Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

An Analytical Study of Secure Drone Communication Models from a Statistical Perspective

Jolly R. Nikhade[1], Shrikant V. Sonekar[2]

[1]PGTD of Computers, RTMNU Nagpur, jollynikhade21@gmail.com
[2]Professor, Department of CSE, J D College of Engineering and Management Nagpur

Drone communications are resource-intensive, limiting maintenance and reconfiguration calculations. Security protocols are frequently simpler, which enhances attack chance in high-node-density networks. To address this problem, researchers have created several low-complexity high-security methods that can neutralise many assaults. Blockchains, PuFs, Distributed Ledgers, etc. enable immutable data security and distributed computing with transparency and traceability. This paper discusses such strategies' functional intricacies, application-specific benefits, deployment-specific traits, and context-specific future scopes. This debate will help researchers choose security models for functionality-specific use cases. Bioinspired models like GA, PSO, and others may perform well in real-time network environments when paired with Q-Learning. This paper analyses examined models based on security, scalability, delay of operation, energy consumption, and deployment cost criteria to help readers choose performance-specific models for diverse circumstances. A unique Drone Security Rank Metric (DSRM) that incorporates all these criteria is also evaluated in this work to help readers select solutions with stronger security, reduced complexity, low latency, low energy, and high scalability in real-time use scenarios.

Keywords: Drone, UAV, Communications, Security, Blockchain, Bioinspired, Deep, Learning, Scenarios.

1. Introduction

Many present and prospective drone applications need tight security, including the Internet of Things. Attackers can imitate, control, and intercept drones like other computers. Maintaining authentication, non-repudiation, confidentiality, and integrity between drones and other "smart objects" like on-ground sensors is crucial.

Every security architecture needs cryptographic key management. Drones' mobility and short flight times and smart objects' resource limits make WSN key management difficult. Symmetric keys are used in most WSN encryption key management systems due to sensors' limited energy and computing power [4, 5]. The symmetric-key technique has significant transmission costs and needs a lot of memory to hold shared pairwise keys. Node mobility,

scalability, and resistance suffer. WSNs may use public key cryptography (PKC), which is more costly to calculate than symmetric key encryption, according to recent ECC implementations [6]. Identity-based PKC and ECC may boost WSN flexibility and scalability [7–9]. When applied directly to WSNs, ECC- and ID-PKC-based techniques with certificates [8] incur certificate administration overhead and computational costs from pairing operations. Drones may be caught because they gather more data than sensors. Researchers must handle critical data flow if an opponent seizes a drone fleet.

Recurrent attacks may change sensor locations in uncontrolled regions. Multiple powerful beacon signals from an attacker might lower the RSSI distance between a sensor and a beacon node. Attackers may degrade WSN location-based services. GPS may battle drones and self-driving automobiles. Satellite range signals locate them. GPS without encryption and authentication is non-military. Academics showed OPS assaults and offered solutions. Replay attacks were employed against Starbucks' location-based ordering by Cho et al. Location spoofing attacks against Skyhook [13], a public WLAN-based positioning system, may jam or repeat localization signals and interfere with service databases [12].

Drone sensor data is subject to physical and cyberattacks due to their mobility in unsafe, uncontrolled settings. An enemy may physically take control of a drone and check its storage for keys and data. Attackers might commandeer drones or install malware via software vulnerabilities.

Malware may steal or damage drone data. More deadly, terrorists may attack people, buildings, or aircraft with a crashed drone. Researchers must identify hijacked drones to avoid risk and cost. Verifying with the ground station or other drones that the target drone is running the original software might uncover tampered drones. TPM may verify executing code [14]. Even tiny price increases hinder drone mass production. Some commercial drones, even amateur ones, lack security. Attestation software may replace TPMs. This method checks embedded device code, static data, and configuration settings without hardware. Hardware-based attestation costs more than software. Software-only approaches operate with any drone without adjustments. Due to these benefits, numerous software-based attestation approaches [15–20] have been developed for resource-constrained embedded devices like sensors. Different placement for verifier and item. It blocks the verifier from accessing device storage. Without secure hardware, a compromised device cannot validate itself, hence software-based attestation needs a third party. Most software-based attestation uses prover-ground station challenge-response. Verifiers prevent replay and pre-computational attacks by verifying target systems. A verifier-downloaded or embedded device-hardcoded verification method calculates challenge responses. The verifier may locally compute the challenge solution to validate the target device's response. The verifier can calculate and compare predicted and received answers because it understands the prover's memory and hardware. If the numbers don't match, the gadget may be fake. Software-based attestation methods include response time estimate [17], self-modifying code [18], programme counter [15, 16], and memory filling [19, 20]. Drones cannot employ software-based attestation for these reasons. Very few platforms provide app programme counters. Some microcontrollers, like AVRs, allow application software programme counter access. Second, network latency and hardware platforms affect SWATT-based attestation reaction time estimations. A drone's wide range of platforms and dynamic wireless communication channel with the ground station owing to

network traffic congestion or packet collisions render the timing-based method inappropriate. Slow and complicated self-modifying code cannot be employed in drone attestation protocols [21]. The UAV needs computer memory. Pseudorandom numbers prevent the opponent from storing viruses, photos, or videos in drone memory [19, 20 Code attestation cannot protect drone records or home base communications. Enemies may seek the drone's secret key to decode communications. Symmetric key-based cryptographic primitives AES and HMAC with small secret keys are vulnerable to white-box attacks[22–24]. Malware or memory analysis may impact the target device's internal state for white-box attackers. Entropy, cold boot, and S-box blanking may extract the 128-bit AES key. Longer secret keys may be obtained by white-box attackers[28].

With additional nodes, security is simplified, increasing attack risk. Because of this, researchers have devised simpler high-security approaches that resist multiple attacks. Blockchain, PuF, and distributed ledgers provided immutable data security, transparency, and traceability[25][26].

2. Literature Review

Researchers suggest several drone network deployment security methods. ECC works for drone internet authentication [1]. An attacker may attack the Internet of Drones using ECC-based authentication. Research shows that UAVs are becoming increasingly frequent [2].

Society is affected more. Agriculture and COVID-19 are monitored by drones. Internet of Drones (IoD) connectivity may enhance navigation and send vital data. As IoD culture evolves, these systems must be secured against data privacy and security problems. Drones may hinder IoD systems from employing commodity security solutions like dynamic and open communication channels. In this paper, researchers suggest PMAP, a small, privacy-protecting mutual authentication and key arrangement system. IoD communication entities check each other and secure session keys using PUF and chaos. $mathrm PMAPD2Z$ authenticates drones and ZSP and establishes secure session keys, while $mathrm PMAPD2D$ verifies them. Only trustworthy ZSPs may detect drones under PMAP's conditional privacy protection. Automatic ISP and application validation tests PMAP's security resistance. Researchers test PMAP, AKA, and IBE-Lite. PMAP cuts electricity, computer, and communication expenses.

UAVs, sometimes known as "surveillance drones," film automobiles, people, and surroundings. Drone-ground station server communication may be intercepted, altered, or erased as shown in [3]. Especially combat surveillance. Lets "man-in-the-middle," "impersonation," "drone hijacking," "replay attacks," so. Secure military communication must be anonymous and untraceable. Researchers suggest ACPBS-IoT, a novel drone-based battlefield access control system, to overcome this crucial problem.

Studies [4] demonstrate that IoT-based drone networks (IoD) that link gadgets, applications, and people are growing. Due to constant development, computers, networks, and media transmission systems gain functionalities. IoD streamlines home, work, military, and smart city rescues. Complex infrastructure has security issues. Need new, specialist IoD solutions. Recently developed IoT security approaches are unsafe and reduce productivity. This project authenticates user-drone communications in restricted airspace using elliptic curve

cryptography. The formal Random Oracle method lets researchers swiftly evaluate the proposed system's security. Finally, several critical and present systems are assessed for practicality.

In the Internet-of-Things worldwide context, drones are utilised in military, safety monitoring, agricultural, smart transportation, shipping, and package delivery [5]. Drone surveillance is challenging due to security. Latency and security flaws make most drone-based user authentication vulnerable. Researchers provide smart city drones secure, low-latency blockchain-based authentication to tackle these issues. In drone networks, researchers employ zone-based design and delegated proof of stake.

Drones facilitate device-to-device communication, improving 5G network coverage and services [6]. Direct-to-device drone usage may be unsafe. The 4G cellular design D2D communication security standard may improve, but core servers still receive a lot of traffic. Same-data 5G D2D security may be delayed by this specification. This study presents 5G D2D proxy signature-based drone authentication. Researchers propose delegation-based decentralized authentication to reduce 5G backhaul traffic. Proxy signers will verify core network users for valid drones.

The Internet of Drones (IoD) may be utilised for military and civilian purposes, according to studies [7]. UAVs (or "drones") may be used widely thanks to ICT and the IoT. Secure communication may need limited access to drone flying zones and the ground maintenance station. Chaudhry et al. launched GCACS-IoT 2021. They misrepresent GCACS-said IoD security. GCACS-IoD may leak the dependable control room (CR) secret key, say researchers.

3. Comparative Analysis

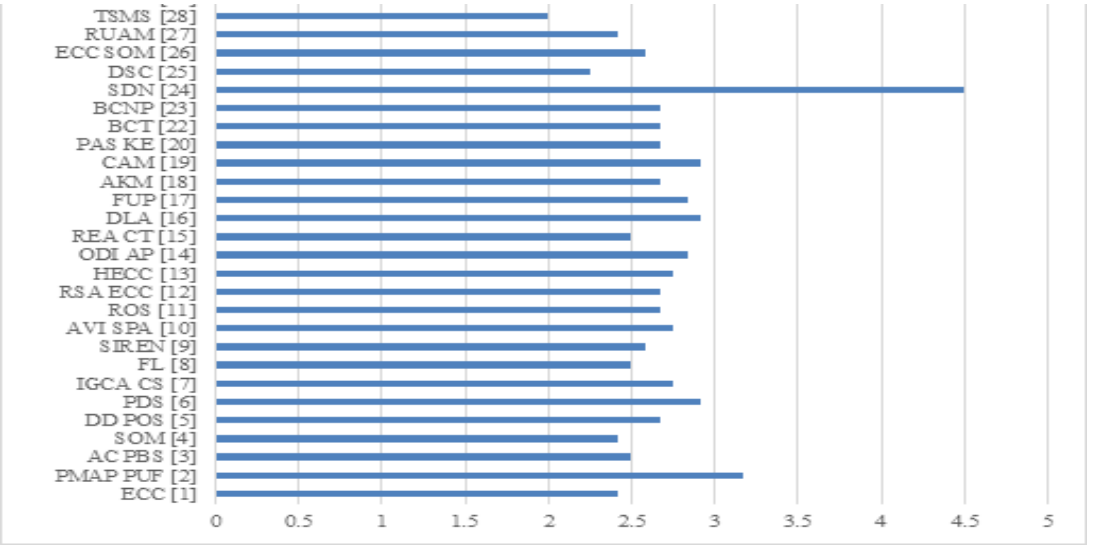
The detailed study of drones communication safety demonstrates that encryption and blockchain are used. To assist readers locate performance-specific models for different scenarios, this section gives a statistical summary of various techniques' security (S), scalability (Sc), delay (D), energy (E), and deployment cost (DC) variables To help readers evaluate these models, these metrics were quantified into Low (L=1), Medium (M=2), High (H=3), and Very High (VH=4) levels. Based on this strategy, Table 1 reveals these features.

Table 1. Comparative analysis of different drone security models

Model	D	DC	E	S	Sc
ECC [1]	H	H	M	H	M
PMAP PUF [2]	H	M	H	VH	VH
AC PBS [3]	H	H	H	H	H
SOM [4]	VH	H	H	H	H
DD POS [5]	H	H	M	H	H
PDS [6]	H	M	H	H	VH
IGCA CS [7]	M	VH	M	H	H
FL [8]	H	H	H	H	H
SIREN [9]	H	VH	M	H	H

AVI SPA [10]	H	H	H	H	VH
ROS [11]	H	H	M	H	H
RSA ECC [12]	H	VH	H	H	VH
HECC [13]	H	H	H	VH	H
ODI AP [14]	H	M	M	H	H
REA CT [15]	H	H	H	H	H
DLA [16]	H	M	H	H	VH
FUP [17]	VH	H	M	VH	H
AKM [18]	H	M	H	H	H
CAM [19]	H	H	M	H	VH
PAS KE [20]	H	M	H	H	H
BCT [22]	H	H	M	H	H
BCNP [23]	VH	H	H	H	VH
SDN [24]	L	M	L	VH	VH
DSC [25]	H	H	H	M	H
ECC SOM [26]	H	M	VH	H	H
RUAM [27]	VH	H	H	H	H
TSMS [28]	H	H	H	L	H

This investigation shows that SDN [24], DPM SITL [30], SDN TDM, and GA PSO have shorter latency, making them suitable for high-speed, secure drone communications. SDN TDM, GA PSO, ANN GA PSO, and CPS models may reduce deployment costs for cost-aware situations. SDN [24], ECC [1], DD POS [5], IGCA CS [7], SIREN [9], ROS [11], and ODI AP [14] have reduced energy usage and may be employed for long-lived networks.



While, work in PMAP PUF [2], HECC [13], FUP [17], SDN [24], MLB [46], and TL [49] are

able to enhance security levels, while PMAP PUF [2], PDS [6], AVI SPA [10], RSA ECC [12], DLA [16], CAM [19], BCNP [23], SDN [24], GA PSO , ANN GA PSO , BCL , and BKDM are capable of deployment for large-scale networks, thus can be used to improve security performance even under larger number of attacks. All these metrics were combined to form an augmented Drone Security Rank Metric (DSRM) that combines all these parameters, which is calculated via equation 1,

DSRM=S/4+Sc/4+1/D+1/DC+1/E… (1)

Based on this evaluation and figure 1, it can be observed that SDN [24], SDN TDM , GA PSO, DPM SITL, ANN GA PSO, PMAP PUF [2], and CPS have higher DSRMs, thus can be used for high-security, high-scalability, low delay, low deployment cost, and high energy efficiency scenarios

4. Conclusion

Blockchain security's benefits, use cases, deployment features, and future applications are covered in this essay. This debate will assist researchers choose application security models. Q-Learning-enhanced bioinspired models like GA, PSO, etc. operate well in real-time networks. Comparing security, scalability, operation delay, energy consumption, and deployment cost might reveal performance-specific models.

Conflicts of Interest

The authors declare that they have no competing interests.

References

1. Zhang, M., Xu, C., Li, S., & Jiang, C. (2022). On the Security of an ECC-Based Authentication Scheme for Internet of Drones. IEEE Systems Journal, 16(4), 6425-6428. https://doi.org/10.1109/JSYST.2022.3162604
2. Pu, C., Wall, A., Choo, K.-K. R., Ahmed, I., & Lim, S. (2022). A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment. IEEE Internet of Things Journal, 9(12), 9918-9933. https://doi.org/10.1109/JIOT.2022.3163367
3. Bera, B., Das, A. K., Garg, S., Piran, M. J., &Hossain, M. S. (2022). Access Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment. IEEE Internet of Things Journal, 9(4), 2708-2721. https://doi.org/10.1109/JIOT.2020.3049003
4. Hussain, S., Chaudhry, S. A., Alomari, O. A., Alsharif, M. H., Khan, M. K., & Kumar, N. (2021). Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones. IEEE Systems Journal, 15(3), 4431-4438. https://doi.org/10.1109/JSYST.2021.3057047
5. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Karimipour, H., Srivastava, G., &Aledhari, M. (2021). Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. IEEE Internet of Things Journal, 8(8), 6406-6415. https://doi.org/10.1109/JIOT.2020.3015382
6. Abdel-Malek, M. A., Akkaya, K., Bhuyan, A., & Ibrahim, A. S. (2022). A Proxy Signature-Based Swarm Drone Authentication With Leader Selection in 5G Networks. IEEE Access,

10, 57485-57498. https://doi.org/10.1109/ACCESS.2022.3178121
7. Das, A. K., Bera, B., Wazid, M., Jamal, S. S., & Park, Y. (2021). iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment. IEEE Access, 9, 87024-87048.
8. Yao, J., & Ansari, N. (2021). Secure Federated Learning by Power Control for Internet of Drones. IEEE Transactions on Cognitive Communications and Networking, 7(4), 1021-1031. https://doi.org/10.1109/TCCN.2021.3076167
9. Hassan, M. Z., Kaddoum, G., &Akhrif, O. (2022). Resource Allocation for Joint Interference Management and Security Enhancement in Cellular-Connected Internet-of-Drones Networks. IEEE Transactions on Vehicular Technology, 71(12), 12869-12884. https://doi.org/10.1109/TVT.2022.3196500
10. Yu, S., Das, A. K., Park, Y., & Lorenz, P. (2022). SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments. IEEE Transactions on Vehicular Technology, 71(10), 10374-10388. https://doi.org/10.1109/TVT.2022.3188769
11. Zhang, J., Cui, J., Zhong, H., Bolodurina, I., & Liu, L. (2021). Intelligent Drone-assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-Hoc Networks. IEEE Transactions on Network Science and Engineering, 8(4), 2982-2994. https://doi.org/10.1109/TNSE.2020.3029784
12. Abulkasim, H., Goncalves, B., Mashatan, A., &Ghose, S. (2022). Authenticated Secure Quantum-Based Communication Scheme in Internet-of-Drones Deployment. IEEE Access, 10, 94963-94972. https://doi.org/10.1109/ACCESS.2022.3204793
13. Khan, M. A., et al. (2021). Securing Internet of Drones With Identity-Based Proxy Signcryption. IEEE Access, 9, 89133-89142.
14. Lei, Y., Zeng, L., Li, Y.-X., Wang, M.-X., & Qin, H. (2021). A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization. IEEE Access, 9, 53769-53785. https://doi.org/10.1109/ACCESS.2021.3070683
15. Akram, M. W., et al. (2022). A Secure and Lightweight Drones-Access Protocol for Smart City Surveillance. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19634-19643. https://doi.org/10.1109/TITS.2021.3129913
16. Jeong, J. Y., Byun, J. W., &Jeong, I. R. (2022). Key Agreement Between User and Drone With Forward Unlinkability in Internet of Drones. IEEE Access, 10, 17134-17144. https://doi.org/10.1109/ACCESS.2022.3150035
17. Ingole, K., &Padole, D. (2023). Design Approaches for Internet of Things Based System Model for Agricultural Applications. In 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) (pp. 1-5). Nagpur, India. doi:10.1109/ICETET-SIP58143.2023.10151606.
18. Cabuk, U. C., Dalkilic, G., &Dagdeviren, O. (2021). CoMAD: Context-Aware Mutual Authentication Protocol for Drone Networks. IEEE Access, 9, 78400-78414. https://doi.org/10.1109/ACCESS.2021.3083549
19. Tanveer, M., Khan, A. U., Shah, H., Chaudhry, S. A., &Naushad, A. (2021). PASKE-IoD: Privacy-Protecting Authenticated Key Establishment for Internet of Drones. IEEE Access, 9, 145683-145698. https://doi.org/10.1109/ACCESS.2021.3123142
20. DjupkepDizeu, F. B., Picard, M., Drouin, M. -A., &GAGNé, G. (2022). Extracting Unambiguous Drone Signature Using High-Speed Camera. IEEE Access, 10, 45317-45336. https://doi.org/10.1109/ACCESS.2022.3170481
21. Alsamhi, S. H., et al. (2023). Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. IEEE Transactions on Green Communications and Networking, 7(1), 328-338. https://doi.org/10.1109/TGCN.2022.3195479

22. Cheema, M. A., et al. (2021). A Drone-Aided Blockchain-Based Smart Vehicular Network. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4160-4170. https://doi.org/10.1109/TITS.2020.3019246
23. Alsolami, F., Alqurashi, F. A., Hasan, M. K., Saeed, R. A., Abdel-Khalek, S., & Ben Ishak, A. (2021). Development of Self-Synchronized Drones' Network Using Cluster-Based Swarm Intelligence Approach. IEEE Access, 9, 48010-48022. https://doi.org/10.1109/ACCESS.2021.3064905
24. Shen, H., et al. (2021). Drone-Small-Cell-Assisted Resource Slicing for 5G Uplink Radio Access Networks. IEEE Transactions on Vehicular Technology, 70(7), 7071-7086. https://doi.org/10.1109/TVT.2021.3083255
25. Jan, S. U., Abbasi, I. A., Algarni, F., & Khan, A. S. (2022). A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET. IEEE Access, 10, 95321-95343. https://doi.org/10.1109/ACCESS.2022.3204271
26. Johri, P., Khatri, S. K., Al-Taani, A. T., Sabharwal, M., Suvanov, S., & Kumar, A. (2021). Natural Language Processing: History, Evolution, Application, and Future Work. In A. Abraham, O. Castillo, & D. Virmani (Eds.), Proceedings of the 3rd International Conference on Computing Informatics and Networks (Vol. 167, Lecture Notes in Networks and Systems, pp. Cite the page range here if available). Springer, Singapore. https://doi.org/10.1007/978-981-15-9712-1_31
27. Rajareega, S. , Vimala, J. &Preethi, D. (2023) Complex intuitionistic fuzzy soft lattice ordered group associated with ℓ-ideal, Journal of Discrete Mathematical Sciences and Cryptography, 26:4, 991–1003, DOI: 10.1080/09720529.2021.1962024
28. Aljader, Huda Kadhim M. &Ajeena, Ruma Kareem K.(2023) The optimized Diffie-Hellman key exchange using the graphical method, Journal of Discrete Mathematical Sciences and Cryptography, 26:6, 1691–1697, DOI: 10.47974/JDMSC-1615