

# Hyperelliptic curve based authentication for the internet of drones

Aloy Anuja Mary Gnanaraj, Farithkhan Abbasali, Aanandha Saravanan Kumar,  
Sathyasri Bala Subramanian, Murugan Chinnathambi

Department of Electronics and Communication Engineering,  
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

## Article Info

### Article history:

Received Sep 17, 2022

Revised Jun 3, 2023

Accepted Jun 30, 2023

### Keywords:

Elliptic curve security

FANET

Hyperelliptic curve

Internet of drones

Unmanned aerial vehicles

## ABSTRACT

Drones provide an alternative progression in protection submissions since they are capable of conducting autonomous seismic investigations. Recent advancement in unmanned aerial vehicle (UAV) communication is an internet of a drone combined with 5G networks. Because of the quick utilization of rapidly progressed registering frameworks besides 5G officialdoms, the information from the user is consistently refreshed and pooled. Thus, safety or confidentiality is vital among clients, and a proficient substantiation methodology utilizing a vigorous sanctuary key. Conventional procedures ensure a few restrictions however taking care of the assault arrangements in information transmission over the internet of drones (IOD) environmental frameworks. A unique hyperelliptical curve (HEC) cryptographically based validation system is proposed to provide protected data facilities among drones. The proposed method has been compared with the existing methods in terms of packet loss rate, computational cost, and delay and thereby provides better insight into efficient and secure communication. Finally, the simulation results show that our strategy is efficient in both computation and communication.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Aloy Anuja Mary Gnanaraj

Department of Electronics and Communication Engineering

Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology

Chennai, Tamil Nadu, India

Email: draloyanujamary@veltech.edu.in

## 1. INTRODUCTION

Unmanned aerial vehicle (UAV) has comparable characteristics to the internet of things (IoT) technology; hence the phrase "internet of drones" was coined. Internet of drones (IoDs) is considered to be a favorable field with various potential benefits such as providing services such as traffic reconnaissance, rescue, and combinational search [1]. IoD is defined as when data is forwarded for additional decision-making by a band of internet-connected vehicles with such an array of the sensor. Many drones form a network and share the collected information in the IoD environment [2]. This environment can be considered an important solution thereby supporting coordination among UAVs and other issues related to UAV communications [3]. Some of the application fields related to IoD are disaster management, geographic mapping, precision agriculture, search and rescue, entertainment, and aerial photography, which is shown in Figure 1. IoD comprises a combination of technologies such as cloud, edge, internet, and 5G services [4]. IoD becomes a vital thing in day-to-day life for various real-time applications like monitoring defense areas, flooded areas, and land sliding areas. Thus, IoD provides support to the traveling experience with safe navigation and road safety [5]–[7]. To facilitate the IoD network, the flying Ad hoc networks (FANETs) has been introduced composing drones that

are used for private and public applications. Some of the interfaces which are used to control the drones are PC, internet, remote control, and cloud environment [8]. Several routing and security challenges have been presented when we incorporate UAVs with IoD. Maintaining security and achieving privacy is a major challenge in IoD related to mobility and accuracy [9]. Certain common trials in UAV-constructed IoD networks are routing, critical-time reaction, data acquisition, and data endorsement. Thus, it is important to do the accurate validation of data from preventing spam messages from entering the UAV [10].



Figure 1. Drone applications

The various jamming attacks that can breach security privacy are signal, global positioning system (GPS), and data. Because of these attacks, the UAV system can get collapsed and lead s to misinterpretation of data [11]. Various attacks such as data packet inoculation, eavesdropping, renunciation of service, backdoor access, baiting, GPS spoofing attacks, are the one that varies from the physical layer to the application layer.

Thus, the main contribution of the proposed approach is described as follows: i) develop an approach to validate the incoming communications, and collect, analyze, and verify the data sent to IoD or UAV; ii) elucidate the methodologies related to authentication and provides more solutions based on IoT-related security applications; and iii) utilize the mathematical concepts of hyperelliptic curve cryptography for data authentication and validate the results with the existing elliptic curve approach for providing better services.

## 2. SECURITY THREATS BASED ON IOD

Nowadays threats have been increased due to unauthorized access and thereby exploiting vulnerabilities. Attacks are classified as active or passive attacks which are prone to cyber-security threats based on the fact that relies on wireless channels for communication [12]. Some of the IoD vulnerabilities gray hole attacks, black hole attacks, wormhole attacks, and fake information dissemination (FID) attacks were analyzed and their performance can be measured utilizing hyperelliptic curve-based authentication algorithms [13], [14]. The cyber security based on IoD attacks is mentioned in Figure 2.

### 2.1. Gray hole attack

The most commonly used algorithms in device-to-device (D2D) communication is optimized link state routing protocol (OLSR). One of the major attacks in OLSR is a gray hole or node isolation attack. In this attack, malicious nodes in the network interrupt the data transmission and transmit false information [15]. Nodes in the network may act as both normal and malicious. Because of this attack, the topological information gets shared within the network and thereby exploiting the vulnerabilities. This may divert the paths and degrades the performance of the throughput and packet delivery ratio [16].

## 2.2. Blackhole attack

In this attack, whenever a node receives an route request (RREQ) packet a blackhole (BH) node starts sending forged route reply (RREP) indicating the cost-effective path even when the destination entry is missing from the routing table [17]. Due to this effect, a malicious node creates the RREP packet and discards the messages received from other intermediate and destination nodes. Thus, malicious node receives all the communicated information from the connected nodes and tries to modify the information [18].

## 2.3. Wormhole attack

One of the major threatening attacks is a wormhole attack on UAVs in which a hostile node receives a data packet and tunnels it to another hostile node which then circulates it to the neighboring nodes [19], [20]. Multiple methods are possible to establish the tunneling are a channel established out of band, a high-powered transmission, and an encapsulated attack. An attack has been created and the effect has been identified by establishing a hostile node as a decoy between the source and destination and able to perform subversions such as packet droppings and manipulation [21], [22].

## 2.4. FID occurrence

It is an occurrence where an aggressor transmits a fake GPS signal and variates the route of the drone. The attacker performs the attack by broadcasting interferences between the source and hostile node to depreciate the location estimated for the drone [23]. There are various strategies to alleviate the problems encountered by an FID attack. The various cyber threats in a UAV have been discussed in the above content. The following section 3 comprises literature findings related to cyber threats, their challenges, and their solutions. Section 4 discusses the proposed hyperelliptic curve cryptography-based authentication. Section 5 discusses the results and discussion based on cyber threats. The last section concludes the parameter analysis and solution improvements.

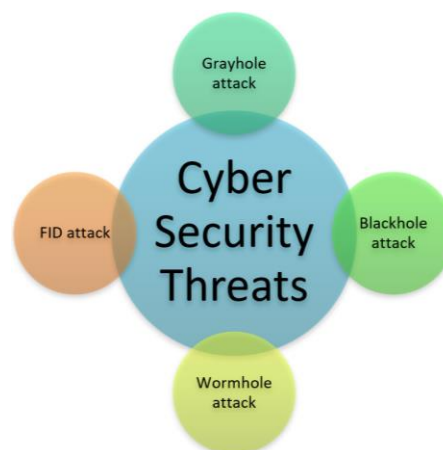


Figure 2. Cyber security threats

## 3. RELATED WORKS

Alzahrani *et al.* [24] concentrated mainly on security related and presented an efficient and privacy-preserving authentication protocol for the internet of vehicles (IoVs). Since the vehicle suffers from attacks such as physical, side channel, and cloning attacks the author introduces road side units (RSU) gateways. It also applies physically unclonable functions (PUFs) to guarantee security characteristics. Three-layered infrastructure architecture is proposed for IoVs for storing secret information. The proposed protocol proves that it provides lower security overhead, and higher throughput and demonstrates robustness against various types of attacks.

Aman *et al.* [25] demonstrated that a more accurate and efficient crowd management process can be made by unmanned aerial vehicles. The environmental-related surveillance data can be monitored and collected by UAVs for sharing information among each other. In mission-critical applications, the battery-operated UAV faced more challenges based on security and privacy. A new insubstantial validation arrangement for UAV situations was introduced to enable the weakness of the existing schemes. An intermediate control center

provides authentication between the user and UAV. The performance requirement of the UAV has been fulfilled utilizing the symmetrical key and elliptical curve crypto mechanism.

Chen *et al.* [21] presented the security issues in smart internet of drone utilizing a software agent named an intelligent personal assistant. The author suggested an efficient authentication protocol named a lightweight privacy-preserving scheme using chebyshev chaotic maps. The proposed protocol proves the robustness of IoD using a verification tool and a random oracle model. This considers the desirable characteristics such as period, computational complexity, key agreement, and authentication. For speeding up the process, the methodology considered a secret token and dynamic user authentication between the communication entities. The authentication process utilized only fewer cryptographic operations to meet the constraints of surveillance systems and proves the effectiveness of the proposed protocol.

Hussain *et al.* [19] discussed that IoV is subject to security issues such as replay, modification, and impersonation attacks. Since there is continuous technological development in hardware where it leads to accelerated growth in IoD. Various schemes are there to measure security breaches and the proposed method considered in this work is the formal Random oracle method. For providing security between the drone and the user, the author considered an ECC and symmetric key primitives-based approach. The scheme proves a better trade-off between security and throughput for drones and is best suited for gaining surveillance.

Li *et al.* [14] suggested that 5G drones play a vital role in the field of various applications specifically in the military and civilian environment. This IoD can able to track individuals and enforce social distancing during the pandemic situation. However, it is suffered from issues such as security and privacy. Blockchain technology provides the solutions for the above issue and has proven that it is best suited for operative environments.

Michailidis and Vouyioukas [12] stated that the security factor is crucial since UAV operational range grows exponentially. This work discussed various cyber-attacks and their causes which impact on day-to-day normal life. The methodology discussed was the STRIDE attack paradigm which provides an effective solution for GPS spoofing and denial-of-service (DoS) attacks. Possible ways to create cyber-attacks on UAVs are password theft, brute force, and mathematical assaults. Password theft can be cracked by using symbols, phrases, and numbers. Brute force attacks can be analyzed by finding short passwords in all possible configurations. Mathematical assault can use statistical methods by guessing a byte from a word. In GPS spoofing, the attacker creates a jamming signal which interferes with the general GPS signal. Thus, malfunction was performed by using GPS spoofing attack. In a DoS attack, the intruder commands and maintains access to a UAV network. The malfunction in the DoS attack was performed by flooding the system with requests or packets.

Qureshi *et al.* [10] proposed the methodology named hominoid-sovereignty cooperative methodology where humanoid geo-position is used for detecting UAV cyber-attacks. An experiment named research environment for supervisory control of heterogeneous unmanned vehicles-swarm attack (RESCHU-SA) methodology is used to analyze the cyberattacks for better security guaranteed. In this work the human act as a supplementary sensor by successfully detecting a spoofing attack.

Sun *et al.* [9] suggested that the common cyber security threads are protocol-grounded attacks, sensor-grounded attacks, negotiated modules, and jammers. The countermeasures for protocol-based attacks are security of communication, data confidentiality protection, replay attack, privacy leakage, and de-authentication attacks. The solution for sensor-based attacks is GPS spoofing/jamming attacks, motion sensors spoofing, and UAV spoofing/jamming attacks. The compromised component problem can be alleviated by IoT security threats and control/data interception. Similarly, jammers are denial of service and stop packet delivery.

Wu *et al.* [8] discussed the vulnerability of cybersecurity attacks namely DoS and DDoS attacks. One of the big challenges in UAVs is to transfer consistent data packets from the foundation to the endpoint UAV. Thus, this paper focused on DoS and DDoS attacks utilizing deep learning algorithms and analysis of the various kinds of threat casing clang-of-death attacks. A bio-inspired algorithm Ant Hoc Net practices the concept of an invasion discovery scheme and the same is to be investigated with other protocols. The model outcomes demonstrated that the anticipated process attains better security than other contemporary protocols.

Saravanan *et al.* [3] suggested that authentication and encryption are necessary between the drones and server for secure communication. A proposed methodology named mutual authentication and key agreement protocol is used to verify the intended user's certificate. The author suggested that to verify the certificate elliptic curve digital signature algorithm (ECDSA) algorithm is used and the elliptic-curve Diffie-Hellman (ECDH) algorithm is preferred to share the common value. Better security has been achieved by elliptic curve cryptography (ECC) even with smaller key sizes when compared to Rivest Shamir Adleman (RSA) and digital signature algorithm (DSA) signature schemes. A simpler key derivation process is followed for exchanging smaller information and communication paths between the IoD and server.

## 4. METHOD

### 4.1. Hyperelliptical curve cryptosystem arithmetic

Various community key cryptography approaches are available such as asymmetric cryptography algorithm, ElGamal cryptosystem, and elliptical curve crypto procedure, one of the public key cryptography protocols (PKC) which is similar to ECC is hyperelliptical curve cryptosystem (HECC). It consists of an algebraic curve viewed as an overview of elliptical curves. The genus of the HECC curve is defined as  $\geq 1$  whereas the genus is equal to 1 for ECC. The standard equation for HECC is normally represented  $v^2 + h(v)u = f(u)$  where  $h, f \in k(u)$   $f$  is monical polynomial, degree polynomial  $f = 2n + 1$ , degree polynomial  $h \leq n$  and if  $y^2 + h(x)y = f(x)$   $x, y \in j * j$  for, then  $2y + h(x) \neq 0$ .

### 4.2. Proposed method

Reliable and resilient is a simple public-key entity in cryptography that serves as either a digital certificate as well as an encrypt at about the same time. Cryptography and digital certificates are two fundamental cryptography tools that ensure security, trustworthiness, and quasi. This mechanism is a relatively recent cryptography approach that expresses the service's success in a logically consistent manner. Especially compared to conventional cryptography and verification techniques, it greatly decreases storage requirements and transport overhead expenses. With such a smaller byte size and small computing costs, hyperelliptical curve encryption delivers superior protection. Both accuracy and confidentiality constraints for a decentralized cryptographic focus mainly our suggested hyperelliptic curve decentralized secret technique as shown in Figure 3.

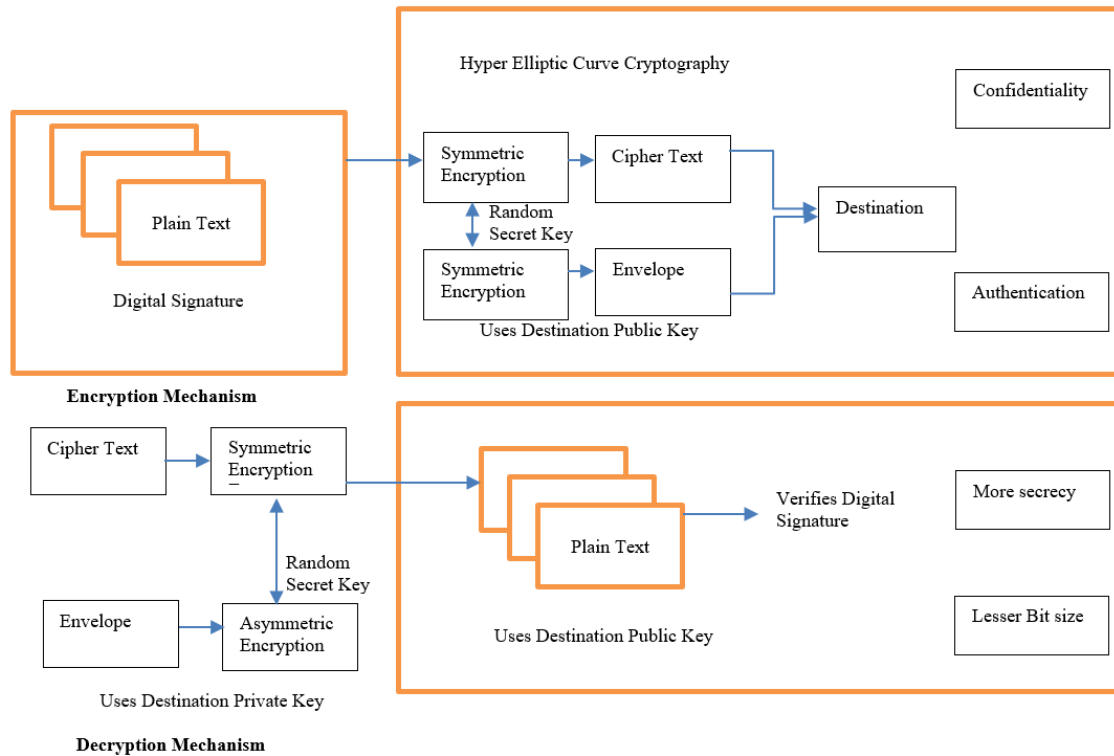


Figure 3. Encryption and decryption mechanism for HECC protocol

The proposed methods generate two authentication tokens, one for the subgroups and the other for the exterior grouping. In a dispersed context, all of those are efficient after locating the private cryptographic key portable node or validator for subgroups as well as the exterior grouping. In this technique, the durability could be computed using the mobility node's energy. This technique is intended for portable devices with limited autonomy in a decentralized system. The HECC is an asymmetrical community key cryptography approach that uses a pair of keys. Each individual seems to have a set of community and secret keys. The secret key can be used for decrypting and signatory generation, while the community key is being used for signatory authentication as shown in Figure 4. Key contract, encrypt, and signatory approaches are three types of schemes built on hyperelliptical curve cryptographic is discussed in following subsection.

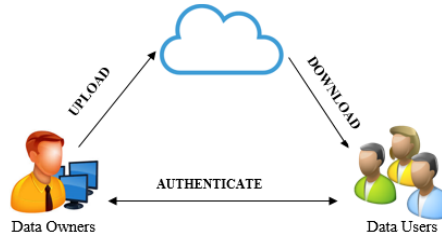


Figure 4. Authentication model in the cloud

#### 4.3. Key contract

To produce the pair of keys, the client uses the HECC protocol. The pair of keys are denoted by the characters  $P_k, d$ , with  $P_k$  denoting the community key and  $d$  denoting the secret key. Although the Diffie-Hellman-based consensus mechanism was created for the multiplication series of data, this can simply be adapted to other categories. Look at the case of  $G$ , groups where members could be effectively expressed but whose grouping functions could be effectively assessed. The grouping consists of hyperelliptic curve Jacobians. Let us assume the succeeding community factors:

- The grouping ' $G$ '.
- A component  $R \in G$  of the larger prime directive  $r$ .

#### 4.4. Encrypt/decrypt approach

When transferring the information to the cloud, the information owner would encrypt them using the community key  $P_k \rightarrow E$ . The computed hash function is saved for later validation, and the encrypted information is transferred to the internet. If  $A$  wishes to transmit  $B$  an information packet, it must first transmit  $M$  to  $B$ .

- It achieves the community key  $P_k$  of receiver user  $B$ .
- It picks a private number  $a \in [1, r - 1]$ .
- Calculate the assessment  $C_1 = a * R$ .
- Calculate the assessment  $C_2 = M + a(P_k)$ .
- Direct  $(C_1, C_2)$  to  $B$ .

Whenever an information customer requires to view a document, a downloading query is sent to the internet, and the information is decrypted using a cipher text. The hashing calculation is performed once more when the material has been retrieved. When comparing files, the authenticity of the files can now be confirmed. Because the document would be uploaded to the cloud, a hashing code is compared would be useful in determining whether a document is flawless while still on the server. The "receive user"  $B$  can decipher the cloud documents by undertaking the succeeding:

- Receive the user the cipher text of the document  $(C_1, C_2)$  from the source  $A$ .
- Evaluate the information assessment  $M = C_2 - bC_1$ .

#### 4.5. Signatory approaches

The electronic signatures process could be used to generate and verify every grouping  $G$  certificate. Transmitter  $A$  must accomplish the following to authenticate a document  $M$ . Indicate an arbitrary integer  $k \in [1, r - 1]$ , and estimate  $Q = kR$ :

- Estimate  $s$  from  $H(M)$  and  $a$ .
- Currently, the signatory is  $(M, Q, s)$ .
- To "authenticate this signatory at the receiving end, the authenticator  $B$  has to carry out the following steps".
- Estimate  $v_1$  and  $v_2$  from  $H(M)$  and  $\phi(Q)$ .
- Estimate  $V = v_1R + v_2P$ .
- Admit the signatory if  $V = Q$ . Else, discard it.

### 5. RESULTS AND DISCUSSION

The proposed model is simulated on NS3 to pronounce the broadcast among various drones through secure authentication for every drone happening through wireless networks. Numerical analysis of the proposed approach is preminent over conventional methodologies such as elliptic curve cryptographic source

authentication scheme based on chebyshev polynomial (ECCPSAS), novel light weight user authentication system (NLWUAS), and multilayer authentication strategy (MAS) by taking into account various parameters such as announcement overhead, envelope transfer proportion, and output delivery.

The performance of communication overhead shown in Figure 5 proves that the proposed HEC delivers an average of 44.60% of overheads that are reduced as compared with other conventional approaches. The proposed methodology reduces the overhead by 7.07%, 18.96%, and 99.14% when compared with ECCPSAS, NLWUAS, and MAS respectively. The enactment of packet delivery is shown in Figure 6 demonstrates that the proposed HEC delivers on an average 10.85% increase in delivery of packets as compared with other conservative approaches. The projected methodology increases the packet delivery ratio by 2.4%, 14.3%, and 15.9% when compared with ECCPSAS, NLWUAS, and MAS respectively. The performance of throughput shown in Figure 7 proves that the proposed HEC delivers an average 49.9 % increase in throughput as compared with other conventional approaches. The proposed methodology increases the throughput by 87.11%, 26.63%, and 35.8% when compared with ECCPSAS, NLWUAS, and MAS respectively. The performance of termination to termination delay is shown in Figure 8 proves that the proposed HEC delivers an average 62.65% decrease in termination to termination delay as compared with other conventional approaches. The proposed methodology decreases end-to-end delay by 8.73%, 80.63%, and 98.6% when compared with ECCPSAS, NLWUAS, and MAS respectively.

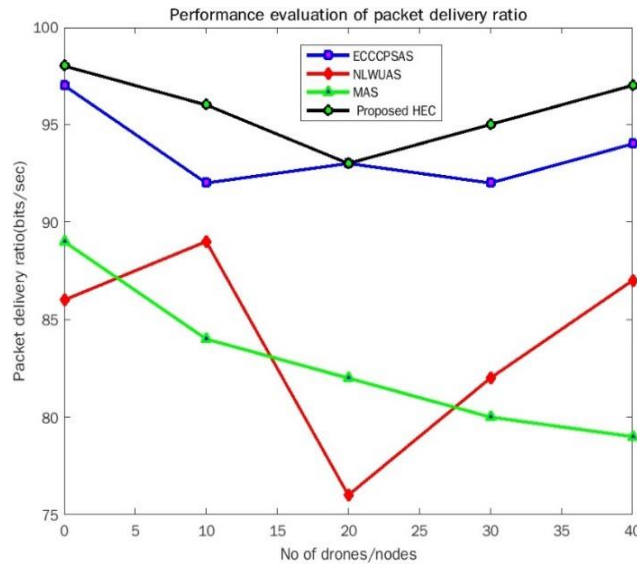


Figure 5. Analysis of packet delivery ratio among various drones

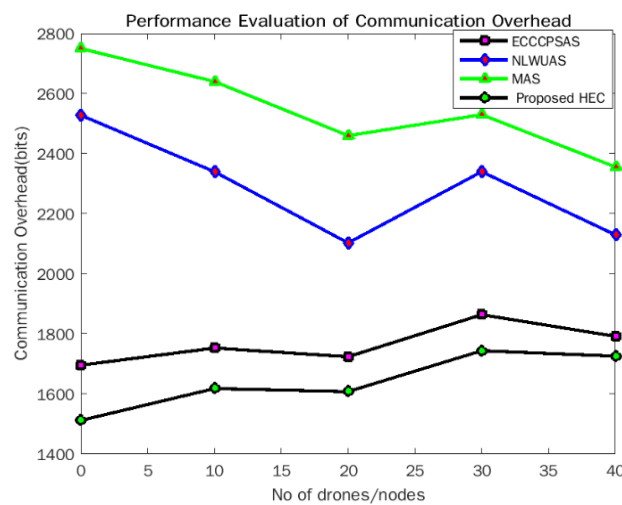


Figure 6. Analysis of communication overhead among various drones



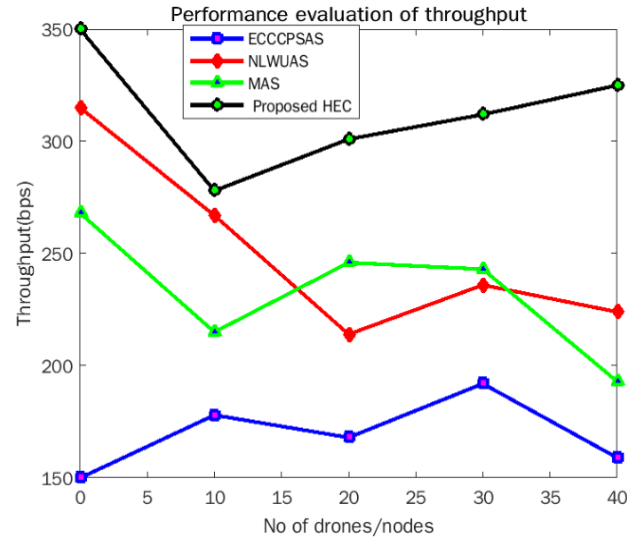


Figure 7. Analysis of throughput among various drones

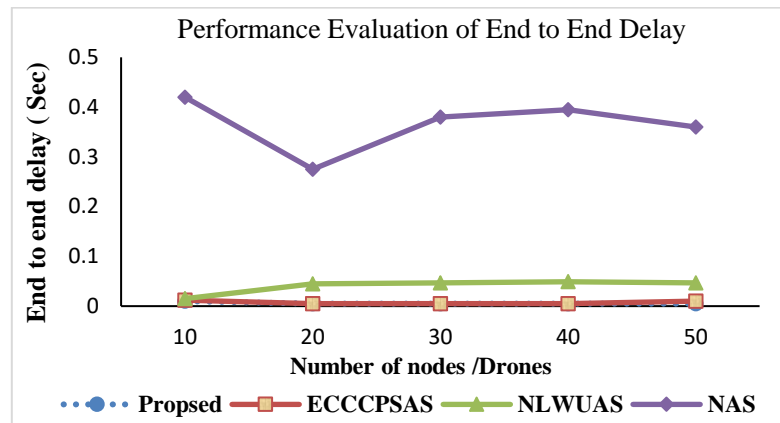


Figure 8. Analysis of end end delay among various drones

## 6. CONCLUSION

The proposed hyperelliptical curve cryptosystem based substantiation methodology is proposed to protect validation services among users in progressive grid schemes. This method also provisions for sharing information between users/drones with server configurations using efficient authentication. There is an improved quality of service (QoS) constraint regarding data transmission when employing the proposed methodology. When compared to ECCCPAS, NLWUAS, and MAS, the proposed methodology enhances throughput by 87.11%, 26.63%, and 35.8%, respectively. And also, the HEC reduces end-to-end delay by an average of 62.65% with lower end-to-end delay by 8.73%, 80.63%, and 98.6% when compared to ECCCPAS, NLWUAS, and MAS, respectively. As compared to existing previous methodologies, the proposed one ensures perfect secrecy and privacy using an authentication approach. This can be extended shortly by implementing some hybrid approaches based on the hyperelliptic curve cryptosystem.

## ACKNOWLEDGEMENTS

We are very grateful to the management of Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai for supporting to do this study.

## REFERENCES





- [1] T. Patel, N. Salot, and V. Parikh, "A systematic literature review on security of unmanned aerial vehicle systems," *Prepr arXiv221205028*, Dec. 2022.






- [2] Y. Mekdad *et al.*, "A survey on security and privacy issues of UAVs," *Computer Networks*, vol. 224, Apr. 2023, doi: 10.1016/j.comnet.2023.109626.
- [3] K. A. Saravanan, N. V. Prasanna, D. Balaji, S. Sivakumar, and K. Karthick, "Public key cryptanalysis scheme using hierarchical structure in wireless sensor networks," *International Journal of Electronics and Communication Engineering*, vol. 7, no. 1, pp. 7–12, 2014.
- [4] S. Ponnann, A. K. Saravanan, C. Iwendi, E. Ibeke, and G. Srivastava, "An artificial intelligence-based quorum system for the improvement of the lifespan of sensor networks," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 17373–17385, Aug. 2021, doi: 10.1109/JSEN.2021.3080217.
- [5] H. Zhu, M. Elfar, M. Pajic, Z. Wang, and M. L. Cummings, "Human augmentation of UAV cyber-attack detection," in *AC 2018: Augmented Cognition: Users and Contexts*, 2018, pp. 154–167, doi: 10.1007/978-3-319-91467-1\_13.
- [6] Y. Zhou, T. Liu, F. Tang, and M. Tinashe, "An unlinkable authentication scheme for distributed IoT application," *IEEE Access*, vol. 7, pp. 14757–14766, 2019, doi: 10.1109/ACCESS.2019.2893918.
- [7] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: attacks, limitations, and recommendations," *Internet of Things*, vol. 11, Sep. 2020, doi: 10.1016/j.iot.2020.100218.
- [8] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5G-enabled drone communications," *IEEE Network*, vol. 35, no. 1, pp. 50–56, Jan. 2021, doi: 10.1109/MNET.011.2000166.
- [9] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fog-based crowd sensing on the internet of vehicles," *Journal of Network and Computer Applications*, vol. 134, pp. 89–99, May 2019, doi: 10.1016/j.jnca.2019.02.018.
- [10] K. N. Qureshi, M. A. S. Sandila, I. T. Javed, T. Margaria, and L. Aslam, "Authentication scheme for unmanned aerial vehicles based internet of vehicles networks," *Egyptian Informatics Journal*, vol. 23, no. 1, pp. 83–93, Mar. 2022, doi: 10.1016/j.eij.2021.07.001.
- [11] J. A. Onieva, R. Rios, R. Roman, and J. Lopez, "Edge-assisted vehicular networks security," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8038–8045, Oct. 2019, doi: 10.1109/JIOT.2019.2904323.
- [12] E. T. Michailidis and D. Vouyioukas, "A review on software-based and hardware-based authentication mechanisms for the internet of drones," *Drones*, vol. 6, no. 2, Feb. 2022, doi: 10.3390/drones6020041.
- [13] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 120–137, Apr. 2021, doi: 10.1080/23742917.2020.1846307.
- [14] K. Li, W. F. Lau, M. H. Au, I. W.-H. Ho, and Y. Wang, "Efficient message authentication with revocation transparency using blockchain for vehicular networks," *Computers and Electrical Engineering*, vol. 86, Sep. 2020, doi: 10.1016/j.compeleceng.2020.106721.
- [15] F. Li, H. Zhang, L. Gao, J. Wang, C. Sanin, and E. Szczerbicki, "A set of experience-based smart synergy security mechanism in internet of vehicles," *Cybernetics and Systems*, vol. 50, no. 2, pp. 230–237, Feb. 2019, doi: 10.1080/01969722.2019.1565115.
- [16] I. U. Khan, A. Abdollahi, M. A. Khan, M. A. Khan, and I. Ullah, "Securing against DoS/DDoS attacks in internet of flying things using experience-based deep learning algorithm," *Research Square*, 2021, doi: 10.21203/rs.3.rs-271920/v1.
- [17] A. Khan, F. Aftab, and Z. Zhang, "BICSF: Bio-inspired clustering scheme for FANETs," *IEEE Access*, vol. 7, pp. 31446–31456, 2019, doi: 10.1109/ACCESS.2019.2902940.
- [18] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019, doi: 10.1109/TVT.2019.2894944.
- [19] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for internet of drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021, doi: 10.1109/JSYST.2021.3057047.
- [20] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Computer Communications*, vol. 162, pp. 102–117, Oct. 2020, doi: 10.1016/j.comcom.2020.08.016.
- [21] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, no. 1, Jan. 2020, doi: 10.3390/electronics9010062.
- [22] A. Chen, K. Peng, Z. Sha, X. Zhou, Z. Yang, and G. Lu, "ToAM: a task-oriented authentication model for UAVs based on blockchain," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13638-021-02039-6.
- [23] S. A. Chaudhry, "Correcting 'PALK: password-based anonymous lightweight key agreement framework for smart grid,'" *International Journal of Electrical Power & Energy Systems*, vol. 125, Feb. 2021, doi: 10.1016/j.ijepes.2020.106529.
- [24] B. A. Alzahrani, A. Barnawi, and S. A. Chaudhry, "A resource-friendly authentication protocol for UAV-based massive crowd management systems," *Security and Communication Networks*, vol. 2021, pp. 1–12, Nov. 2021, doi: 10.1155/2021/3437373.
- [25] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, Jan. 2021, doi: 10.1109/JIOT.2020.3010893.

## BIOGRAPHIES OF AUTHORS






**Aloy Anuja Mary Gnanaraj**     working as a professor in the Department of Electronics and Communication Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. She graduated in electronics and communication engineering at Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu, India. She secured a master of engineering in communication systems at National Engineering College, Kovilpatti, Tamil Nadu, India. She graduated Ph.D. in the field of quantum cryptography at the College of Engineering, Guindy, Chennai, India. She is in the teaching profession for more than 16 years. She has presented several papers in national and international journals, conferences, and symposiums. Her area of interest includes wireless networks and quantum computing. She can be contact at email: draloyanujamary@veltech.edu.in.






**Farithkhan Abbasali**    received a B.E. degree in electronics and communication engineering from Anna University, Chennai, in 2005, and an M.E. degree in communication systems from Anna University of Technology, Coimbatore 2009 respectively. He has been pursuing his Ph.D. in Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, since 2016. Currently, he is working as an assistant professor at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. He has got 12 years of experience in teaching. He has published more than 10 papers in various reputed journals and conferences. His research interests include wireless sensor networks, cryptography and information security, computer networks, machine learning, and deep learning. He can be contact at email: farithkhan@veltech.edu.in.






**Aanandha Saravanan Kumar**    is currently working as an associate professor in the Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. He received his B.E degree in the department of Electronics and Communication Engineering from Madras University in 1998 and his M.E. degree in communication systems from Anna University in 2006. He also obtained Ph.D. in wireless sensor networks from Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. He has more than 22 years of experience in research and teaching. He has published more than 20 papers in international and national journals. His research includes wireless networks, the internet of things, body area networks, and artificial intelligence. He can be contact at email: aanandhasaravanan@veltech.edu.in.



**Sathyasri Bala Subramanian**    working as an associate professor in the Department of Electronics and Communication Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. She graduated in electronics and communication engineering at Rajalakshmi Engineering College, Chennai, Tamil Nadu, India. She secured a master of engineering in embedded systems technologies at Vel Tech, Chennai, Tamil Nadu, India. She graduated Ph.D. in the field of wireless networks at the College of Engineering, Guindy, Chennai, India. She is in the teaching profession for more than 18 years. She has presented several papers in national and international journals, conferences, and symposiums. Her area of interest includes wireless networks, IoT, cognitive radio, and wearable technologies. She can be contact at email: sathyasrib@veltech.edu.in.



**Murugan Chinnathambi**    working as an assistant professor in the Department of Electronics and Communication Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. He graduated in electronics and communication engineering at Sri Nanthanan College of Engineering and Technology, Tirupattur, Tamil Nadu, India. He secured a master of technology in networking engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India. He is in the teaching profession for more than 8 years. He has presented several papers in national and international journals, conferences, and symposiums. His area of interest includes wireless communication and data networks. He can be contact at email: muruganc@veltech.edu.in.