Authorized Arming and Safeguarded Landing Mechanisms for Drones

Gunasekaran Raja, *Senior Member, IEEE*, Sudha Anbalagan, Kottilingam Kottursamy, Guggilam Swetha Aparna,
Jeyalakshmi Kumaresan, Mansoor Ihsan
[1,4,5]Department of Computer Technology, Anna University, Chennai,
[2,3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai,
[6]University of Salford, Manchester, UK,
[1]dr.r.gunasekaran@ieee.org, [2]sudhaa@srmist.edu.in, [3]kottilik@srmist.edu.in, [4]guggilamswetha99@gmail.com,
[5]getmetojeya@gmail.com, [6]m.ihsan1@salford.ac.uk

***Abstract*—Safety and security is a major concern that needs attention in the field of Unmanned Aerial Vehicles (UAVs) or drones. The failure to ensure high standards of security will inevitably result in the endangerment of people and property. Crafting such security measures is heavily dependent on the hardware and software control capabilities of drones. In a drone mission, arming involves controlling drone motors and plays a critical part in its flight. Unauthorized arming is a major security challenge associated with drones. To this end, a Randomized Logistic map based Time-dependent One Time Password (Randomized LTOTP) algorithm as a mechanism of authenticating the drone-arming procedure is proposed. In addition, unintended flight termination is a potential safety threat that needs to be mitigated in any drone application. Existing systems trigger drone landing as soon as they detect low battery levels. This often results in hazardous and spontaneous landing conditions. As an attempt to mitigate this issue, a Flag based Battery Fail-Safe (FBFS) algorithm is proposed to monitor in-flight battery levels and safeguards the landing by prolonging the mission until the landing is safe. The simulation results show that the Randomized LTOTP algorithm achieves 92% randomness, which improves the security of the arming process, and FBFS improves the flight time approximately by 3-fold compared with the existing algorithm.**

***Index Terms*—UAV Arming, OTP Authentication, Fail-Safe System, Authorized Arming, Safeguarded Landing**

I. Introduction

Unmanned Aerial Vehicles (UAV) promises a wide range of applications such as military, agriculture, rescue operation, inventory, and in most of the commercial fields [1]. The global commercial drone market is expected to reach about 13.37 billion US dollars by the end of 2025 [2]. UAVs share plenty of sensible data like telemetry and telecommand data with the ground control station. Thus, UAVs are the potential targets in which an adversary can harm the UAV or access the data it contains. Moreover, UAVs are vulnerable to attacks, as they communicate through a wireless network. Thus, security is always an issue in UAV networks [3]. It is critical to secure the data present in UAV when it is in motion. Therefore, safeguarding UAVs from unapproved access and interruption is indispensable for UAVs' future advancement, which can be achieved through authentication [4], [5]. Moreover, if a significant defense mechanism like authentication fails, all other security measures become redundant, placing the entire UAV mission under threat [6].

The existing security systems use client authentication and data origin authentication but have drawbacks due to their symmetric nature. Furthermore, existing mechanisms provide authentication only to pre-decided legitimate users who have a secret key but are incapable of providing non-repudiation [7]. Non-repudiation is a security assurance to ensure that a sending communication entity cannot deny the origin of its message. The specified challenges can be resolved by using One Time Password (OTP) based authentication mechanisms such as chaotic map based OTP [8] and Time-based OTP (TOTP) [9], [10]. Unlike conventional static passwords that are valid for a long time, OTPs are dynamic and restricted for one-time use, making OTP-based authentication desirable for primary security mechanisms.

Besides security, safety is another important aspect of drone navigation. A drone's flight safety majorly depends on its battery life and confined flight time, making these factors significantly challenging to handle. Limited battery life shortens drone flight duration, causing drones to return to their ground control stations for recharge. This may prolong the actual mission completion and, therefore, unsuitable for time-critical missions. For lithium batteries, the battery capacity is limited and cannot be recharged easily [11]. Hence, currently Electronic Fuel Injection (EFI) engines are preferred as they provide about 25% fuel saving [12]. Unmanned air crafts require a software-driven framework to handle battery failure issues and provide enhanced safety.

The contributions towards enhancing the authenticated arming and battery fail-safe mechanisms are as follows:

- The Randomized LTOTP is generated by performing an eXclusive OR (XOR) operation with a chaotic map-based random number and TOTP value. The proposed mechanism improves the randomness of OTP, thereby enhancing security.
- A Flag based Battery Fail-Safe (FBFS) mechanism is proposed to trigger the safe landing of drone only if the battery has not recovered after going below a threshold value for more than 3 times. Thus, FBFS prevents unsafe landing and increases the span or lifetime of the drone mission.

This paper is organized as follows. In Section II, literature related to UAV safety and security is discussed. In Section III, the proposed LTOTP is discussed in detail with necessary preliminaries. In Section IV, the proposed fail-safe system is elaborated. In Section V, the simulation results are presented and discussed. The work is concluded in Section VI, highlighting the results achieved.

II. Related Work

Various literature related to security and fail-safe mechanisms of UAVs are studied in detail and presented as follows:

Authentication is the primary security measure for many systems, which is achieved using encryption techniques, OTP, and so on. In [13], the TOTP generation algorithm is used for securing the Wi-Fi network. But the limitation of the design is that the user needs to generate TOTPs periodically to maintain the server link. Alternatively, [14] uses the OTP authentication mechanism based on the Advanced Encryption Standard (AES) and a Linear Congruential Generator (LCG). As AES performs 128 rounds of operations to generate a secret key, this mechanism increases the security establishment time and complexity.

To provide mutual authentication between the mobile terminal and the server, [15] uses a secure cross-layer authentication scheme by combining radio frequency fingerprinting with OTP. However, this method increases the authentication execution time, resulting in a decrease of transaction speed. A TOTP authentication via Secure Tunnel (TOAST) is used as an authentication scheme in [10]. TOAST is a mobile app that stores the seed value on mobile phones using a protective password key obtained from the server over a protective Transport Layer Security (TLS) tunnel and uses it to create OTP.

OTPs have also been employed in recent platforms such as those of cryptocurrency and blockchain. A secret key based TOTP generation is used as a security mechanism for cryptocurrency [16]. However, the use of same secret key throughout the session degrades the effectiveness of OTP. A two-factor authentication scheme based on TOTP is used in [9] for hyperledger fabric blockchain. Logistic maps can also be used to generate OTP [17]. In contrast to a normal logistic map, enhanced logistic maps have more randomness and chaotic performances [18]. A robust wireless network authentication for passengers at high-speed train is proposed in [8], which uses 2 chaotic maps to calculate OTP and improve security.

In addition to security, UAV's safety plays a vital role in many drone applications. Fail-safe mechanisms are the primary measure to ensure safety in drone missions. There are various fail-safe mechanisms in a drone like maintaining stability, battery monitoring, fault detecting, etc. A fail-safe system proposed in [19] activates an emergency parachute when the UAV is unable to maintain a stable flight. Servo actuator's failure may result in the loss of UAV controlling mechanism, which can lead to potential safety issues. In [20], a low-cost fault detection and fail-safe system are designed for detecting servo actuators breakdowns in mini-UAV.

Thus, in order to enhance the efficiency of the existing OTP mechanisms, the proposed Randomized LTOTP increases the randomness of the OTP using a logistic-chaotic map and Linear Congruential Generator (LCG). Additionally, the existing battery fail-safe is enhanced by the proposed FBFS mechanism by extending the flight time at low battery levels and preventing unsafe landing.

III. Randomized Logistic map based TOTP

Drone arming gives the operator full control over the drone and plays a significant role in UAV operations. Thus, the lack of security in this process can result in unauthorized arming and leads to misuse, crashing, stealing, etc. of drone and its data. In real drone flight scenarios, arming is done using the arming switch. The arming alert is turned on as soon as the switch is pressed. The arming alert is merely an indication of ongoing arming and signals user to stay away from the drone, as it may take off at any moment. However, arming alert does not guarantee successful drone arming. Hence, the proposed Randomized Logistic map based TOTP (Randomized LTOTP) authentication not only offers authorized arming but also confirms successful arming of the drone.

In the Randomized LTOTP algorithm, a random number generated using Logistic Chaotic-map based Random Number Generation (LCRNG) is XORed with a hash-based TOTP. Then the XOR value is shuffled using LCG to further increase randomness in OTP generation. The logistic chaotic map helps in improving OTP randomness; and TOTP authentication guarantees that OTP is valid only for 30 seconds, as it time-bounded. The Randomized LTOTP based on LCRNG, TOTP and LCG algorithms are discussed as follows.

A. Logistic chaotic-map based Random Number Generation

A chaotic map is a discrete map that depends on initial conditions and exhibits chaotic behaviour. Logistic map is a chaotic map and its randomness arise from very simple non-linear dynamical equations. Logistic map describes how the variable changes with time. In particular, the future value depends on the current value and a parameter (r). Therefore, it can be considered as a model for a time-varying system [18]. Randomized LTOTP uses a LCRNG algorithm to generate the initial random number, which is further processed with TOTP and shuffled using LCG.

A chaotic map is a function $f : S \to S$ where S is the sample space of function f and its expected outcome set is $O = \{O_1, O_2, \ldots\ldots, O_k\}$, where k is the number of possible outputs. Mathematically, logistic map is represented as $f(x) = x_{n+1} = rx_n(1 - x_n)$, where r is the parameter that controls the chaotic behaviour and x_n is the previous point in the map with x_0 as the initial point.

A partition of S has to be calculated to find the boundaries of the map. Let the partition be λ, and λ = $\{\lambda_1,\ \lambda_2....,\ \lambda_k\ \}$ and λ must meet the following condition

$$\begin{cases} \cup_{i=1}^{i=k}\lambda_i = \text{S} \\ \forall\lambda_i,\ \lambda j \in \lambda : \quad \lambda_i\ \cap\ \lambda j\ = \phi \\ \forall\lambda_i,\ \lambda j \in \lambda : \quad P[f(x) = \lambda i] = P[f(x) = \lambda j] \end{cases} \tag{1}$$

Algorithm 1 Logistic Chaotic-map based RNG

Input: Chaotic maps f_1 and f_2, initial states x_0 and y_0, number of OTP digits: n
Output: n-bit binary random number(R)

```
 1: for i = 1 to n  do
 2:     $x_i$ = $f_1(x_i) = rx_{i-1}(1-x_{i-1})$
 3:     $y_i$ = $f_2(y_i) = ry_{i-1}(1-y_{i-1})$
 4:     $bits$ = $\max(x_i, y_i)$
 5:     if $bits > 0.5$ then
 6:         $O_i$ = 1
 7:     else
 8:         $O_i$ = 0
 9:     end if
10: end for
11: Return $n$-bit binary random number (R)
```

The conditions for λ are explained as follows: i) when a union of all partition is performed, the sample space S must be obtained. ii) the partitions must be distinct and iii) the probability of $f(x)$ lying in the partition λ_i must be equal to that of λ_j.

The boundary value between λ_1 and λ_2 which satisfies (1) must be calculated. Calculation of boundary is crucial as it prevents the death of chaotic property due to boundary crisis. At boundary crisis, maximum value of 1 is reached by the map and chaotic property disappears.

However, we cannot obtain boundaries in S with the finite iteration results, since the boundaries change over the iterations [8]. To avoid this calculation overhead, Randomized LTOTP uses two logistic maps $f_1 : S \to S$ and $f_2 : S \to S$ with initial states x_0, y_0 and same r (r = 4) value. Their outputs can be determined in each iteration as $x_i = f_1(x_i)$ and $y_i = f_2(y_i)$, where

$$f_1(x_i) = \ rx_{i-1}(1-x_{i-1}) \tag{2}$$

$$f_2(y_i) = \ ry_{i-1}(1-y_{i-1}) \tag{3}$$

The binary output of an iteration for the random number generation can be determined by

$$O_i = \begin{cases} x_i, & x_i > y_i \\ y_i, & x_i < y_i \end{cases} \tag{4}$$

The randomness of logistic map can be proved mathematically by simply proving that $P[O = x_i] = P[O = y_i] = 0.5,\ 1 \leq i \leq n$. Let us consider that for both maps f_1 and f_2, their partitions are α = { α_1,...,α_k} and β = {β_1,...,β_k} respectively. According to (1), $\forall \alpha_i,\ \beta_j \quad P[f(x) = \alpha_i] = P[f(x) = \beta_j] = \dfrac{1}{k}$.

As f_1 and f_2 have same r value (r=4) and same number of iterations, the corresponding x_i and y_i are independent and fall in different regions [8]. Then the probability of getting x_i is

$$P[O = x_i] = P[x_i > y_i]$$

$$= \lim_{k\to\infty} \sum_{l_1=1}^{k-1} P[f_1(x_i)\ \in \alpha_{l_1}] \sum_{l_2=l_1+1}^{k} P[f_2(x_i)\ \in \beta_{l_2}] \tag{5}$$

= $\lim_{k\to\infty} \frac{k-1}{2k}\ = 0.5$

Similarly, the probability of getting y_i is

$$P[O = x_i] = P[x_i < y_i]$$

$$= \lim_{k\to\infty} \sum_{l_1=1}^{k-1} P[f_1(x_i)\ \in \alpha_{l_1}] \sum_{l_2=1}^{l_2-1} P[f_2(x_i)\ \in \beta_{l_2}] \tag{6}$$

= $\lim_{k\to\infty} \frac{k-1}{2k}\ = 0.5$

Therefore, from (5) and (6), the randomness of logistic map is proved. The random number generation process using LCRNG is described in Algorithm 1. LCRNG considers 2 logistic chaotic maps f_1 and f_2 and its initial states x_0 and y_0 as input. The generated output (R) is a n-bit binary number. In step 1, LCRNG iterates for n times to generate a n-bit random number. In every iteration, 2 values x_i and y_i using f_1 and f_2 are obtained. The maximum value of x_i and y_i is taken to decide the bit. If the maximum value is greater than 0.5 then bit is 1, otherwise 0.

B. Time-Based OTP

TOTPs are generated based on the uniqueness of the current time. It is an extension of Hash based Message Authentication Code (HMAC)-OTP (HOTP), in which a non-decreasing value based on the current time is used. TOTP mechanism is often used in many applications for increased security [9]. To generate TOTP in Randomized LTOTP, the drone and user must pre-establish the security parameters T_0, T_X and secret key K. The time counter C_T can be calculated using the following equation

$$C_T \ = \ \left[\frac{T \ - \ T_0}{T_x}\right] \tag{7}$$

where T_x , T and T_0 represents the number of duration count, unix time and epoch respectively. After calculating C_T from (7), the HOTP value is calculated. The HOTP value is a d-digit decimal value calculated using (9)

$$TOTP\ value(K) = HOTP\ value(K,\ C_T) \tag{8}$$

$$HOTP\ value(K,\ C_T) = HOTP(K,\ C_T)\ mod\ 10^d \tag{9}$$

where d is length of OTP

$$HOTP(K,\ C_T) = truncate(HMAC_H(K,\ C_T)) \tag{10}$$

Thus, HOTP is a truncation of the HMAC of the counter C_T with the secret key K, and an hash function H. The truncation takes the 4 least significant bits of the MAC and uses them as an offset, i, which is further used to select 31 bits from MAC, starting at bit $i + 1$. The truncated HOTP value from (10) is used in (8) to calculate the TOTP.

Algorithm 2 Randomized Logistic map based TOTP

Input: n-bit binary random number (R) from LCRNG and TOTP

Output:OTP for arming authentication

```
 1: n = 4*d
 2: for i = 1 to n  do
 3:     a = rand()
 4:     c = rand()
 5:     $X_i = (aX_{i-1} + c)\ mod\ m$
 6:     $nbit[i] = R[X_i]$
 7: end for
 8: for i = 1; i < n; i = i + 4 do
 9:     digit = Binary-to-integer(nbit[i:i+4])
10:     digit = to-string(digit)
11:     OTP = OTP + digit
12: end for
13: Send OTP to user via SMS
```

C. Randomized LTOTP generation

Randomized LTOTP generation XORs the random number generated by the logistic map and TOTP value calculated from (8) to produce the final n-bit random number, which is further rearranged randomly using LCG. This type of OTP generation produces more randomness than existing solutions and facilitates time-critical authentication. Thus, the Randomized LTOTP generation method improves the security in arming.

A LCG yields a sequence of pseudo-randomized numbers calculated with a discontinuous piece wise linear equation. Therefore, LCG can be used to randomly arrange the n-bit random number obtained by XOR of TOTP and the output of LCRNG (R). The XOR output of TOTP and R is represented as RNG. This RNG is provided as input to LCG for further randomization. Randomized LTOTP uses 4 bits per digit of OTP; thus, for a four digit OTP, it needs 16 (4*4) bits. Thus, the number of bits can be determined by $n = 4 * d$, where d is the number of digits required for OTP.

The LCG is defined mathematically by,

$$Y_{n+1} = (\alpha Y_n + c)\ mod\ m \tag{11}$$

where Y, α, c and Y_0 represents the sequence of pseudo-random numbers, multiplier, increment and initial value respectively. The increment and multiplier values are taken randomly to avoid repetition and period in modulo operation. The bits are randomly arranged and stored in a n-bit array. The final n-bit array is converted to d-digit OTP. The process of Randomized LTOTP is summarized in Algorithm 2. The algorithm considers n-bit output (R) from LCRNG and TOTP as input and generates a randomized LTOTP for arming as output. In step 1, the number of bits for OTP is calculated based on the number of digits required for OTP (d). The LCG is iterated for n times to shuffle the XORed value of LCRNG and TOTP. In steps 3 and 4, the increment (c) and multiplier (a) of LCG are taken as random values. In step 5 and step 6, LCG shuffles the input value and stores it in a n-bit array. Step 8 to 12 converts the bits into d-digit OTP. In step 13, Randomized LTOTP is sent to the user via SMS.

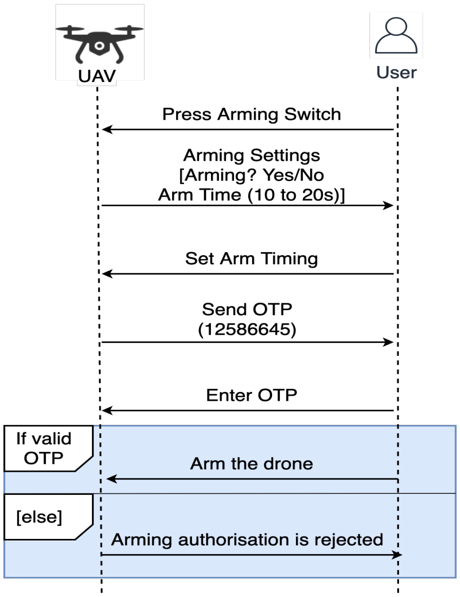

Fig. 1. Sequence Diagram of OTP based Arming of drone

The UAV is facilitated with a raspberry pi module interfaced with Global System for Mobile communications module to enable OTP communication with the user. When arming is turned on, a randomized LTOTP is sent to the authorized user by the UAV. The user enters the received OTP to arm the UAV. If the OTP matches, then user can arm the UAV; otherwise, the arming request is rejected. The process of authorized arming is illustrated in Fig. 1.

IV. Flag based Battery Fail-Safe Mechanism

Even if a UAV mission succeeds in offline testing, there are several reasons possible for a UAV to fail in completing the pre-planned mission path. Such unsuccessful flight missions may be due to unexpected levels of battery draining. To address the aforementioned issue, battery limit or size can be increased. However, this results in increased charging time and a reduction in payload. Further, longer charging periods at stations impacts consistent and productive flight missions. Thus, it might be challenging to tap the effectiveness of the upgraded battery, and therefore real-time missions are often planned with constrained battery limits.

In existing fail-safe systems, during a mission, when the battery level drops to low levels, the drone terminates the mission and comes back to land, by triggering of Return To Land (RTL) or LAND commands automatically. A Flag-based Battery Fail-Safe (FBFS) system is proposed to monitor the battery level at regular intervals throughout the mission and alert the user if the voltage drops below a threshold. Every time the battery goes below the specified threshold, a flag is incremented. If the flag is raised more than 3 times, the drone triggers the landing as the battery recovery chances are very low; otherwise, the drone continues the mission.

Algorithm 3 Flag based Battery Fail-Safe Mechanism

Input: Drone IP to arm drone
Output: Drone take-off, Voltage check and landing of drone

```
 1: Connect to the drone using IP of drone
 2: Perform Basic pre-arm check and ensure safe take-off
 3: while periodically monitoring battery and flag $< 3$ do
 4:     if battery_voltage $<$ 12.20 V and mode = AUTO then
 5:         Change mode to LAND
 6:         Increment flag
 7:     else if battery_voltage $>$ 12.20 V and mode = LAND then
 8:         Change mode to AUTO
 9:     else
10:         Continue the mission
11:     end if
12: end while
```

Algorithm 3 summarizes the proposed FBFS mechanism for UAVs based on the EFI engine. The Battery Fail-Safe algorithm receives the drone IP as input, and the output is drone take-off and landing control. In step 1 to step 2, the algorithm ensures that the drone is armed and is in the mission. Step 3 ensures that the drone's battery level is monitored periodically, and fail-safe flag is raised not more than 3 times. In step 4 to step 10, the algorithm checks if the battery voltage stays above 12.20 V threshold, then the mission continues; otherwise, it triggers LAND mode and the fail-safe flag is incremented once. If the battery voltage regains more than 12.20 V intermittently and if the mode is in LAND, the algorithm quickly switches the drone back to AUTO mode to continue the mission. Thus, the proposed battery fail-safe mechanism terminates the mission only when the battery power has gone below the threshold for more than 3 times. In other words, it prolongs the mission through battery monitoring using the EFI framework and facilitates safe landing.

V. Results and Discussions

The Randomized LTOTP algorithm and FBFS are implemented using DroneKit-Python and ArduPilot simulator. In addition, the Randomized LTOTP authentication uses a Raspberry Pi and GSM module for OTP communication with the user. DroneKit-Python communicates with drones over Micro Air Vehicle (MAV) Link, which enables programmatic access for features like telemetry and telecommand. The drone travels in the waypoints selected in the ArduPilot simulator.

The bifurcation diagram of the chaotic map implemented is shown in Fig. 2. When r is less than 3, the value generated by the logistic map is precise and stable. With r above 3, the values generated fork into two discrete ways. For instance, At $r = 3.2$, the map values oscillate solely between two values: one around 0.5 and the other around 0.8. Similarly, as r continues to increase, the map values bifurcate even more. At $r = 3.9$, the map has bifurcated so often that the generated values bounce randomly. The system is completely unpredictable at $r = 4$, which is the r value used in the implementation.

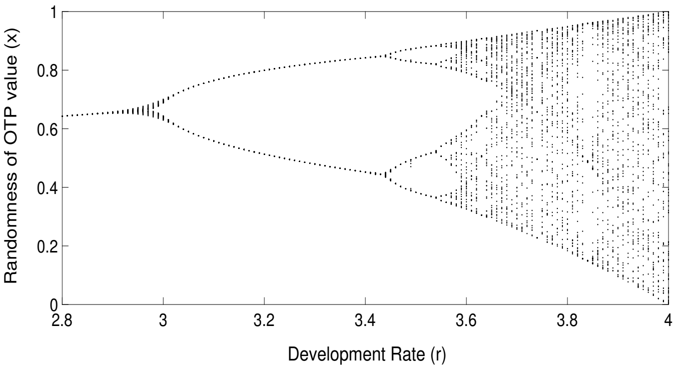

Fig. 2. Bifurcation diagram of Logistic map

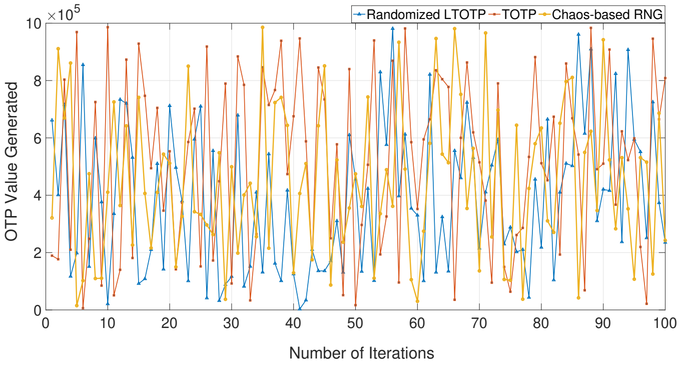

Fig. 3. OTP Values Comparison for various OTP algorithms

The graph in Fig. 3 shows the OTP values generated using the TOTP [9] algorithm, Randomized LTOTP algorithm and Chaos-based Random Number Generation (Chaos-based RNG) [8]. An analytical study called runs test is used to assess the randomness of OTP generated by the algorithms. In the runs test, the null hypothesis H_0, specifies that the sequence is in random manner and H_a is the alternative hypothesis. In the statistical runs test, the p-value is the probability of obtaining results as extreme randomness, assuming that the null hypothesis is correct. A smaller p-value indicates stronger evidence towards the alternative hypothesis. The p-value is plotted for the OTP algorithms, as shown in Fig. 4. Thus, the p-value of 0.9208 for Randomized LTOTP indicates that 92 out of 100 times the null hypothesis is true, which indicates increased randomness of the proposed algorithm. For chaos-based RNG algorithm [8], Enhanced Logistic Map (ELM) [18], TOTP algorithm [9] and HOTP algorithm [9], the p-value indicates that the randomness achieved out of 100 times are as follows: 76, 55, 3 and 2 respectively. Consequently, it is observed from these findings that the Randomized LTOTP indicates the highest randomness among the algorithms. The graph in Fig. 5 shows the drone flight time at low battery levels, while triggering existing fail-safe and FBFS algorithm. From the graph, it is observed that the FBFS extends the drone's flight time when compared to the existing fail-safe algorithm. Thus, FBFS facilitates safe landing at low battery levels.

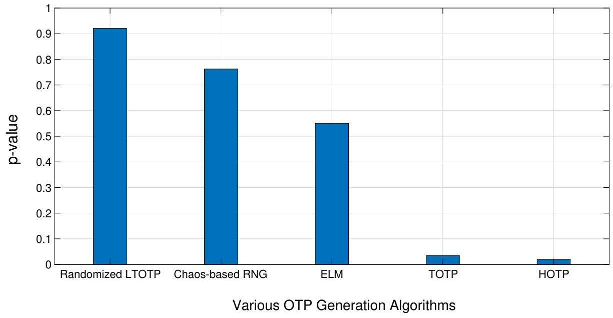

Fig. 4. Randomness Comparison for various OTP algorithms

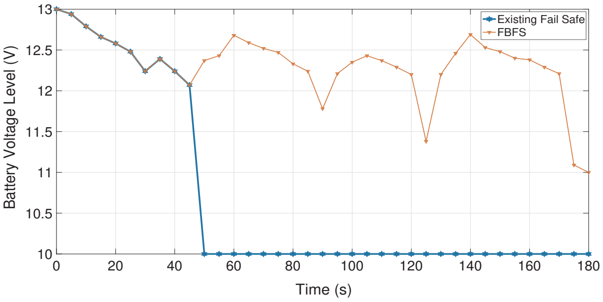

Fig. 5. Flight time comparison between existing fail-safe and FBFS

VI. Conclusion

UAVs are sophisticated technology and used across a wide range of applications. But, safety and security is still a concern in the design of many UAV applications. In order to prevent unauthorized arming, the proposed Randomized LTOTP mechanism uses a combination of logistic chaotic maps, TOTP, and LCG to improve the randomness of the OTP and to enable time-bound validity. The Randomized LTOTP mechanism provides 92% randomness and performs better when compared with other existing authentication mechanisms, thereby improving UAV security. To enhance the security of the Randomized LTOTP mechanism, the generated OTP value is made valid only for 30 seconds. To ensure the safety and reliability of UAV applications, the proposed FBFS mechanism continuously monitors the battery power and prevents unsafe landing of the drone at lower battery levels.

VII. Acknowledgement

This Publication is an outcome of the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia).

References

[1] G. Raja, S. Anbalagan, V. S. Narayanan, S. Jayaram, and A. Ganapathisubramaniyan, “Inter-UAV Collision Avoidance using Deep-Q-Learning in Flocking Environment,” in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 1089–1095, IEEE, 2019.

[2] *Commercial Drones Are Revolutionizing Business Operations*. Available at https://www.prnewswire.com.

[3] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, “Lightweight Security Authentication Mechanism Towards UAV Networks,” in *2019 International Conference on Networking and Network Applications (NaNA)*, pp. 379–384, IEEE, 2019.

[4] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir, “A Quantum-Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 681–690, 2020.

[5] D. Zhang, Y. Liu, L. Dai, A. K. Bashir, A. Nallanathan, and B. Shim, “Performance analysis of fd-noma-based decentralized v2x systems,” *IEEE Transactions on Communications*, vol. 67, no. 7, pp. 5024–5036, 2019.

[6] R. Arul, G. Raja, A. K. Bashir, J. Chaudry, and A. Ali, “A Console GRID Leveraged Authentication and Key Agreement Mechanism for LTE/SAE,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2677–2689, 2018.

[7] X. Jiang and J. Ling, “Simple and effective one-time password authentication scheme,” in *2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA)*, pp. 529–531, IEEE, 2013.

[8] T. Xu, D. Gao, P. Dong, C. H. Foh, H. Zhang, and V. C. Leung, “Improving the Security of Wireless Communications on High-Speed Trains by Efficient Authentication in SCN-R,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7283–7295, 2019.

[9] W.-S. Park, D.-Y. Hwang, and K.-H. Kim, “A TOTP-based two factor authentication scheme for hyperledger fabric blockchain,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 817–819, IEEE, 2018.

[10] M. L. T. Uymatiao and W. E. S. Yu, “Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore,” in *2014 4th IEEE International Conference on Information Science and Technology*, pp. 225–229, IEEE, 2014.

[11] E. F. Costa, D. A. Souza, V. P. Pinto, M. S. Araújo, A. M. Peixoto, and E. P. da Costa, “Prediction of Lithium-Ion Battery Capacity in UAVs,” in *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pp. 1865–1869, IEEE, 2019.

[12] “hardware design of a small uas helicopter for remote sensing operations,”

[13] C. Sudar, S. Arjun, and L. Deepthi, “Time-based one-time password for Wi-Fi authentication and security,” in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1212–1216, IEEE, 2017.

[14] Imamah, “One time password (otp) based on advanced encrypted standard (aes) and linear congruential generator(lcg),” in *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, pp. 391–394, 2018.

[15] Y. Chen, H. Wen, H. Song, S. Chen, F. Xie, Q. Yang, and L. Hu, “Lightweight one-time password authentication scheme based on radio-frequency fingerprinting,” *IET Communications*, vol. 12, no. 12, pp. 1477–1484, 2018.

[16] K. A. Taher, T. Nahar, and S. A. Hossain, “Enhanced cryptocurrency security by time-based token multi-factor authentication algorithm,” in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 308–312, IEEE, 2019.

[17] W. Chankasame and W. San-Um, “A chaos-based keyed hash function for secure protocol and messege authentication in mobile ad hoc wireless networks,” in *2015 Science and Information Conference (SAI)*, pp. 1357–1364, IEEE, 2015.

[18] D. Herbadji, N. Derouiche, A. Belmeguenai, T. Bekkouche, A. Labiad, M. Lashab, and A. Herbadji, “A New Image Encryption Scheme Using an Enhanced Logistic Map,” in *2018 International Conference on Applied Smart Systems (ICASS)*, pp. 1–6, IEEE, 2018.

[19] V. K. Tofterup and K. Jensen, “A methodology for evaluating commercial off the shelf parachutes designed for suas failsafe systems,” in *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 129–137, IEEE, 2019.

[20] G. Fuggetti, A. Ghetti, and M. Zanzi, “Safety improvement of fixed wing mini-UAV based on handy FDI current sensor and a FailSafe configuration of control surface actuators,” in *2015 IEEE Metrology for Aerospace (MetroAeroSpace)*, pp. 356–361, IEEE, 2015.