Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System

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

***Abstract*—With the continuous miniaturization of electronic devices and the recent advancement in wireless communications, unmanned aerial vehicles (UAVs) will find many new uses in people's production and life, bringing great convenience to the public. Meanwhile, the cybersecurity of UAVs is gaining significant attention due to both financial and strategic information and value involved in aerial applications, and UAV and sensitive data collected by embedded sensors are subject to new security challenges and privacy issues. Traditional cryptographic techniques can be deployed to provide fundamental security services, however, they have been shown to be inefficient because of intrinsic resource constraints of UAVs and the open nature of wireless communication. For the sake of providing secure authentication between communication parties and further ensuring data security and privacy, this paper proposes a lightweight mutual authentication protocol, also referred to as *PCAP*, for secure communications between UAVs and ground station. The basic idea of the *PCAP* is that UAV and ground station use the challenge-response pair of physical unclonable function as the initial condition of chaotic system to randomly shuffle the message which piggybacks a seed to generate a secret session key. We conduct simulation experiments using OMNeT++ to validate the effectiveness of the *PCAP*. The simulation results show that the *PCAP* can achieve better performance in terms of computation cost, communication overhead, and energy consumption of communication compared to prior cryptographic technique, indicating a viable approach for securing communications between UAVs and ground station.**

***Index Terms*—Unmanned Aerial Vehicles, Authentication Protocol, Physical Unclonable Function, Chaotic System**

I. Introduction

Unmanned aerial vehicles (UAVs), widely known as drones[1], have emerged as a key part of the fourth industrial revolution (often referred to as Industry 4.0) [1], and provide an unprecedented opportunity to revolutionize mobility networks. UAVs are no longer only limited to military applications, but they are also becoming progressively popular in various civilian application domains [2], such as disaster mitigation and relief, filmmaking and photography, delivery/fulfillment, agriculture/conservation, etc. According to [3], [4], it is expected that the sales of UAVs will surpass $12 billion in 2021, and the potential economic benefit of integrated unmanned airborne systems will generate an estimated $82 billion and create up to 100,000 jobs by 2025. Aerial technology is transforming industries of all types by optimizing processes, cutting costs, and reaching both figurative and literal places that were once unattainable. Drone delivery services show enough potential that Amazon, Alphabet, Walmart, and other giants are hailing it as the future of e-commerce fulfillment. In 2019 the Federal Aviation Administration (FAA) approved United Parcel Service (UPS) Flight Forward to become the first-ever drone service operating as a commercial airline to deliver medical supplies to hospitals in United States. The age of artificial intelligence, digital connectivity, automation and intelligent machines has arrived. Even though the ''Jetson lifestyle'' isn't upon us just yet, we envision that the advancements in UAV technology will totally change the world as we know it in just a few short years [5].

UAVs are flying robots equipped with various equipment to collect and analyze the physical phenomena and real-time information, and transmit data back to ground station via wireless communication [6]. Due to both financial and strategic information and value involved in aerial applications, the UAV system is vulnerable to attacks that target either the cyber and/or physical elements, the interface between them, the wireless link, or even a combination of multiple components [7]. Since 2006, U.S. Customs and Border Protection has operated UAVs to patrol the U.S. borders with Mexico and Canada, watching for drug smugglers and unauthorized border crossers. However, it has been reported by the U.S. Department of Homeland Security and the U.S. Customs and Border Protection agency that drug traffickers have hacked their UAVs to cross the US-Mexican border illegally in January 2016 [8]. In addition, an adversary can send unauthorized commands to the drone to take its control from ground station, and then catch and withhold the drone [9]. This is exactly how the ''anti-drone-gun'' operates [10], or hijacking the drone to have it go to an arbitrary waypoint [11]. Therefore, investigating potential cyber threats against UAVs and designing the state-of-the-art security mechanisms are the top priority to ensure the cybersecurity of UAV applications [12].

The existing standard primitives and cryptographic protocols can be deployed to provide fundamental security services, however, they have been shown to be inefficient in terms of energy/time consumption for small aerial drones that operate

[1]In this paper, UAV and drone will be used interchangeably.

978-1-7281-8154-7/20/$31.00 ©2020 IEEE

with resource-limited microprocessors [13]. Thus it has become obvious that lightweight protocols are the only suitable solutions to provide security services such as confidentiality, authentication, and integrity. In addition, UAVs should have tamper-resistant capabilities that enforce authenticated policies and cannot be overridden. An adversary may attempt to probe or alter the circuit, this will irreversibly modify the slight physical variations in the integrated circuit, which in turn should prevent regeneration of sensitive data such as secure session key. In light of these, we propose a lightweight mutual authentication protocol and its corresponding techniques to energy-efficiently protect the communications between UAVs and ground station and measure its security resiliency and performance tradeoff through simulation experiments. Our major contribution is briefly summarized in twofold.

1) We propose a lightweight mutual authentication protocol, also referred to as *PCAP*, for secure communication between UAVs and ground station. The basic idea of the *PCAP* is that UAV and ground station use the challenge-response pair of physical unclonable function (PUF) as the initial condition of chaotic system to randomly shuffle the message which piggybacks a seed to generate a secret session key.
2) We revisit a prior well-known cryptographic technique, Wazid et al.'s approach [14], and modify it to work in the framework for performance comparison and analysis.

We develop a customized discrete event driven simulation framework by using OMNeT++ [15] and evaluate its performance through simulations in terms of computation cost, communication overhead, and energy consumption of communication. The simulation results show that the *PCAP* can achieve better performance in terms of computation cost, communication overhead, and energy consumption of communication compared to Wazid et al.'s approach [14], indicating a viable approach for securing communications between UAVs and ground station.

The rest of the paper is organized as follows. Prior schemes are provided and analyzed in Section II. Section III gives a brief introduction to PUF and chaotic system. A network model and the proposed lightweight mutual authentication protocol are presented in Section IV. Section V focuses on simulation results and their analyses. Finally, concluding remarks with future research direction are provided in Section VI.

II. Related Work

The authors in [16] propose an authentication and key agreement (AKA) scheme for the Internet of Drones (IoD) architecture, where a secure one-way hash function and the bitwise exclusive-or operation are deployed to achieve authentication between drones and users before sharing the collected data. The proposed AKA scheme is comprised of three phases: the setup phase, the registration phase, and the mutual authentication phase. In the setup phase, a control server generates its master private key and other public system parameters. During the registration phase, mobile user and drone join IoD environment, register on control server and get their secret key via a secure channel. In the authentication phase, the registered mobile user and drone can communicate with each other securely after establishing a session key. In [17], a temporal credential based anonymous lightweight authentication scheme, also called TCALAS, is proposed for resource limited unmanned drones in IoD environments. In the TCALAS, the legitimate and registered users are only allowed to get the services from the remote drones by registering to ground station server (GSS). Prior to providing services, all the remote drones need to register with GSS. Once the registration is done, the remote drone is assigned with secret credential which is only known to drone and GSS. The registered users have the facility to update their passwords and/or biometrics at any time without involving further the GSS. The authors in [18] propose an privacy-preserving authentication framework to address the security and privacy concerns in IoD. The framework assures the authentication efficiency when deploying on resource-constrained small-scale UAVs by utilizing the lightweight online/offline signature design. In addition, a predictive authentication approach is investigated with mobile edge computing to reduce the authentication cost for potential authentication activities. Finally, a buffer pseudonym and public key update strategy are designed to enable the protection of privacy in terms of UAV's identity, location, and flying routes.

In [19], an authentication and key agreement scheme (SLAKA) is proposed based on fuzzy extractor, the cryptographic hash function, and the bitwise exclusive-or operation. In the SLAKA, mutual authentication between a wearable device and the mobile terminal can be achieved, after that, a session key can be negotiated at both ends for future secure communications. The authors in [20] claim that one-time password is an authentication scheme that represents a promising solution for IoT and smart city environments. Thus, they extend the one-time password principle and propose an approach of one-time password generation that relies on elliptic curve cryptography and isogeny in order to ensure IoT security. In [21], a Physical Unclonable Function (PUF) based secure user key-exchange authentication (SUKA) protocol for vehicle-to-grid systems is proposed. The proposed protocol uses PUF to achieve a two-step mutual authentication between an electric vehicles and the grid server, which can avoid storing any secret information in electric vehicles and aggregators. The grid server only stores one set of challenge-response pairs for every electric vehicle. When an electric vehicle wants to authenticate with the grid server, two session keys are established: one session key between the aggregator and the grid server, and another one between the electric vehicle and the aggregator.

In [22], 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

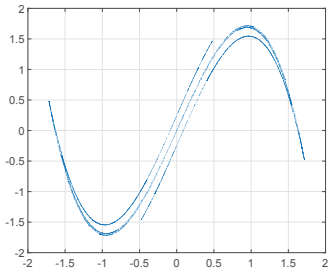


Fig. 1. Duffing map, where $x_0 = 0.5$ and $y_0 = 0.5$.

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 [23], a 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 updating the information into the distributed ledgers to reduce the burden of drones. In order to address the challenging information leakage problem of eavesdropping attack, the [24] leverages the physical characteristics of wireless channels to achieve the goal of secure transmissions in unmanned aerial vehicles communication networks.

In last several years, a few authentication protocols have been proposed for UAV communications. However, little attention has been paid to an authentication protocol using physical unclonable function and chaotic system.

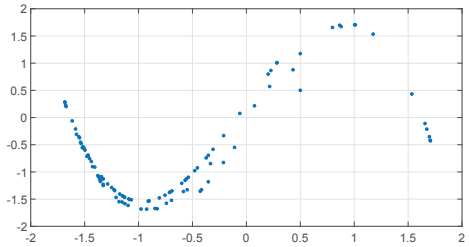
III. Preliminary Background

A. Physical Unclonable Function

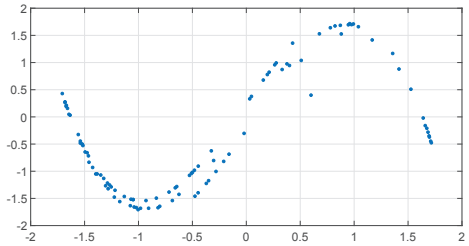
Based on the fact that integrated circuits have very slight physical differences due to inevitable variations in the manufacturing process, a physical unclonable function (PUF) can be regarded as a unique physical identity of a device, which is similar as biometric features (e.g., fingerprints or retina) to human beings. Alternatively, a PUF is defined as a circuit with an input to output mapping that depends on the unique characteristics of the physical hardware on which it is executed [25]. For each PUF, an input query or 'challenge' receives an instance-specific output or 'response', a process known as a challenge-response pair (CRP). In general, a PUF can be represented as a function P in the following:

$$R = P(C), \tag{1}$$

where C and R is the input challenge and output response of the PUF, respectively. With the physical and secure one-way function Eq. (1), the PUF can produce the same response with the same challenge. However, the same challenge will produce responses far apart with high probability if it is provided to different PUFs. Thus, PUF can provide two valuable features for securing device: (i) the ability to dynamically regenerate a sensitive value using only public information; and (ii) the ability to provide tamper resistance against various physical attacks.



(a) $x_0 = 0.5$ and $y_0 = 0.5$



(b) $x_0 = 0.6$ and $y_0 = 0.4$

Fig. 2. Duffing map with different initial condition after 100 iterations.

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 condition, 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 condition. Duffing map contains a single cubic term and is expressed bellow,

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = -b \cdot x_n + a \cdot y_n - y_n^3 \end{cases} \tag{2}$$

where a and b are constant parameters. The output of the Duffing map highly depends on the initial condition represented by x_0 and y_0. The constant parameters are usually set to $a = 2.75$ and $b = 0.2$ to produce chaotic behavior. The Duffing map showing chaotic behavior is plotted in Fig. 1. Disregarding the initial point (x_0, y_0), the Duffing map outputs points around the Duffing map attractor in a random way. As shown in Fig. 2, any change in the initial condition will affect the plot of these points.

IV. The Proposed Lightweight Mutual Authentication Protocol

A. Network Model

The network model is described in Fig. 3, which consists of two participants: UAVs and ground station. Each UAV

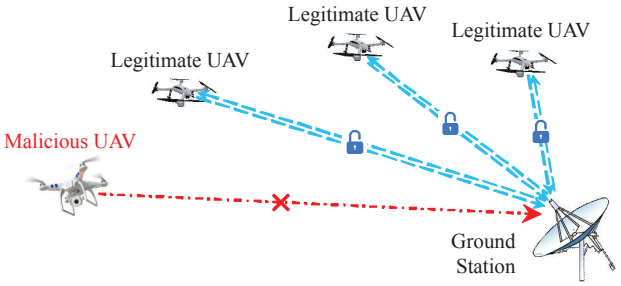


Fig. 3. Network model.

is equipped with an integrated circuit consisting of a PUF. Any adversary that attempts to probe or alter the circuit of captured UAV will irreversibly modify the slight physical variations in the integrated circuit, which in turn changes the PUF challenge-response mapping, or even destroys the PUF. Each UAV has limited resources due to the stringent constraints imposed by the size, weight, and power limitations. The ground station is considered as a trusted party and has no limitation of resources. During the system deployment phase, the ground station obtains an initial CRP from each UAV securely by using the time-based one-time password algorithm mechanism [26]. Once the UAV exchanges the initial CRP with the ground station, it can function independently. Thus, the ground station stores the ID and the CRP for each UAV, while the UAV does not store any secret information. Due to the long distance between UAV and operator and the lack of physical protection, the UAV can be easily captured by an adversary. An open nature of wireless communication can also enable the adversary to overhear, duplicate, corrupt, or alter the data. The goal of the adversary is to establish an authentication with the ground station without being detected to cause more financial and strategic damage.

B. Proposed Lightweight Authentication Protocol

The basic idea of the proposed lightweight mutual authentication protocol is that UAV and ground station use the challenge-response pair (CRP) of physical unclonable function (PUF) as the initial condition of Duffing map to randomly shuffle the message which piggybacks a seed to generate a secret session key. The proposed protocol for UAV and ground station to communicate with each other is shown in Fig. 4. The detailed steps are as follows.

1) The UAV ID_X randomly generates a nonce N_X, and then sends the nonce N_X along with its ID ID_X to ground station ID_{GS}.
2) The ground station ID_{GS} locates the entry of UAV ID_X and retrieves the corresponding CRP_X^i (C_X^i,R_X^i) in the memory. If the entry of UAV ID_X does not exist, the authentication request is rejected. The ground station ID_{GS} generates a random number PRF_{GS} and creates the message M_X, $\{ID_X \| N_X \| PRF_{GS}\}$. Then, the ground station ID_{GS} randomly shuffles the sequence of the bytes of message M_X using the Duffing map with the CRP (C_X^i,R_X^i) as the initial condition, and generates the encrypted message M_X^*. Finally, the ground station ID_{GS} generates the message authentication code (MAC) MAC_X, which is calculated as $C(M_X^* \| CRP_X^i \| PRF_{GS})$, and sends C_X^i, M_X^* and MAC_X to the UAV ID_X. Here, C is a MAC function.
3) The UAV ID_X first generates the response R_X^i using its PUF with the challenge C_X^i. With the CRP_X^i (C_X^i,R_X^i), the UAV ID_X restores the message M_X. The UAV ID_X then obtains PRF_{GS} from the message M_X, and verifies the MAC MAC_X with M_X^*, CRP_X^i, and PRF_{GS}. If the message authentication code verification fails, the authentication process is terminated. Otherwise, the UAV ID_X generates a random number PRF_X and computes the new challenge C_X^{i+1} using $PRNG(PRF_X \| PRF_{GS})$. Here, *PRNG* is a pseudorandom number generator. Then, the UAV ID_X computes the new response R_X^{i+1} using its PUF with the new challenge C_X^{i+1}, and forms the new CRP_X^{i+1} (C_X^{i+1},R_X^{i+1}), which will be used for future authentication process. After that, the UAV ID_X creates the message M_{GS}, $\{ID_X \| PRF_X \| PRF_{GS} \| R_X^{i+1}\}$, and randomly shuffles the sequence of the bytes of message M_{GS} using the Duffing map with the CRP (C_X^i,R_X^i) as the initial condition and generates the encrypted message M_{GS}^*. Finally, the UAV ID_X generates the MAC MAC_{GS}, which is calculated as $C(M_{GS}^* \| CRP_X^i \| PRF_X)$, sends M_{GS}^* and MAC_{GS} to ground station ID_{GS}.
4) The ground station ID_{GS} restores M_{GS} using the CRP_X^i (C_X^i,R_X^i), and obtains PRF_X and R_X^{i+1}. Then, the ground station ID_{GS} verifies the MAC MAC_{GS} with M_{GS}^*, CRP_X^i, and PRF_X. If the verification succeeds, the ground station ID_{GS} computes the new chal-

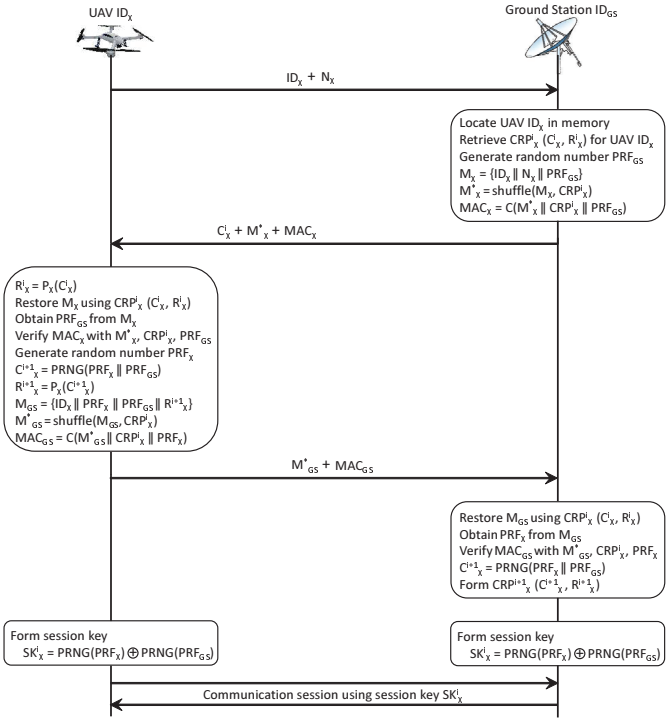


Fig. 4. The proposed lightweight authentication protocol.

lenge C_X^{i+1} as $PRNG(PRF_X \| PRF_{GS})$, and forms the new CRP_X^{i+1} (C_X^{i+1},R_X^{i+1}). Otherwise, the authentication process is terminated.

5) The ground station ID_{GS} and the UAV ID_X construct the secret session key SK_X^i, which is calculated as $PRNG(PRF_X) \oplus PRNG(PRF_{GS})$.

By this time, the mutual authentication between the ground station ID_{GS} and the UAV ID_X is finally succeeded and the secret session key has been securely established for the following secure communication.

V. Performance Evaluation

A. Security Analysis

The *PCAP* is designed to defend against different security attacks such as cloning attacks, man-in-the-middle attacks, replay attacks, and tampering attacks. The Duffing map is used to randomly shuffle the sequence of bytes in the message to achieve the desired effect of encryption, and finally ensure the authenticity of the messages exchanged between UAV and ground station. The UAV and the ground station are not required to use any computationally intensive cryptographic algorithms to encrypt and decrypt the messages, which significantly reduces the computational cost of the authentication protocol. In the scenario of man-in-the-middle attacks, an adversary is unable to generate any valid encrypted messages because it lacks the initial condition of the Duffing map. In addition, each communication session will have a different CRP, which is used as the initial condition for the Duffing map to randomly shuffle the sequence of bytes in the message. Therefore, the exchanged messages will expire when the communication session ends. Any future replay of previously eavesdropped messages will be rejected by either the UAV or the ground station. Thus, the adversary is unable to either replay previous eavesdropped messages nor to alter the communication in real-time. The *PCAP* relies on the random sequence generated by the Duffing map to shuffle the sequence of bytes in the message. The rationale behind this design is to harden the task of deciphering the encrypted message by an external party. Any alteration in the sequence of bytes of message will lead to an erroneous message, resulting in that the MAC cannot be verified successfully. This sequence is only shared between the UAV and the ground station as they are the only two parties with correct initial condition and seed for the Duffing map.

B. Experimental Evaluation

We conduct simulation experiments using OMNeT++ [15] to evaluate the performance of our approach *PCAP* in terms of computation cost, the number of exchanged messages per communication session, and energy consumption of communication. We also revisit prior scheme, Wazid et al.'s approach [14], and modify it to work in the framework for performance comparison and analysis. A 150 $\times$ 150 (m^2) square network area is considered, where 2 and 3 nodes is deployed for our approach *PCAP* and Wazid et al.'s approach, respectively. For the *PCAP*, one node simulates UAV and the other node simulates ground station. However, for Wazid et al.'s approach, 3 nodes represent UAV, server, and user, respectively.

TABLE I
Computation Cost

Approach	UAV	Server	User/GS*
Wazid et al.'s approach	1.5384 ms	1.8175 ms	15.8692 ms
PCAP	0.6249 ms	0 ms	1.2694 ms

$*$: User and GS (Ground Station) is used in Wazid et al.'s approach and our approach *PCAP*, respectively.

First, we measure the computation cost of Wazid et al.'s approach and our approach *PCAP* in Table I. As shown in Table I, the computation cost of Wazid et al.'s approach in terms of UAV, server, and user is 1.5384 ms, 1.8175 ms, and 15.8692 ms respectively, which is significantly higher than that of our approach *PCAP*. In Wazid et al.'s approach, a larger number of hash functions and bitwise XOR computations are used to generate secure information, which requires more computational time with the limited computation resources. The largest amount of computational time is observed at the user side, because the user is involved in multiple phases, such as predeployment, user registration, login, and authentication and key agreement. Compared to Wazid et al.'s approach, the *PCAP* uses the challenge-response pair (CRP) of physical unclonable function (PUF) as the initial condition of Duffing map to generate the secure information, which requires a smaller amount of operations. As a result, the computation cost of the *PCAP* is much lower than that of Wazid et al.'s approach. In addition, the *PCAP* does not need the intermediate server to establish the secure communication between UAV and ground station, thus, the computation cost of server is 0 ms.

TABLE II
Number of Sent Messages

Approach	UAV	Server	User/GS
Wazid et al.'s approach	1 message	2 messages	2 messages
PCAP	2 messages	0 message	1 message

TABLE III
Number of Received Messages

Approach	UAV	Server	User/GS
Wazid et al.'s approach	1 message	3 messages	1 message
PCAP	1 message	0 message	2 messages

Second, we measure the number of sent messages and the number of received messages in Table II and III, respectively. In Table II, ground station and UAV need to send out 1 and 2 messages in order to establish one secure session key for future communication in the *PCAP*. However, Wazid et al.'s approach requires a total 5 messages to be sent by UAV, server and user in order to successfully establish one session key. As shown in Table III, compared to the *PCAP*, each party in Wazid et al.'s approach receives more number of messages in the process of establishing one session key.

Finally, in Table IV, the energy consumption of establishing one session key is measured based on the number of sent and received messages [27]. In the *PCAP*, the server is not

TABLE IV
ENERGY CONSUMPTION OF COMMUNICATION (JOULE)

Approach	UAV	Server	User/GS
Wazid et al.'s approach	0.112×10^{-3}	0.277×10^{-3}	0.174×10^{-3}
PCAP	0.174×10^{-3}	0	0.163×10^{-3}

required for the establishment of secure session key, thus the energy consumption of server is 0. The *PCAP* shows a little bit higher energy consumption of UAV compared to that of Wazid et al.'s approach. This is because the UAV sends and receives more messages in our approach, as a result, a higher energy consumption of UAV is observed. However, the *PCAP* shows better performance than Wazid et al.'s approach in terms of the energy consumption of user/ground station. Since the user in Wazid et al.'s approach sends out more messages, more energy consumption is obtained. Please note that sending a message consumes more energy than receiving a message according to [28]. In summary, more energy consumption of establishing one session key is observed by Wazid et al.'s approach (total: 0.563×10^{-3} joule) than our approach *PCAP* (total: 0.337×10^{-3} joule).

VI. CONCLUSION

Internet of Drones (IoD) has been widely used in various application domains, and brings a great convenience to people in daily life. In the last several years, a few authentication schemes for UAVs have been proposed. However, most of them are subject to high computation cost and communication overhead. Therefore, we proposed a lightweight mutual authentication protocol and its corresponding techniques to energy-efficiently protect the communications between UAV and ground station. The basic idea of our approach is that UAV and ground station use the challenge-response pair of physical unclonable function as the initial condition of chaotic system to randomly shuffle the message which piggybacks a seed to generate a secret session key. In order to evaluate the effectiveness of the proposed approach, we developed a customized discrete event driven simulation framework and compare it with a prior approach. The simulation results show that the proposed lightweight mutual authentication protocol is viable approach for securing communications between UAVs and ground station. Since radio propagation and its channel dynamics cannot easily be captured by simulation models, we plan to develop a small-scale testbed with small quad-copters to see the full potential of the proposed protocol.

ACKNOWLEDGMENT

This research was supported in part by *NASA WV EPSCoR Grant # 80NSSC20M0055* and startup grant in the Dept. of CSEE at Marshall University.

REFERENCES

[1] A. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial Cyberphysical Systems: A Backbone of the Fourth Industrial Revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, 2017.

[2] C. Pu and L. Carpenter, "To Route or To Ferry: A Hybrid Packet Forwarding Algorithm in Flying Ad Hoc Networks," in *Proc. IEEE NCA*, 2019, pp. 367–375.

[3] *Commercial Unmanned Aerial Vehicle (UAV) Market Analysis*, 2020, https://www.businessinsider.com/commercial-uav-market-analysis.

[4] *5 Ways Drones Are Changing the World*, 2018, https://www.entrepreneur.com/article/306599.

[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] R. Altawy and A. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[8] *US Border Patrol Drones Hacked by Drug Cartels*, 2016, https://www.hackread.com/us-border-patrol-drones-hacked-by-drug-cartels.

[9] D. Shepard, J. Bhatti, and T. Humphreys, "Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle," *GPS World*, vol. 23, no. 8, pp. 30–33, 2012.

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

[11] 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.

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

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

[14] M. Wazid, A. Das, N. Kumar, A. Vasilakos, and J. Rodrigues, "TOTP: Time-Based One-Time Password Algorithm," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[15] A. Varga, *OMNeT++*, 2014, http://www.omnetpp.org/.

[16] D. Bernstein, "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, vol. 154, pp. 455–464, 2020.

[17] J. Srinivas, 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.

[18] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *Journal of Information Security and Applications*, vol. 48, no. 7, p. 102354, 2019.

[19] J. Li, N. Zhang, J. Ni, J. Chen, and R. Du, "Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems," *IEEE Internet of Things Journal (Early Access)*, pp. 1–1, 2020.

[20] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)," *IEEE Systems Journal (Early Access)*, pp. 1–1, 2020.

[21] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight Mutual Authentication Protocol for V2G Using Physical Unclonable Function," *IEEE Trans. Veh. Technol. (Early Access)*, pp. 1–1, 2020.

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

[23] 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.

[24] 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.

[25] J. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," in *Proc. IEEE FiCloud*, 2016, pp. 99–106.

[26] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," *Internet Request for Comments*, 2011.

[27] B. Groves and C. Pu, "A Gini Index-Based Countermeasure Against Sybil Attack in the Internet of Things," in *Proc. IEEE MILCOM*, 2019, pp. 1–6.

[28] C. Pu, "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937–4949, 2020.