Towards Efficient Security-based Authentication for the Internet of Drones in Defense Wireless Communication

P. TAMIL SELVI
Michael Job College of Arts and Science for Women
T. Santhi Sri
Koneru Lakshmaiah Education Foundation
M. Nagabhushana Rao
Vidya Jyothi Institute of Technology
ramesh babu (rameshbssv@gmail.com)
Raghu Institute of Technology
K Venkateswar rao
IT & Technical Consultant
Abhiram Srikanth
Ahmedabad University

Research Article

Keywords: Internet of things, internet of drones, unmanned aerial vehicles, authentication, security, wireless communications

Posted Date: June 18th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-612545/v1

Towards efficient security-based authentication for the internet of drones in defense wireless communication

P. TAMIL SELVI[1], T.Santhi Sri[2], M. Nagabhushana Rao[3], BSSV Ramesh Babu[4], K Venkateswara Rao[5], Mr. Abhiram Srikanth[6]
[1]Department of Information Technology, Michael Job College of Arts and Science for Women, Sulur, Coimbatore
[2]Department of CSE, Koneru Lakshmaiah Education Foundation
[3]Department of IT, Vidya Jyothi Institute of Technology, Hyderabad.
[4]Department of ECE, Raghu Institue of Technology, Visakhapatnam.
[5]IT & Technical Consultant, Computer Science Department, Vijayawada, AP, India
[6]Department of Physics, Ahmedabad University, Navrangpura, Ahmedabad, Gujarat
[1]tamilselvigrgsat@gmail.com, sri_santhi2003@yahoo.com, mnraosir@gmail.com,
[4]rameshbssv@gmail.com, [5]mailtovenkibujji@gmail.com, [6]abhiram.s@ahduni.edu.in

Abstract

Drones are the recent advancements in defense applications as they can perform unmanned aerial surveys. The internet of drone (IoD) is an emerging concept in drone/node communication, which has evolved with the 5G oriented networks. Due to the rapid usage of high-speed advanced computing systems and 5G networks, the user data is continuously updated and shared. Therefore, security/privacy is necessary between users and an efficient authentication approach using a robust security key. Existing techniques have several limitations while handling the attack sequences in data transmission over IoD environment systems. A novel elliptic curve cryptographic-based Chebyshev polynomial source authentication schema (ECCCPSAS) is proposed to enable secure data services between users to access information directly from one drone/node authorized access from other drone/user in 5G network systems. Also, use Elliptic curve cryptography for secure authentication to each node to share session key with a similar secure channel to transmit data with interactive computational complexity and secure communication in wireless IoD. The theoretical security-related analysis presented in this paper gives better insight into efficient, secure data transmission with increased quality of service parameters described in wireless IoD environment.

Key Terms: Internet of things, internet of drones, unmanned aerial vehicles, authentication, security, wireless communications.

1. Introduction

Internet of things (IoT) is the combination of interrelated computed devices that share data via communication systems [1]. Internet of drones (IoD) is the structured layout network to explore and exchange/access data in between unnamed area vehicles (UAV) to control and providing navigation services and airspace [2] [3]. IoD offers various services like surveillance of traffic, delivery of packet ratio, rescue, and search combinations [4]. The IoD has become most popular today to provide different applications that describe people's lives [5],[6]. An essential representation of IoD concerning various services and entities .i.e. Unnamed Area Vehicles (UAV)

and also consists of external users with control rooms (i.e., internal servers) [7-9]. Based on general architecture, each drone computes the following services in figure 1 concerning control of normal and flight with sensor communications [10].

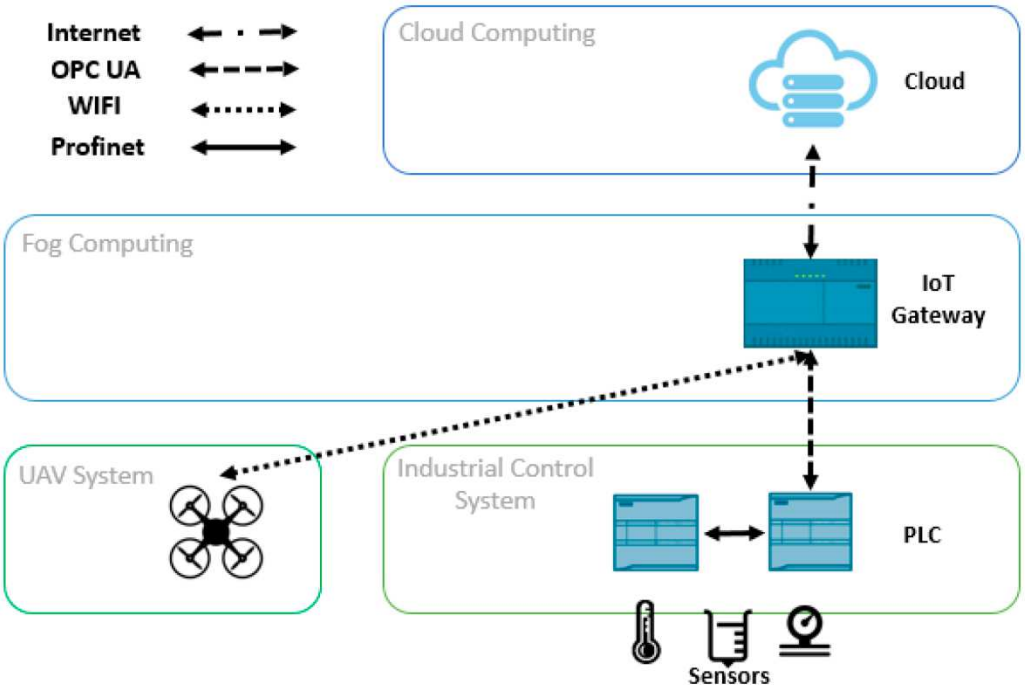

Figure 1 Monitoring services of drones with gateway network computing environment.

As shown in figure 1, each drone computes different services like power consumption via inbuilt sensors [11-14], data communication, actuators, and sensor communication with energy supply between drones [15]. Each drone present in the zone sent required information to the control room at the server; inbuilt sensors present in the drone explore information via physical media in wireless network communication [16]. For efficient data accumulation in IoD, many security/privacy-related challenges are present in the IoD network described in [17, 18].

Different types of traditional approaches were introduced to provide efficient and reliable data transmission over IoD-based network communication. Hassanalian and Abdelkefi et al.; gave a study on flying automatons, ranging from unmanned air vehicles to shrewd clean. Moreover, they talked about the structure and manufacture difficulties of small-scale ramble, existing techniques for expanding their continuance, and different route and control procedures [19]. Furthermore, they also examined the current automatons' confinements just as the proposed answers for the up-and-coming age of automatons.

Gharibi et al. exhibited a theoretical model for designing the Internet of Drones (IoD) based framework. The key ideas of three existing enormous scale systems, for example, aviation authority organize, cell system, and internet, are investigated to the novel engineering for ramble traffic the executives [20],[21]. Lobby et al.; talked about the open doors accessible to improve

open and business ramble activities. For example, automatons, such as military automatons and rebellious automatons, are additionally given in [8] wireless communication over IoD environment.

Security is the major challenge in accessing different nodes/drones; based on real-time data [22,23], various threats should be protected to secure IoD environment [24]. Each user should understand and acquire data from real-time applications for different drones via a specific drone zone; it is achievable for each user to explore data from nodes/drones. Because of third-party services present in network/network, IoD has different cyber-related vulnerabilities [25]. To acquire efficient analysis of cyber vulnerabilities, IoD applications monitor security, avoid a collision, and extend the security features to provide traffic efficiencies in crowd space (which is the place to contain different drones) [26]. So that in data sharing (&) communication between other drones, they carried out ad hoc features in handling data transmission at a specific range [27]. Because of unstable network connectivity, the data transmission quality is the major obstacle to exploring and controlling drones in a network [28].

The principal intention behind this research is to provide multi-level security for different users by accessing data from drones within the network region [29, 30]. This issue happens only if users directly access real-time related data from servers in the IoD environment [31]. Therefore, to access data from real-time streams, users need to access data from accessed drones with authorized drone access to restrict unauthorized access of data from done presently in IoD environment. This procedure motivates to implementation of an efficient and secure authentication approach in IoD security environment. So that in this paper, we propose a novel Elliptic curve cryptographic based Chebyshev polynomial Source Authentication Schema (ECCCPSAS). This approach describes Chebyshev polynomial for different nodes over finite characteristics with trapped vulnerabilities. For efficient authentication between users/clients, use the elliptic curve crypto system to provide authentication to the entire user with server communication in a wireless infrastructure-oriented IoD environment.

The main contributions of this approach are as follows:

a) Describe the authentication-related methodologies used in IoT-related security applications and gives more solutions.
b) We propose Chebyshev polynomial Source Authentication schema to enable and provide efficient, secure authentication over nodes in IoT-related Wireless environments.
c) Use Chebyshev polynomials for linear data transmission between drones and also enable different characteristics in wireless communication.
d) Also, use Elliptic curve cryptography for secure authentication and enable services with interactive communication described in wireless 5G networks.
e) Explore different experimental results of the proposed approach regarding traditional approaches like novel lightweight user authentication scheme (NLWUAS), multi-level authentication scheme (MAS) in wireless ad hoc IoD environment.

2. System Design & Implementation

The proposed approach permits proficient energy with data transmission and gadget revelation in the 5G-based IoT and BSNs utilizing various UAVs. Right off the bat, we present the underlying framework model, traffic model and afterward assess the energy standards over the at first characterized framework model.

a) Basic Network Model

The network involves a zone isolated into a progression of macrocell indicated by set M. These macrocells fill in as the entryway to all the IoT and BSN gadgets for conveying over different cells. The femtocells uphold the development of a network between the body sensors and give availability to the IoT. Leave W alone the arrangement of tiny cells, which structure the center layer between the macrocell and the femtocells. All together to give on-request backing to availability between the macrocell and the femtocells, a set U of UAVs is sent in which UAVs structure their tiny cells named as "UAV little cell."

UAVs' small cell arrangement permits better inclusion just as better availability since UAVs can be sent on demand, accordingly, settling Ubuntu Network Tool in the 5G networks. The whole network involves a set V of sensors supporting BSN just as IoT

b) Basic Preliminaries Used in Construction of Authenticated Network Model

The basic preliminaries relate to Chebyshev polynomial [2] [4] in reliable data streaming with basic definitions as follows:

Let us consider $m \in h \,\&\, a \in [-1,1]$, if Chebyshev polynomial definitions $P_m(a) = [1,-1] \to [1,-1]$, iterations from $P_m(a)$ is described as

$$P_m(a) = 2aP_{n-1}(a) - P_{n-2}(a), m \geq 2 \quad \ldots\ldots\ldots\ldots (1)$$

$$P_0(a) = 1.P_0(a) = a \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

As a result, Chebyshev polynomial are described as algebraic polynomials [5], so that extended version of finite field H_t

Let $a, m \in H_t, m \geq 2$ be the set and T be a prime number for recursive relations described as

$$P_m(a) : H_T \to H_T, P_m(a) = \left(2aP_{m-1}(a) - P_{m-2}(a)\right)\left(\bmod t\right), m \geq 2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\text{And } P_0(a) = 1(\bmod t), P_1(a) = a(\bmod t) \quad \text{..... (4)}$$

Sub set characteristics of Chebyshev polynomial on the basic of authenticated key exchange with

$$P_n\left(P_n(a)\right) = P_{n-m}(a) = P_m\left(P_n(a)\right)\left(n, m \in H\right) \quad \text{..... (5)}$$

Basic property relates to finite field communication, based on above equation 2-5 $a, n, m \in H_t, n, m \geq 2$

$$\begin{aligned} &P_n\left(P_m(a)\right)\left(\bmod t\right) = P_n\left(P_m(a)(\bmod t)\right)\left(\bmod t\right) \\ &= P_{n-m}(a)(\bmod t) \\ &= P_m\left(P_n(a)(\bmod t)\right)\left(\bmod t\right) \\ &= P_m\left(P_n(a)(\bmod t)\right) \end{aligned} \quad \text{..... (6)}$$

We define Chebyshev polynomial from eq(6) formula described as follows:

$$\begin{aligned} &P_0(a) = 1 \bmod t \\ &P_1(a) = x \bmod t \\ &P_n(a) = 2 \times a \times P_{m-1}(a) - P_{m-2}(a) \bmod t \end{aligned} \quad \text{..... (7)}$$

$t \in \mathrm{T}, a \in [0, t-1] \,\&\, m \in \mathrm{M}.$ Can be changed with from eq (7)

$$P_m(a) \bmod p = \frac{\kappa_1^m + \kappa_2^m}{2} \bmod t \quad \text{..... (8)}$$

It be the Chebyshev polynomial description with different parameters

c) Elliptic Curve Cryptography with different polynomials

For example p>3, be an odd unique primary number from (8). Elliptic curve EC is defined as follows:

$$EC : y^2 = x^3 + xa + a \bmod t, \quad \text{..... (9)}$$

Where a,b belongs to F_t and $6a^3+27b^2 = 0$ mod t. Combination of set $EC(F_t)$, consists of all points (x,y) belongs to F_p on the same curve and combine with special point O, we will call it as infinity of point in curve.

For sending information from source to destination, verification of generated keys in source side and destination may verify using signature generation & verification procedures in network communication, these two procedures having following steps for cryptography signature verification in communication between different nodes.

Step 1: Generate random integer K_X , $1 \le K_X \le M-1$

Step 2: Calculate r = x_X mod M, where $(x_X;y_X) = k_X G$. If r = 0, go back to step 1.

Step 3: Calculate $z_X \leftarrow z(n,r)$, z be the hash related function, such as SHA-1, and _ denotes the bit format of hash function.

Step 6: Calculate $s = rd_X h_X + K_X \bmod M$, s = 0, go back to step 2.

Step 5: pair (r; s) is the signature

Verification of signature procedure having following steps in source authentication in network communication,

i. Identifies that $Q_X \neq O$, invalid communication
ii. Identifies that lies on the curve
iii. Identifies that QX = O

Finally, generation and verification in-network message communication from the above equations (9) as follows:

$$\begin{aligned}(x_1, x_2) &= sG - rh_X Q_X \\ &= (rd_X z_X + k_X)G - r_X Q_X \\ &= k_X G + rz_X Q_X - rz_X Q_X \\ &= k_X G\end{aligned} \qquad \text{..... (10)}$$

Therefore, we have x_1 = r, and the verifier should Accept the signature of each node/drone with different parameters in IoD environment

d) Novel Authenticated Privacy Model

The proposed approach consists of five different phases for providing privacy to the data sharing in drones. This involves in initialization of drone/node, registration of drone, secure authentication to drone, and update authentication data to the drone.

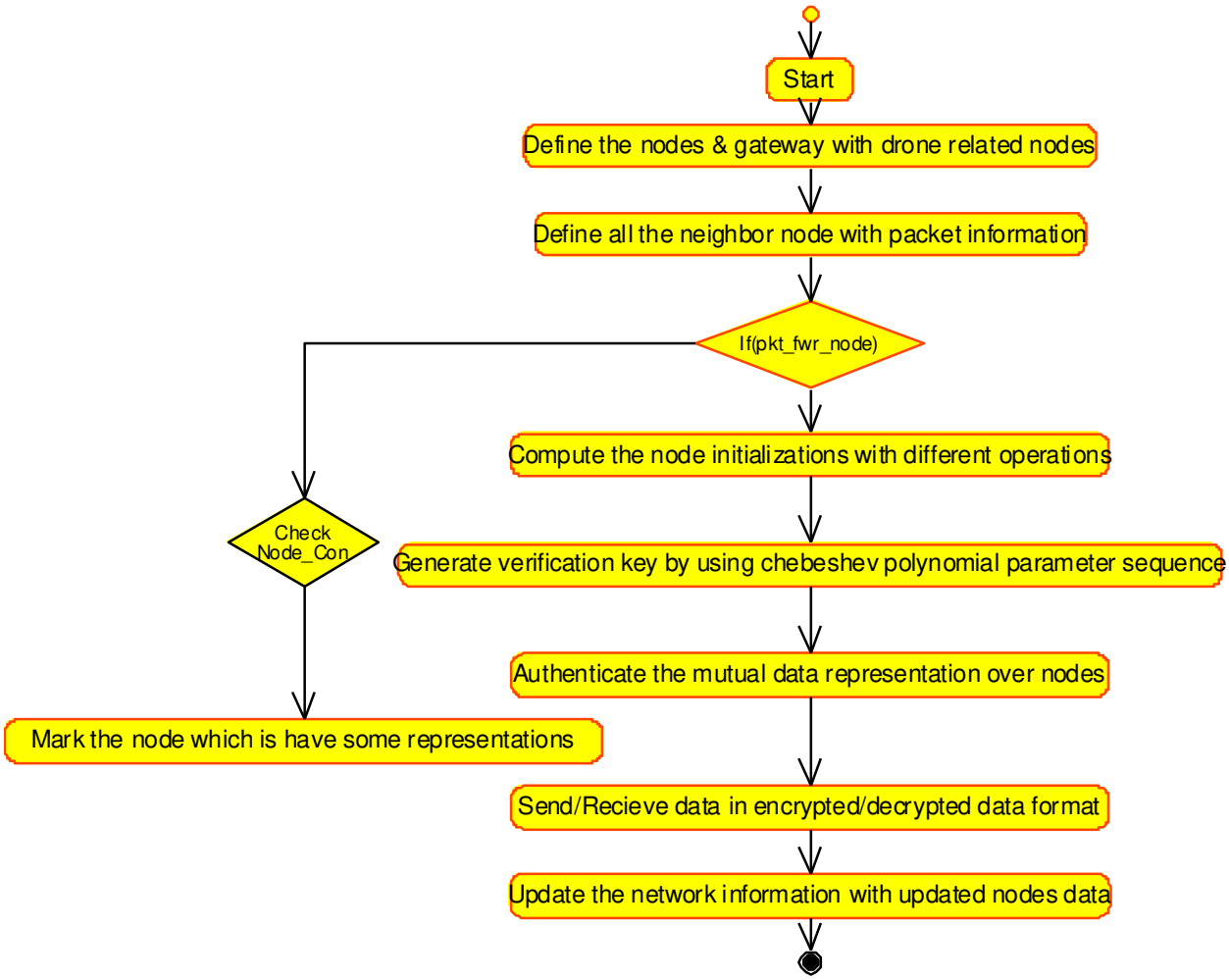

Figure 2 Proposed flow chart of data transmission in 5G related wireless network communications

The proposed technique is mentioned in Figure 2, which represents secure user authentication concerning mutual intention between different users in wireless network transmission. First, initialize all the nodes/drones with respect to malicious nodes in packet data transmission. All the nodes check every time with polynomial key secure authentication with neighbor node and compute malicious node identification in wireless ad hoc 5G networks.

3. Experimental Evaluation

This section describes the performance of the proposed approach to existing approaches, i.e. a novel lightweight user authentication scheme (NLWUAS), multi-level authentication scheme (MAS) in IoD environment. Use the latest NS3 simulator to describe the data transmission between different drones with secure authentication for all the drones/nodes in wireless communication. For secure data transmission, use elliptic curve cryptography with a different Hellman algorithm for each node 32-64 bits transmission for the public cryptosystem. Numerical results are

introduced to show the approval and viability of the proposed plans. We expect that the height of the UAV is fixed at H = 100 m. +e number of GTs is N = 10, and they are consistently dispersed inside a 2D roundabout zone with a range 0.8 km. +e QoS prerequisite for each GT is Qm = 30Mbits. We set the correspondence transmission capacity B = 1 MHz, and the commotion power ghostly thickness is N0 = −170 dBm/Hz. +e commotion delay, packet transmission, energy is σ2 = N0B = −110 dBm. We likewise accept that the steady transmission intensity of each GT is P = 10 dBm, and the reference-got signal-to-commotion proportion is c0 = 80 dB.

In addition, from equations (12-15), we set c1 = 9.26 × 10−4 and c2 = 2250. +e limit precision ε in Algorithm 1 is set as 10−6. +e beginning and last areas of the UAV are thought to be q[1] = q[M] = [500, 0]T. +e most extreme speed and increasing speed of the UAV are set as Vmax = 100m/s and amax = 5m/s2, individually. +e beginning and last speeds are accepted as v[1] = v[M] = [0, 30]T. Figure 6-7 shows the throughput of each GT for various period times. We can see that the difference in throughput per GT is firmly identified with time and area. For model, for the tenth GT, its throughput quickly increments from T = 100 s to T = 120 s, which implies that the UAV can accomplish a premium channel to speak with the tenth GTin the later skyline time, prompting a higher transmission rate. Note that, for the three plans, the throughput of each GTis not monotonically expanding as to the skyline time. The period can influence the UAV's direction, and afterward, it affects the channel conditions, which impacts the GT planning. Then again, if the UAV flies without thinking about QoS necessities (i.e., the unique case II), it very well may be seen that the throughput of the third and seventh GTs are underneath the QoS edge, as appeared in figures 2 and 3.

The throughput of the third GT is zero in Figures 6– 7, which implies that the third GT isn't designated any space to send information. Subsequently, in extraordinary case II, the UAV can't guarantee the base correspondence necessity for each GT. Concerning the plan with average time portion, each GT is designated an equivalent number of time allotments for transferring information to the UAV. Subsequently, these GTs' throughputs are moderately standard and even. Notwithstanding, the ideal EE of this case is the most minimal, as appeared in Figure 8. Figure 8 shows the combination execution of the proposed Algorithm 1. In this outcome, we think about three configuration plans for T = 140 s. It tends to be seen that the energy productivity increments quickly with the number of emphases toward the start and afterward rises gradually until it meets the recommended exactness. Furthermore, it is watched that the UAV can accomplish higher Efficient Energy (EE) when it flies without thinking about QoS necessities, and the UAV's EE is least at the point when it receives the strategy for regular time assignment, which is by our experiments.

For efficient communication overhead evaluation, identify each bit of data transmission from 32-160 bits, apply secure algorithm with ECC on each node point $T = T_x + T_y$ for 160 bits compare with traditional approaches in communication cost compared and values described in table 1.

Table 1 Communication overhead for data transmission between nodes.

No. of drones/nodes	ECCCPSAS (Comm... bits)	NLWUAS (Comm... bits)	MAS (Comm... bits)
10	1696	2528	2750
20	1753	2340	2640
30	1724	2103	2460
40	1864	2340	2530
50	1792	2100	2356

As shown in table 1, figure 3 describes the increased number of nodes in wireless data transmission, then automatically secure communication is very high in the proposed approach with low floss in bit transmission.

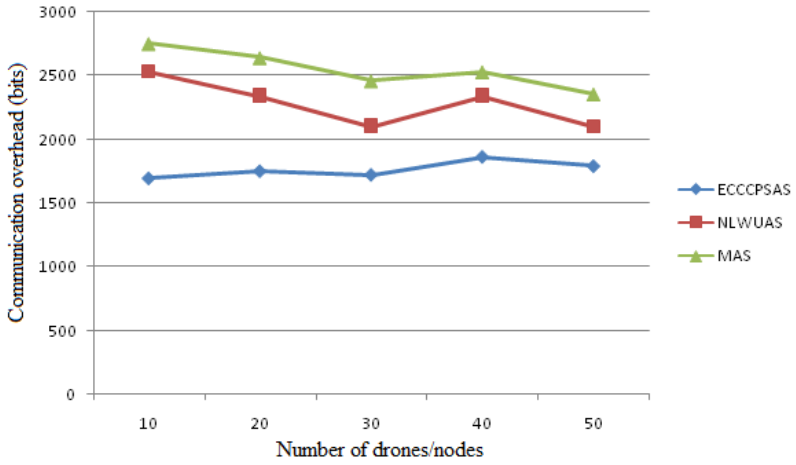

Figure 3 Performance evaluation of communication overhead

The data transmission rate for other drones/node communication is described in table 2 as per the evaluation plot in figure 4.

Table 2 Packet delivery ratio values with different node/drone communication

No. of drones/nodes	ECCCPSAS (Comm... bits)	NLWUAS (Comm... bits)	MAS (Comm... bits)

10	97	86	89
20	92	89	84
30	96	76	82
40	92	82	86
50	94	87	79

As described in figure 4, table 2, if the server increases the drones with efficient data transmission between drones, then automatically increase the delivery ratio of the proposed approach compared to traditional techniques because of communication overhead in wireless IoD medium.

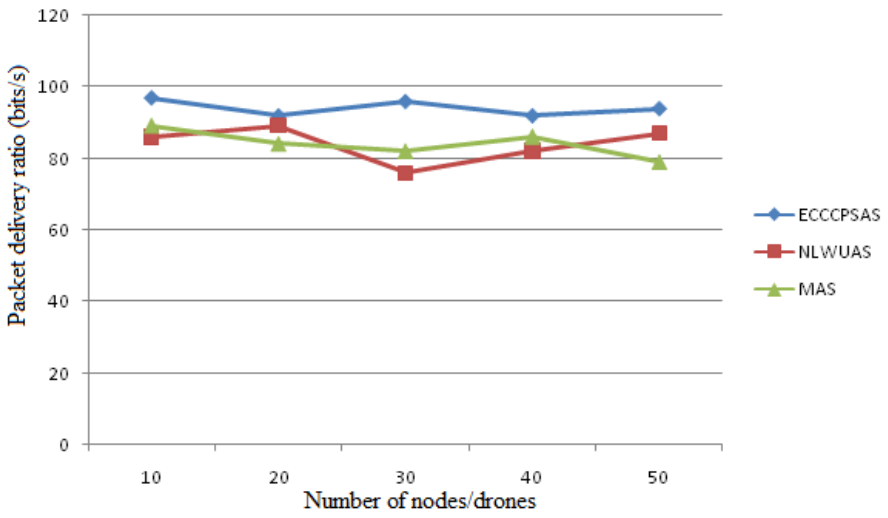

Figure 4 Performance evaluation of packet delivery ratio with different drone/node communication

Based on data transmission, the throughput evaluation of the proposed approach establishes better and efficient communication between different nodes in the wireless medium concerning the throughput values described in table 3 and figure 5 with bits transmission.

Table 3 Throughput values with different bit communication.

No. of drones/nodes	ECCCPSAS (Comm... bits)	NLWUAS (Comm... bits)	MAS (Comm... bits)

10	150	315	268
20	178	267	215
30	168	214	246
40	192	236	243
50	159	224	193

As described in figure 5 and tables, they describe the performance evaluation of throughput for different node communication in a wireless IoD environment. We observe that the proposed approach gives better throughput results with respect to secure data transmission in evaluating bits transmitted between nodes.

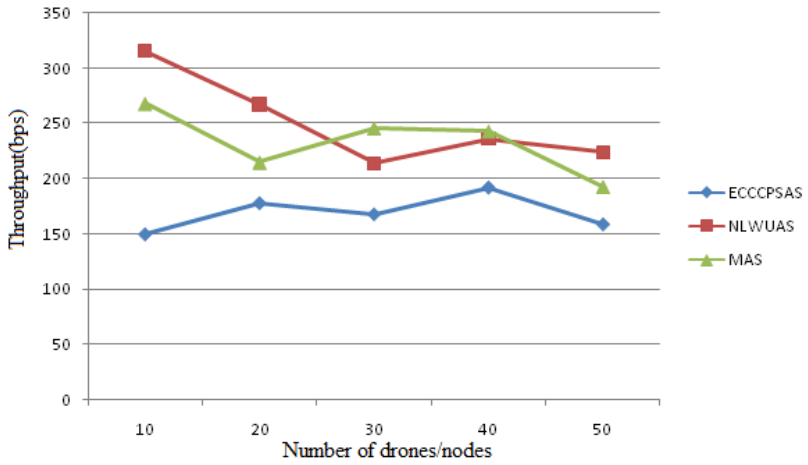

Figure 5 Performance evaluation of throughput with respect to transmission bits

The end-to-end delay between different nodes concerning data transmission with time constraints applied on each node with secure communication: delay values and performance evaluation described in table 4 and figure.6.

Table 4 End-to-end delay values with data transmission.

No. of drones/nodes	ECCCPSAS (Comm... bits)	NLWUAS (Comm... bits)	MAS (Comm... bits)
10	0.0018	0.023	0.42
20	0.0024	0.034	0.28
30	0.0038	0.038	0.38

40	0.0026	0.046	0.39
50	0.0042	0.039	0.37

As described in figure 6, it shows end-to-end delay is very low in the proposed approach because of communication overhead and delivery ratio and throughput variations in wireless IoD environment.

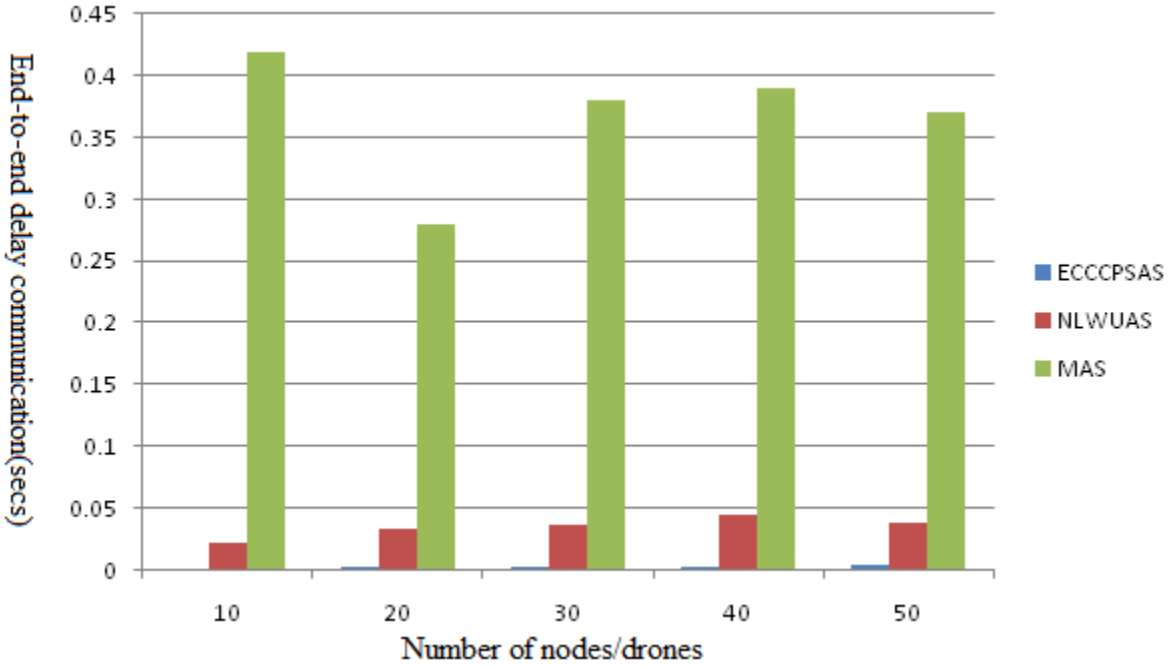

Figure 6 Performance of end-to-end delay over node communication in wireless 5G networks.

We computed different network parameters during the implementation experiment to improve the quality of service parameters with other notations in wireless communication. Finally, based on the above results, our proposed approach gives better and efficient results to improve network performance with varying inscriptions in wireless IoD environments.

4. Conclusion

In this paper, a Novel Elliptic Curve Cryptographic based Chebyshev Polynomial Authentication Approach is propose to enable the secure authentication services between users in IOD based advanced network systems. It supports efficient authentication to data accessed drone with server configuration in sharing information between users/drones. In this approach, use verification-based session key for efficient and successful privacy and mutual authentication between drones associated with users which drones are securely communicated and also prevent different types of

guising attacks to be stopped as adversary. We also use Chebyshev polynomial-based approach on client server architecture to support efficient verification in the IoD-based network environment. It is an advanced computing approach to enable security and resist different types of attack sequences and reduce the time cost for computing data transmission. Numerical results of this approach suggest improving quality of service parameters with respect to secure data transmission.Compared to existing approaches, the simulated results show high throughput and data transmission and decrease the delay and computation overhead in data transmission. Thus significant results are achieved from consumption of computational overhead, end-to-end delay and packet loss and other sequential parameters. Further improvement of this work is to extends and provide secure energy-aware communication overhead described in future enhancement

Compliance with Ethical Standards

There is no funding for this work.

Disclosure of potential conflicts of interest

No Conflict of Interest.

Research involving human participants and/or animals

Not applicable

References

[1] Ashok Kumar Das, Mohammad Wazid, “Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment”, IEEE INTERNET OF THINGS JOURNAL, 2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

[2] Lin C, He D, Kumar N, Choo KKR, Vinel A, Huang X, “Security and privacy for the internet of drones: challenges and solutions,” IEEE Commun Mag, vol.56, no.1, pp.64–69, 2018.

[3] Jong-Hyouk Lee Mohammad Wazid, Ashok Kumar Das, "Authentication protocols for the internet of drones: taxonomy, analysis and future directions," Journal of Ambient Intelligence and Humanized Computing, 2018.

[4] Seung-Hyun Seo,Jongho Won, and Elisa Bertino ,"A Secure Communication Protocol for Drones and Smart Objects," Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security Pages 249-260, 2015.

[5] Jangirala, S., Das, A.K., Kumar, N. and Rodrigues, J., "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," IEEE Transactions on Vehicular Technology, 2019.

[6] Koubaa, A., Qureshi, B., Sriti, M.F., Allouch, A., Javed, Y., Alajlan, M., Cheikhrouhou, O., Khalgui, M. and Tovar, E., "Dronemap planner: A service-oriented cloud-based management system for the internet-ofdrones," Ad Hoc Networks, vol.86, pp.46-62, 2019.

[7] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1953– 1966, 2015.
[8] Minh-Triet Tran,1 and Anh-Duc Duong, "Improved Chebyshev Polynomials-Based Authentication Scheme in Client-Server Environment", Hindawi Security and Communication Networks Volume 2019, Article ID 4250743, 11 pages https://doi.org/10.1155/2019/4250743.
[9] Yaping Li2, Zhijun Zhang, " User Authentication Protocol Based On Chebyshev Polynomial For Wireless Sensor Networks" 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference(IAEAC 2018)
[10] Choi Younsung, Lee Donghoon, Kim Jiye, et al. security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. Sensors, 2014, 14(6): 10081-10106.
[11] H.-Y. Lin, "Improved chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 482–488, 2015.
[12] H. Zhu, "Cryptanalysis and Improvement of aMobile Dynamic ID Authenticated Key Agreement Scheme Based on Chaotic Maps," *Wireless Personal Communications*, vol. 85, no. 4, pp.2141–2156, 2015.
[13] S. A. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, and M. K. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography,"*Wireless Personal Communications*, vol. 96, no. 4, pp. 5355–5373, 2017.
[14] A. Irshad, H. F. Ahmad, B. A. Alzahrani, M. Sher, and S. A. Chaudhry, "An efficient and anonymous chaotic map based authenticated key agreement for multi-server architecture," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 12, pp. 5572–5595, 2016.
[15] H. Nagel, G. Bondt, and B. Custers, "Drone technology: Types, payloads, applications, frequency spectrum issues and future developments," in The Future of Drone Use Opportunities and Threats from Ethical and Legal Perspectives. Springer Gabler Verlag, 2016, vol. 27, ch. 2, pp.21–45.
[16] M. Wazid, A. K. Das, and J.-H. Lee, "Authentication protocols for the internet of drones: taxonomy, analysis and future directions," Journal of Ambient Intelligence and Humanized Computing, 2018, DOI: 10.1007/s12652-018-1006-x.
[17] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," IEEE Access, vol. 4, pp. 1148–1162, 2016.
[18] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments. The Hague: T.M.C. Asser Press, 2016, pp. 21–45.
[19] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," IEEE Transactions on Dependable and Secure Computing, 2018.
[20] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud Centric Authentication for Wearable Healthcare Monitoring System," IEEE Transactions on Dependable and Secure Computing, 2018, DOI: 10.1109/TDSC.2018.2828306.
[21] M. S. Farash, M. Turkanovic, S. Kumari, and M. Hölbl, "An efficient ′user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," Ad Hoc Networks, vol. 36, pp. 152–176, 2016.

[22] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028–3043, 2017.
[23] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks," IEEE Access, vol. 5, pp. 3376–3392, 2017.
[24] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, Aug 2018
[25] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's Law in Passwords," IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2776–2791, Nov 2017.
[26] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," IEEE Transactions on Dependable and Secure Computing, 2018, doi: 10.1109/TDSC.2017.2764083.
[27] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment," IEEE Internet of Things Journal, 2018, doi:10.1109/JIOT.2018.2888821.
[28] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," IEEE Communications Magazine, vol. 56, no. 1, pp. 64–69, 2018.
[29] R. J. Hall, "An Internet of Drones," IEEE Internet Computing, vol. 20, no. 3, pp. 68–73, 2016
[30] R. Doss, W. Zhou, and S. Yu, ``Secure RFID tag ownership transfer based on quadratic residues,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 2, pp. 390401, Feb. 2013.
[31] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, ``Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment,'' IEEE Trans. Depend. Sec. Comput., 2016. [Online]. Aavailable: https://doi.org/10.1109/TDSC.2016.2616876.
[32] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," IEEE Internet of Things Journal, vol. 3, no. 6, pp.899–922, 2016.
[33] S. Challa, M. Wazid, A. K. Das, N. Kumar, G. R. Alavalapati, E. Yoon, and K. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028–3043, 2017.