a part of delivery in business. Business and technology giants like Amazon, Google, Facebook and Walmart have started delivering the products and services via drones for the speedy delivery and customary satisfaction. However, aerial drones applications are vulnerable to a myriad of cyber attacks targeting their communication links with Ground Control Station (GCS), as well as with other air units [8]. Therefore, investigating potential cybersecurity threats against drones and designing the state-of-the-art security mechanisms are the top priority to improve the security of drone applications.

Unfortunately, the open nature of wireless channel and the limited battery capacity, computing capability, and communication bandwidth make it become a highly challenging task [9]. Communication between drones and GCS is established by the communication protocol via a wireless channel, which makes them vulnerable to various attacks since the communication protocol does not support security procedures [10]. The GCS and drones exchange data through an unauthenticated wireless channel without encryption, thus, the data communication can be easily hacked. For example, an adversary can send unauthorized commands to the drone

978-0-7381-1116-2/20/$31.00 ©2020 IEEE
DOI 10.1109/CSE50738.2020.00020

to take its control from GCS, and then catch and withhold the drone. This is exactly how the ”anti-drone-gun” operates [11], or hijacking the drone to have it go to an arbitrary waypoint [12]. Therefore, it is critical to ensure the security of communication in drone applications.

In this paper, we propose a lightweight digital signature protocol, also named as *DroneSig*, to protect drone from man-in-the-middle (MITM) attack, where an adversary eavesdrops the communication between GCS and drone, and impersonates the GCS and sends fake commands to terminate the ongoing mission or even take control over the drone. In the DroneSIG, the GCS generates a digital signature based on the command message by using the chaotic system and appends the digital signature to the command message. Before executing the received command, the drone validates the digital signature by comparing it to its own generated digital signature from the received command message. If the validation of digital signature fails, the command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position. We develop a customized simulation framework and evaluate its performance through extensive simulations in terms of energy consumption, computation time, CPU cycle, memory usage, and code size. We also revisit prior AES, DES, and 3DES [13], and modify them to work in the framework for performance comparison. The simulation results show that the proposed DroneSIG can achieve better performance in terms of energy consumption, computation time, CPU cycle, memory usage, and code size compared to AES, DES, and 3DES.

The rest of the paper is organized as follows. Prior schemes are provided and analyzed in Section II. A system model and the proposed DroneSIG are presented in Section III. Section IV focuses on simulation results and their analyses. Finally, concluding remarks are provided in Section V.

II. Related Work

A significant volume of research work has mainly focused on developing security mechanisms and features to ensure the basic security services of drones, such as confidentiality, integrity, and authentication, and protect drones from various cyber attacks. In [14], a temporal credential based anonymous lightweight user authentication mechanism is proposed to address authentication problem in IoD environment based on three-factor scheme using user’s mobile device, password and biometrics. An optimized public key infrastructure based framework integrated with lightweight symmetric primitives is proposed for small aerial drones in [15], where special precomputation methods and optimized elliptic curves are harnessed to reduce the computational overhead and energy consumption. In [16], an encryption mechanism that improves the communication security of open source drones is proposed based on Galois Embedded Crypto (GEC) and ArduinoLibs Crypto library to provide safer and more secure communication service for radio control link. A medium-interaction portable drone honeypot, also called HoneyDrone, is designed for protecting drones in [17]. The basic idea of HoneyDrone is to emulate a number of drone-specific and drone-tailored protocols, lure adversary into attacking drone honeypot, and record and analyze malicious activities to detect potential attackers.

In [18], a look-up table shuffling mechanism that supports white-box block cipher with dynamics is proposed to protect unmanned vehicles from white-box attacks, where attackers with sufficient knowledge of a target unmanned vehicle can steal secret information stored in the unmanned vehicle through taking advantage of advanced reverse engineering techniques and exploiting the vulnerabilities of open-source software. Since no short secret key is used by an unmanned vehicle during the protocol, the shuffling mechanism can be safely executed in the white-box environment and make it hard for a white-box attacker to successfully encrypt/decrypt any plaintext/ciphertext even if the attacker has the knowledge of the entire look-up table. In [19], a new system model is proposed to secure drone communication for the data collection and transmission in the IoD environment, where public blockchain technology is used for the storage of collected data from the drones and update the information into the distributed ledgers to reduce the burden of drones. According to experimental evaluation, the proposed system model makes the real-time drone-based applications more reliable and scalable, and can defend against various risks and attacks.

The [20] proposes to use information fusion by combining a visual sensor and inertial measurement unit to detect GPS spoofing attack in an airborne fog computing system. In order to address the challenging information leakage problem of eavesdropping attack, the [21] leverages the physical characteristics of wireless channels to achieve the goal of secure transmissions in unmanned aerial vehicles communication networks. In addition, an overview of security threats and attacks against communication protocol for unmanned systems and potential security solutions are also presented in [10]. The [22] proposes a blockchain and cloud storage based framework to guarantee the UAV data integrity. The hashed data records collected from drones are stored in blockchain network and a blockchain receipt for each data record is also stored in the cloud, which can reduce the burden of moving drones with the limit of battery and process capability while gaining enhanced security guarantee of the data. The [23] presents the ideology of secure utilization of drones for inter-service operability in ultra-dense wireless networks by exploiting the features of the blockchain. The authors in [24] propose a lightweight authentication and key agreement scheme in which there are only secure one-way hash function and bitewise XOR operations when drones and users mutually authenticate each other. The proposed scheme is comprised of three phases: the setup phase, the registration phase and the mutual authentication phase. In the setup phase, control station generates its master private key and other public system parameters. In the registration phase, user and drone register on control station and get their secret key via a secure channel. In the last phase, user and drone communicate wit each other securely after establishing a session key.

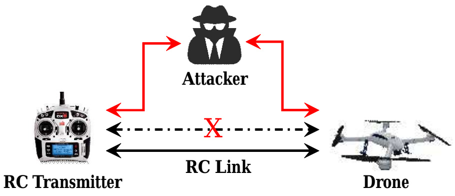
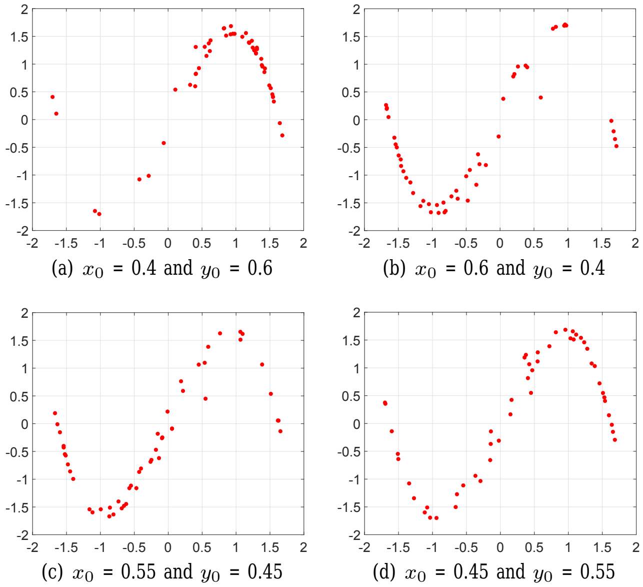


Fig. 1. System model.



(a) x_0 = 0.4 and y_0 = 0.6

(b) x_0 = 0.6 and y_0 = 0.4

(c) x_0 = 0.55 and y_0 = 0.45

(d) x_0 = 0.45 and y_0 = 0.55

Fig. 2. Duffing map with different initial conditions after 50 iterations.

In summary, various cryptographic techniques have been well studied to protect drones from cyber attacks. However, to the best of our knowledge, there is no comprehensive and lightweight defense mechanism against MITM attack for drones.

III. The Proposed Lightweight Digital Signature Protocol

In this section, we first introduce the system model and chaotic system, then propose a lightweight digital signature protocol, also named as *DroneSig*, to protect drones from MITM attack.

A. System Model

Fig. 1 shows a basic system diagram where there is a Radio Control (RC) link to be used by the GCS to manually control the drone. However, communication link between GCS and drone is established via wireless channel, which is vulnerable to various security attacks due to its openness [25]. To be specific, the GCS exchanges data with drone through an unauthenticated and unencrypted channel, as a result, the communications can be easily hacked by MITM attack. An adversary with an appropriate RC transmitter can eavesdrop the communication between GCS and drone, and impersonates the GCS and sends fake commands to terminate the ongoing mission or even gain direct control over drone [16]. Here, a successful communication link attack without involving ”anti-drone-gun” has already been demonstrated on a popular DSMx radio protocol to hijack the drone in [26].

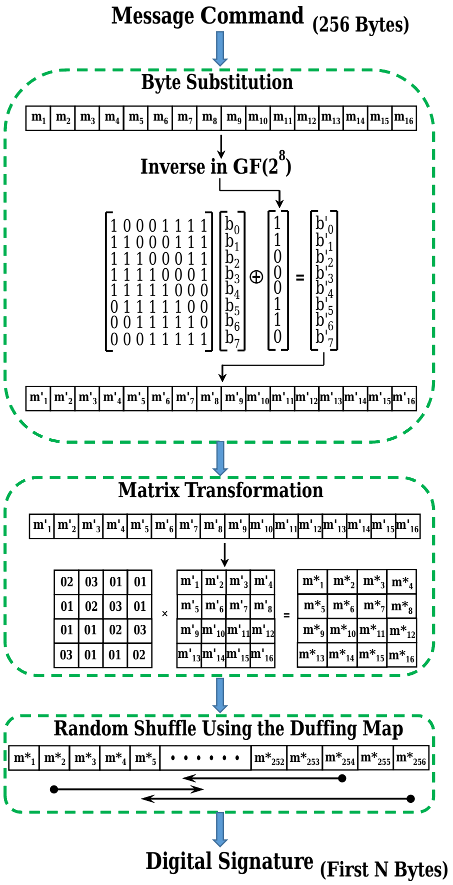


Fig. 3. Overall structure of the DroneSig.

B. Chaotic System

Chaotic system is a dynamical and determined system with the extrinsic nature of nonlinear behavior, pseudo-randomness, broad spectrum, and sensitivity to initial conditions. In the past few decades, a state of disorder and nonlinear dynamics have been used in the design of cryptographically secure pseudo-random number generators. These pseudo-random number generators use the control parameters and the initial condition of the chaotic maps as their keys. Without the right initial conditions, the correct pseudo-random sequence cannot be regenerated. Duffing map is a two-dimensional discrete-time and dynamical system that exhibits chaotic behavior. It is widely known to display chaos for certain parameter values and initial conditions. Duffing map contains a single cubic term and is expressed bellow,

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = -b \cdot x_n + a \cdot y_n - y_n^3 \end{cases} \tag{1}$$

where a and b are constant parameters. The output of the Duffing map highly depends on the initial conditions represented by x_0 and y_0. The constant parameters are usually sent to a = 2.75 and b = 0.2 to produce chaotic behavior. Disregarding the initial point, (0.5, 0.5), the Duffing map outputs points around the Duffing map attractor in a random way. As shown in Fig. 2, any change in the initial conditions will affect the plot of these points.

C. Lightweight Digital Signature Protocol

The DroneSig adopts a technique that is similar to cryptographic encryption, but requires less computational resources. In addition, the DroneSig is designed to encode and decode binary information without using standard cryptographic techniques, such as DES or AES. In DroneSig, the digital signature is generated by using a random number generator, Duffing map, which can assist both GCS and drone to achieve the same key without the necessity to wirelessly share it on a public wireless medium.

The DroneSig consists of three functions: byte substitution, matrix transformation, and random shuffling. Fig. 3 shows the overall structure of the DroneSig. Each message command has 256 bytes and are divided into a set of 16-byte blocks. Byte substitution and matrix transformation will be applied to each block, whilst random shuffling will be performed on all blocks. First, each individual byte of 16-byte block is mapped into a new byte according to

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} b_0^*\\ b_1^*\\ b_2^*\\ b_3^*\\ b_4^*\\ b_5^*\\ b_6^*\\ b_7^* \end{bmatrix} \oplus \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} b_0^{'}\\ b_1^{'}\\ b_2^{'}\\ b_3^{'}\\ b_4^{'}\\ b_5^{'}\\ b_6^{'}\\ b_7^{'} \end{bmatrix} \tag{2}$$

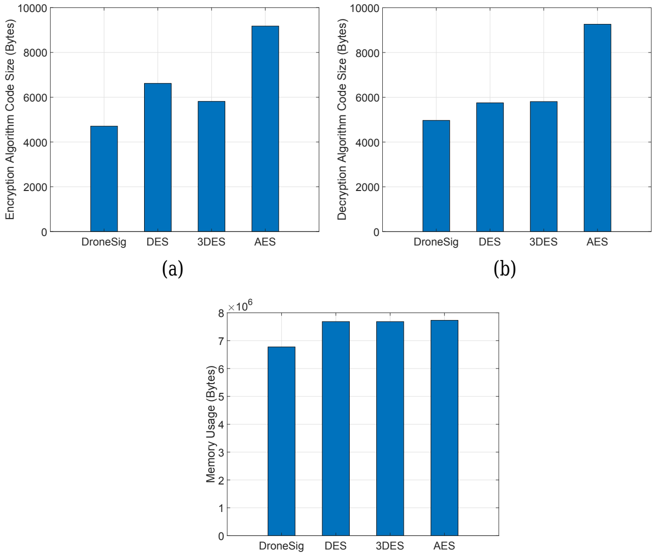
Here, $(b_7^*b_6^*b_5^*b_4^*b_3^*b_2^*b_1^*b_0^*)$ is the value of multiplicative inverse in GF(2^8) for input byte $(b_7b_6b_5b_4b_3b_2b_1b_0)$. As an example, considering the input byte {95}. the multiplicative inverse in GF(2^8) is $\{95\}^{-1}$ = {8A}, which is (10001010). According to Eq. (2), the result byte is {2A}. The process of byte substitution is showing below.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 0\\1\\0\\1\\0\\0\\0\\1 \end{bmatrix} \oplus \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 0\\1\\0\\1\\0\\1\\0\\0 \end{bmatrix} \tag{3}$$

Second, the 16 substituted bytes in block are depicted as a 4 × 4 square matrix, and each byte of a column in square matrix is mapped into a new value that is a function of all four bytes in that column. The transformation is defined by matrix transformation in Fig. 3. Each element in the product matrix is the sum of products of elements of one row and one column. In this case, the individual additions and multiplications are performed in GF(2^8). The matrix transformation on a single column can be expressed as

$$\begin{aligned} s^{'}_{0,j} &= (2 \cdot s0, j) \oplus (3 \cdot s1, j) \oplus s2, j \oplus s3, j\\ s^{'}_{1,j} &= s0, j \oplus (2 \cdot s1, j) \oplus (3 \cdot s2, j) \oplus s3, j\\ s^{'}_{2,j} &= s0, j \oplus s1, j \oplus (2 \cdot s2, j) \oplus (3 \cdot s3, j)\\ s^{'}_{3,j} &= (3 \cdot s0, j) \oplus s1, j \oplus s2, j \oplus (2 \cdot s3, j) \end{aligned} \tag{4}$$

Third, the 256 bytes of all blocks will be randomly shuffled using the Duffing map to generate the digital signature, which includes the first *N* bytes of the shuffling output. The shuffling process is reversible. When the drone receives the command message, it only executes the command after verifying the authenticity of the digital signature, proving that the communication has been held with the authenticated GCS. The drone will validate the digital signature by comparing it to its own generated signature from the command message. If this validation of digital signature fails, the command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position.



(a) (b)

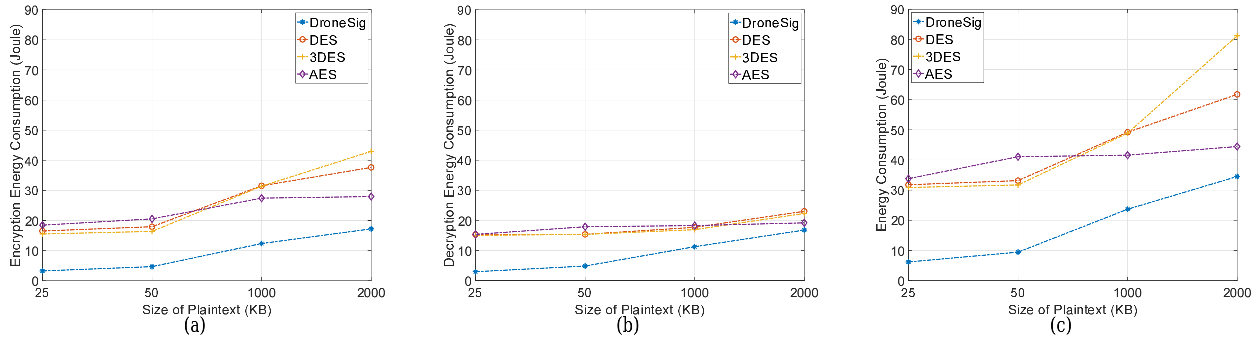
(c)

Fig. 4. Performance of code size and memory usage against the size of plaintext.

IV. Performance Evaluation

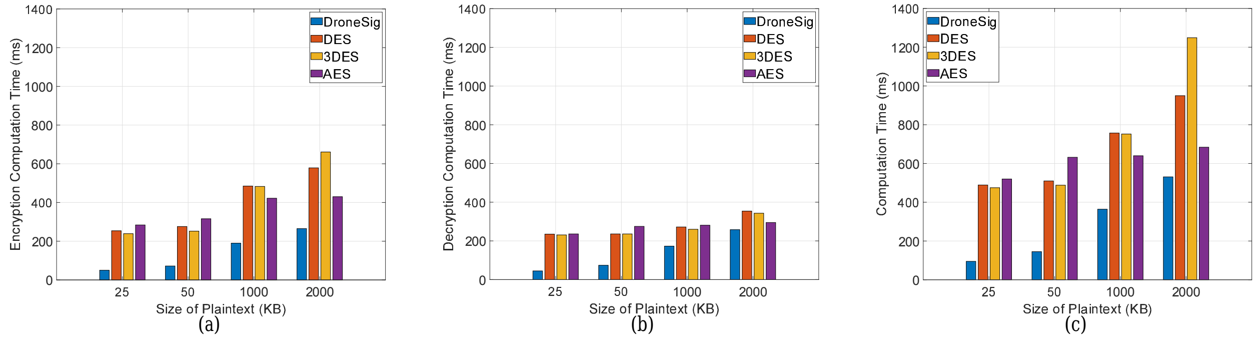
In this paper, we develop a customized simulation framework to conduct our experiments in terms of code size, memory usage, energy consumption, computation time, and CPU cycle. We also revisit existing AES, DES, and 3DES [13], and modify them to work in the framework for performance comparison and analysis. The size of plaintext is changed between 25 and 2000 KB.

First, the performance of code size and memory usage is measured with the changes of the size of plaintext in Fig. 4. Here, the code size is measured as the file size of algorithm. As shown in Fig. 4(a) and (b), the DroneSig has the smallest code



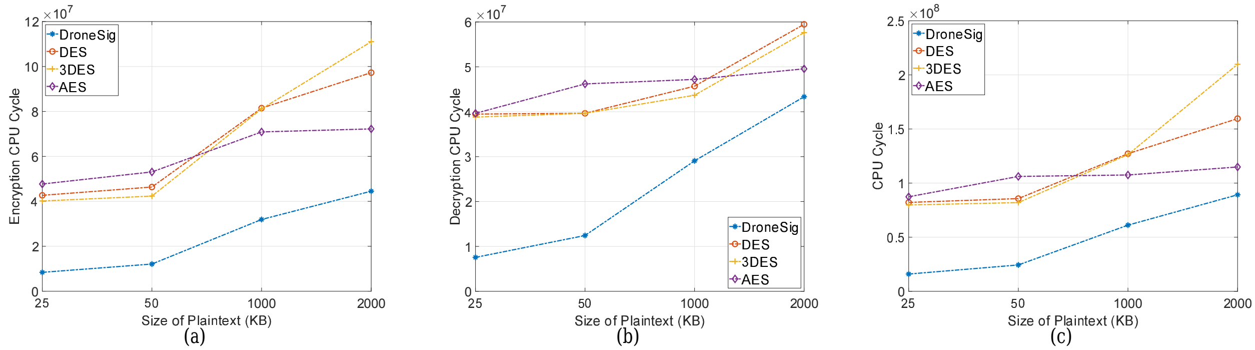
(a) (b) (c)

Fig. 5. Performance of energy consumption against the size of plaintext.



(a) (b) (c)

Fig. 6. Performance of computation time against the size of plaintext.



(a) (b) (c)

Fig. 7. Performance of CPU cycle against the size of plaintext.

size in terms of encryption and decryption algorithms compared to AES, DES, and 3DES. This is because the DroneSig has a less number of operations for encryption and decryption processes, which make the file size of algorithms smaller. The AES has the largest code size in terms of encryption and decryption algorithms because it is the most complex algorithm which consists of four transformation functions: substitute bytes, shift rows, mix columns, and add round key. In Fig. 4(c), we measure the memory usage of four schemes. It is clear that the DroneSig has the smallest memory usage compared to AES, DES, and 3DES.

Second, we measure the performance of energy consumption against the size of plaintext in Fig. 5. As shown in Fig. 5(a), the DroneSig achieves the lowest encryption energy consumption compared to AES, DES, and 3DES. This is because the DroneSig performs three lightweight operations, byte substitution, matrix transformation, and random shuffling, which consume less amount of energy to be executed. Most importantly, three lightweight operations are only executed one time in the process of encryption. Thus, the lowest encryption energy consumption is observed by the DroneSig. However, for AES, DES, and 3DES, the same encryption operations are performed in multiple rounds. As a result, a large amount of energy is consumed. In Fig. 5(b), it is clear that the decryption energy consumption of the DroneSig is lower than that of other three schemes. Since the decryption is the reverse process of encryption, the similar operations will be applied to ciphertext. Therefore, the lowest decryption energy consumption is obtained by the DroneSig. The total energy consumption is measured in Fig. 5(c), where the DroneSig provides the lowest total energy consumption compared to AES, DES, and 3DES. This is because the DroneSig has lowest encryption and decryption energy consumption.

Third, the performance of computation time is measured with varying size of plaintext in Fig. 6. The computation time is proportional to the complexity of algorithm. As the algorithm becomes more complex, it requires a larger computation time. In the DroneSig, there are only three operations and those operations are only executed one time for encryption and decryption. However, AES, DES, and 3DES are traditional cryptographic techniques, and several complex operations are executed in multiple rounds for encryption and decryption. Compared to DroneSig, AES, DES, and 3DES are much more complex. Therefore, the DroneSig can achieve the smallest computation time in terms of encryption and decryption, which are shown in Fig. 6(a) and (b), respectively. In Fig. 6(c), the DroneSig outperforms AES, DES, and 3DES in terms of total computation time because the DroneSig can achieve the smallest encryption and decryption computation time.

Forth, we measure the performance of CPU cycle by changing the size of plaintext in Fig. 7. As shown in Fig. 7(a) and (b), the smallest number of CPU cycles is obtained by the DroneSig in terms of encryption and decryption. Since the DroneSig significantly reduces the number of operations in the process of encryption and decryption, a smaller number of CPU cycles is required to complete the operations of encryption and decryption. However, AES, DES, and 3DES are more complex than DroneSig. Thus, a larger number of CUP cycles is required to execute all operations. In Fig. 7, the total number of encryption and decryption CPU cycles is measured for all schemes. The DroneSig provides the best performance compared to others because the DroneSig can achieve a smaller number of CPU cycles in terms of encryption and decryption.

V. Conclusion

In this paper, we proposed a lightweight digital signature protocol (DroneSig) to protect drones from man-in-the-middle attack, where an adversary eavesdrops the communications between Ground Control Station and drone, and impersonates the Ground Control Station and sends fake commands to terminate the ongoing mission or even take control over the drone. The basic idea of the DroneSig is that the drone will only execute the new command after validating the received digital signature from the Ground Control Station, proving that the new command message is coming from the authenticated Ground Control Station. If the validation of digital signature fails, the new command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position. In order to evaluate the effectiveness of the proposed approach, we developed a customized simulation framework and compare it with prior approaches. The simulation results show that the proposed DroneSig is a viable and competitive approach defending drones against man-in-the-middle attack.

References

[1] C. Pu, "Link-quality and traffic-load aware routing for UAV ad hoc networks," in *Proc. IEEE CIC*, 2018, pp. 71–79.

[2] C. Pu and C. Logan, "To Route or To Ferry: A Hybrid Packet Forwarding Algorithm in Flying Ad Hoc Networks," in *Proc. IEEE NCA*, 2019, pp. 1–8.

[3] *Global Small Drones Market 2018-2025 - Exemptions Made By the FAA to Allow the Use of Small Drones in Several Industries*, https://www.prnewswire.com/news-releases/global-small-drones-market-2018-2025—exemptions-made-by-the-faa-to-allow-the-use-of-small-drones-in-several-industries-300721794.html.

[4] *Commercial drones are here: The future of unmanned aerial systems*, https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems.

[5] C. Pu and L. Carpenter, "Psched: A Priority-Based Service Scheduling Scheme for the Internet of Drones," *IEEE Systems Journal (Early Access)*, pp. 1–1, 2020.

[6] C. Pu, "Stochastic Packet Forwarding Algorithm in Flying Ad Hoc Networks," in *Proc. IEEE MILCOM*, 2019, pp. 490–495.

[7] C. Lin, D. He, N. Kumar, K. Choo, A. Vinel, and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, 2018.

[8] A. Sanjab, W. Saad, and T. Başar, "Prospect Theory for Enhanced Cyber-Physical Security of Drone Delivery Systems: A Network Interdiction Game," in *Proc. IEEE ICC*, 2017, pp. 1–6.

[9] C. Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," *IEEE Access*, vol. 6, pp. 68 472–68 486, 2018.

[10] 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. 87 658–87 680, 2019.

[11] *Dronebuster*, http://flexforce.us/product/dronebuster/.

[12] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An Efficient UAV Hijacking Detection Method Using Onboard Inertial Measurement Unit," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, pp. 96:1–96:19, 2018.

[13] W. Stallings, *Cryptography and Network Security*. Pearson, 2006.

[14] S. Jangirala, A. Das, N. Kumar, and J. Rodrigues, "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, 2019.

[15] M. Ozmen and A. Yavuz, "Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones," in *Proc. IEEE MILCOM*, 2018, pp. 1–6.

[16] M. Podhradsky, C. Coopmans, and N. Hoffer, "Improving Communication Security of Open Source UAVs: Encrypting Radio Control Link," in *Proc. IEEE ICUAS*, 2017, pp. 1153–1159.

[17] J. Daubert, D. Boopalan, M. Mühlhäuser, and E. Vasilomanolakis, "Improving Communication Security of Open Source UAVs: Encrypting Radio Control Link," in *Proc. IEEE NOMS*, 2018, pp. 1–6.

[18] J. Won, S. Seo, and E. Bertino, "A Secure Shuffling Mechanism for White-box Attack-resistant Unmanned Vehicles," *IEEE Trans. Mobile Comput.*, vol. 19, no. 5, pp. 1023–1039, 2020.

[19] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A New Secure Data Dissemination Model in Internet of Drones," in *Proc. IEEE ICC*, 2019, pp. 1–6.

[20] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight Security and Safety of Drones in Airborne Fog Computing Systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, 2018.

[21] B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV Communication Networks over 5G," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 114–120, 2019.

[22] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards Data Assurance and Resilience in IoT Using Blockchain," in *Proc. IEEE MILCOM*, 2017, pp. 261–266.

[23] V. Sharma, I. You, and G. Kul, "Socializing Drones for Inter-Service Operability in Ultra-Dense Wireless Networks using Blockchain," in *Proc. ACM MIST*, 2017, pp. 81–84.

[24] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, vol. 154, pp. 455–464, 2020.

[25] C. Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System," in *Proc. IEEE LANMAN*, 2020, Accepted to Appear.

[26] Https://arstechnica.com/information-technology/2016/10/drone-hijacker-gives-hackers-complete-control-of-aircraft-in-midflight/.