Crowd Monitoring System Based on Unmanned Aerial Vehicles: Secure Key Agreement Scheme

Sandhya. S, Jeshik S, Prajwal Gajanan Hegde

Abstract: Unmanned Aerial Vehicles (UAVs) can be applied to survey or for monitoring a huge crowd where conventional monitoring systems fail. Even though UAVs are proven to be an effective way for monitoring and surveying, they present a threat of data being leaked when it is being transferred to the user's device. To mitigate these dangers, a secure channel must be established between the user and the UAVs. There are multiple key agreement methods already in place, but they are either of a heavy authentication type or less secure against attacks from unscrupulous parties. In this paper, we propose an approach to mitigate such threats using a public-key cryptographic method with session-based authentication. The process mentioned above is simulated using NS2 software, and its efficiency will be recorded at the end.

Keywords: UAV, Attacks, Cryptography, Security, Authentication, Session Keys, Simulation.

I. INTRODUCTION

Unmanned aerial vehicles, or drones as they are more commonly recognised, have become widely used in many different industries due to their adaptability, portability, and ability to operate in a variety of conditions. Unmanned Aerial Vehicles (UAVs) holds excellent potential for crowd monitoring, as they can offer large-scale, real-time surveillance and data collection.

Nevertheless, several security issues arise when using UAVs for crowd monitoring, particularly regarding the secure transmission of data between control centres and UAVs. Sensitive data collected by UAVs in a crowd surveillance system must be transmitted securely to prevent interception or manipulation by unscrupulous parties. It is vital to safeguard the confidentiality, integrity, and validity of this information, as breaches may result in dangers to public safety, privacy violations, and the dissemination of false information. Because UAVs are subject to special limitations, including limited computational resources, energy constraints, and the dynamic nature of UAV networks, conventional security precautions may not be immediately applicable.

To solve these issues, a secure key agreement mechanism is essential. By creating cryptographic keys between UAVs and control stations, or between UAVs, such a technique enables data encryption to be transferred over a network and prevents unauthorised access. To ensure that the resource constraints of unmanned aerial vehicles (UAVs) are met, the key agreement process must be both practical and resilient against various types of attacks. Several factors should be considered when creating a secure key agreement system for UAV-based crowd surveillance. Initially, to lessen the computational and energy overhead on UAVs, the strategy needs to be lightweight. Secondly, it should possess the ability to manage the mobility and frequent changes in network topology that are typical of UAV systems, and it needs to facilitate the dynamic creation and distribution of keys. Finally, it should be able to smoothly integrate with current UAV communication protocols without introducing excessive complexity or latency. Conclusively, the creation of a secure key agreement framework is vital for the successful implementation of unmanned aerial vehicle (UAV)-based crowd monitoring systems. This is because it guarantees the safety of data acquired and transmitted by UAVs, safeguarding individual privacy and the integrity of the monitoring operation. In this proposed paper, we utilise one of the public key cryptographic methods used for secure key sharing. The Diffie-Hellman secure key sharing mechanism is used. In this method, a pair of public keys is generated using each party's secure private key. These public keys are shared between them, and finally, a final key is generated. If both parties generate the same key, the authentication is then valid; otherwise, a potential attack may occur.

II. RELATED WORK

[1] Addresses the security challenges in the Internet of Drones (IoD) environment, which is subject to several vulnerabilities such as unauthorized access and data interception. Here, they have utilised authenticated encryption, hashing, and physical unclonable functions to secure IoD in the event of attacks. Additionally, computation, communication, and energy overheads are optimised. Even though the performance measured is addressed in [1] there is a chance that attacks take place in between communication, so to make UAVs secure from network attacks [2]made use of session key agreement to ensure data privacy, authentication and protection against cyber-attacks. Here, a secure key is distributed to all the UAVs and the ground control station, which is subsequently employed to create authentication while transmitting data.

Manuscript received on 10 September 2024 | Revised Manuscript received on 12 September 2024 | Manuscript Accepted on 15 October 2024 | Manuscript published on 30 October 2024.

*Correspondence Author(s)

Dr. Sandhya. S, Assistant Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore (Karnataka), India. E-mail: Sandhya.sampangi@rvce.edu.in

Jeshik S, Department of Computer Science and Engineering, R V College of Engineering, Bangalore (Karnataka), India. E-mail: Jeshiks.scn23@rvce.edu.in

Prajwal Gajanan Hegde*, Department of Computer Science and Engineering, R V College of Engineering, Bangalore (Karnataka), India. E-mail: Prajwalgh.scn23@rvce.edu.in

Retrieval Number: 100.1/ijitee.K998113111024
DOI: 10.35940/ijitee.K9998.13111024
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Another way to secure the communication between the consumer and the drone is to make use of physical layer security (PLS) [3] which leverages randomness of the wireless channel to establish secure keys among UAVs without the need for pre-shared key or heavy computational overhead. In this literature, they utilised channel estimation, feature extraction, quantisation, and information reconciliation and privacy amplification. Another use case for UAVs is in disaster recovery, where existing infrastructure is compromised, and the need for multi-factor authentication arises, combining biometric passwords and the use of smart cards. These, combined with Physical Unclonable Functions (PUFs), provide a hardware-based security mechanism that is resistant to cloning and tampering [4]. Even though secure through secure is achieved, there is always a possibility that the safe key may be leaked. To address this issue, a privacy-preserving authenticated key agreement system that doesn't need secret key storage on devices is introduced in [5]. It utilises the double PUF approach to ensure both computational efficiency and security. When considering the connectivity of the UAVs, there's a possibility that it may not be connectable to a wireless network at all times. So to provide connectivity to UAVs [6] 5G/6G networks authentication framework is being put to use. In literature [6] Elliptical Curve Cryptography (ECC) is utilized to provide three-phase process for authentication which includes initial access, authentication and key agreement phase. In the case of a swarm of UAV systems, using a consensus mechanism to validate transactions within the UAV network is efficient. Paper [7] made use of blockchain based secure authentication algorithm to ensure integrity with the UAV systems. Although there are several secure key exchange schemes, a man-in-the-middle attack can still compromise the existing system, making UAV-generated data vulnerable. To avoid this issue, literature [8] introduced random numbers and timestamps to ensure absolute time safety of the communication. Key generation and distribution are always a security issue when it comes to public key cryptography, so to avoid this issue, a [10] intermediatory layer is introduced to in between user and the drone. This layer securely stores keys and is used for authentication between drones and users. To adapt to a dynamically changing topology, a secure infrastructure is required. In the paper [11] this is implemented using mutual authentication and ECC [12]. Another way to reduce computation overhead is to group a set of closely placed UAVs. For this group, a single session key is shared, and each drone is validated. To address impersonation and DoS types of attacks on the UAV network, the paper [13] made use of fuzzy extractor is used. A fuzzy extractor is utilised to generate secret parameters using user biometrics, and the security of the data is analysed through BAN logic and the RoR model. Another way to create secure keys is to utilise chaotic systems to produce unpredictable and safe keys. A secure, lightweight authentication technique designed for the Internet of Drones, which is suggested in [9] which employes authenticated key agreement and ProVerif software for analysing network security.

III. METHODOLOGY

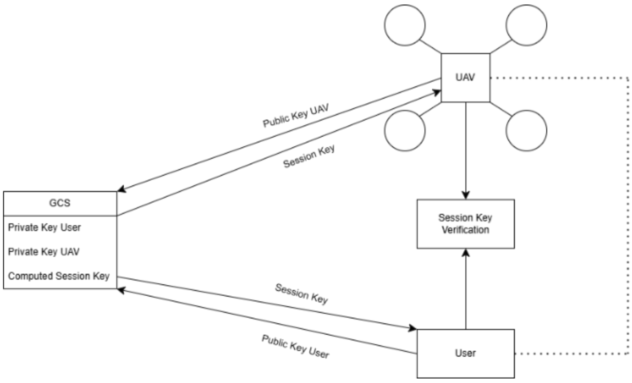

Fig. 1: Block Diagram of UAV System

To initiate secure communication between the user and the UAV, we are utilising public key cryptography. Diffie-Hellman is a renowned public-key cryptography algorithm used in key exchange.

We leverage the Diffie-Hellman feature to generate a public key at both the UAV and the User. When each public key is shared with the Ground Control System, which holds the private keys of both the UAV and the User. GCS generates a shared key. If the shared key from both the User and the UAV is the same, a unique session key is generated. The drone and the User communicate their session keys to the session key verifier. If both session keys are found to be the same, then a direct connection between the UAV and the User is established. After a specified duration, a new session key is generated using the previous session key. By doing this, we can prevent a man-in-the-middle attack from continuously listening to the conversation between the UAV and the User.

Table 1. Time Complexity Comparison

Metric	µTesla-Based Authentication	iGCACS-IoD	TAGKA (UANET)	Blockchain-Based Spectrum Sharing	Our System
Time Complexity	O (1) or O(n)	O (n log n)	O(n^2) or O (n log n)	O (log n) or O(n)	O (log n)

The approach's mathematical model is implemented by taking large prime numbers agreed upon by both parties. A primitive root modulo p is a number whose powers generate all the integers from 1 to p-1. Random numbers are chosen by each party and kept secret. There is also a public key, which is computed from the private key using the formula ga mod p (where 'a is the private key). Shared key is generated at Ground Control Station (GCS) using the user's and drone's private keys, resulting in the same value if there is no corrupt value.

Steps for authentication are mentioned below:
1. Agreement on Public Parameters (**p** and **g**):
Both drone and user agree on **p,** a large prime number and a generator **g** (publicly known)

A. Private Key Generation

The drone generates a private key a (a random integer). User generates public key **b** (a random integer).

B. Public Key Computation

Drone computes **A = g^a mod p** and forwards it to GCS. The user computes **B = g^b mod p** and forwards it to GCS. GCS computes the shared secret key using the formula S1 = Ba mod p and S2 = Ab mod p. If both S1 and S2 are the same, then secure communication is achieved.

4. This key is used in the generation of a session key between the drone and the user directly, without the involvement of GCS.

The time complexity of various systems for secure communication and spectrum sharing varies significantly. The µTesla-based authentication system offers a time complexity of O(1) or O(n), indicating highly efficient performance. The iGCACS-IoD system has a time complexity of O(n log n), striking a balance between complexity and efficiency. TAGKA for UANET exhibits a more variable complexity, ranging from $O(n^2)$ to O(n log n), reflecting its potentially higher computational demands. The Blockchain-Based Spectrum Sharing system operates with a time complexity of O(log n) or O(n). In contrast, our system achieves a time complexity of O(log n), indicating optimised performance.

IV. DEPLOYMENT PHASES

NS2 (Network Simulator 2) is a discrete event-driven simulation tool primarily used for simulating networking protocols and scenarios. It supports a wide range of protocols in various network types, including wired, wireless, and satellite networks. NS2 is used to create a 4-node network.

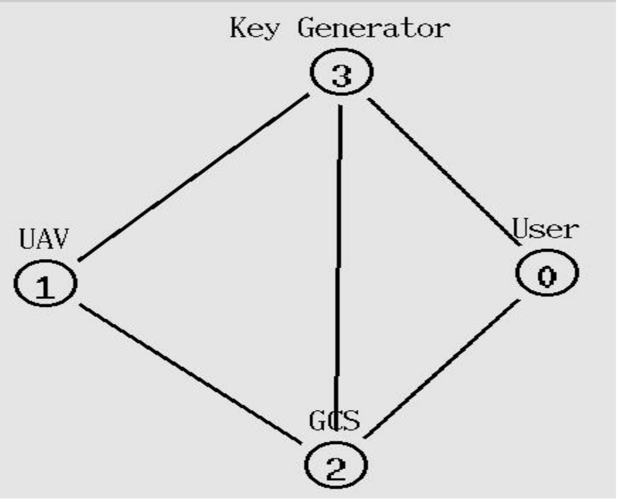

Fig. 2: Network Graph-1

Node 0 represents GCS, node 1 represents UAV, node 2 represents User, and node 3 represents Session Key Generator. First, these nodes are set up to form a connection. Node 1 and Node 2 compute their public key with the help of modular arithmetic using prime numbers.

Computed public keys are shared with GCS, which holds the private key of both node one and node 2. GCS computes a session key for both the UAV and the User separately. After computing the session key, it is compared; if the session key is not equal, then the connection request between the UAV and the User is denied by

GCS: Else if the session keys of both the UAV and the User are equal, the session key is shared with the Session Key Generator, UAV, and User. Only after that, communication between the user and the UAV occurs through a session key generator. After the first session key generation, GCS doesn't participate further between the UAV and the User.

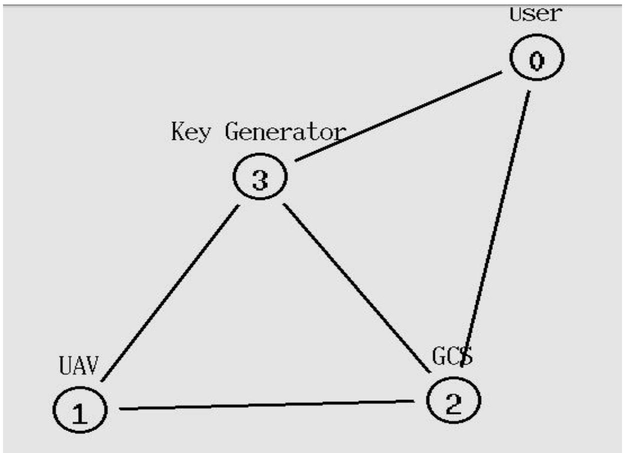

Fig. 3: Network Graph-2

The session key generator is used to generate a new session key whenever the quantum expires. The session key generator produces a new set of keys. These keys are exchanged between the User and the UAV, which facilitates secure communication between the drone and the user. By creating a session key after a specific time quantum, we can avoid getting caught in a man-in-the-middle attack. A Man-in-the-Middle (MitM) attack occurs when a perpetrator secretly intercepts and potentially alters communication between two parties, causing them to believe they are communicating directly with each other. This allows the attacker to steal critical data, manipulate messages, or inject malicious content without either party being aware of it.

V. RESULTS

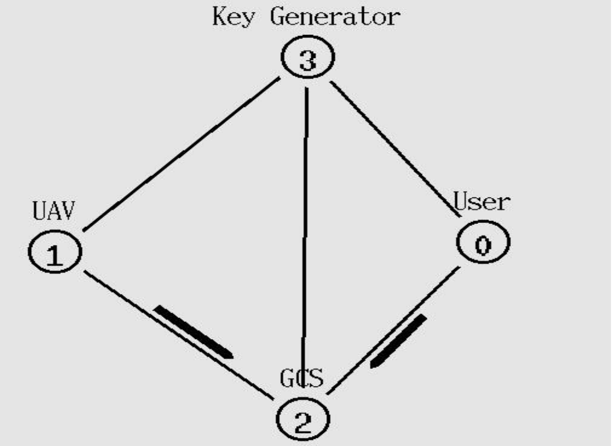

Fig. 4: Public Key Movement

In the above figure, the User and UAV send their public keys to the GCS. This movement is indicated by a dark-coloured arrow mark (Fig. 4),

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

and the GCS contains the private key of both the user and the UAV.

After a matched session is generated from GCS, direct communication between the UAV and the user occurs. This is illustrated in Fig., where a black arrow mark indicates the movement of data between the User and UAV. By doing this, secure and lightweight communication is achieved between the UAV and the user, utilising Diffie-Hellman and secure session key exchange.

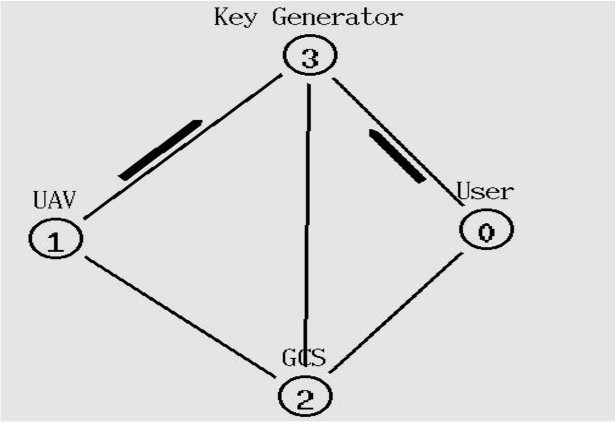

Fig. 5: Session Key Movement

VI. CONCLUSION

The secure key agreement scheme proposed for UAV-based crowd monitoring effectively balances lightweight computation with robust security by utilising Diffie-Hellman cryptography. The system's dynamic session key renewal significantly mitigates the risk of man-in-the-middle attacks, ensuring secure communication between the UAVs and ground control stations. However, the central reliance on ground control station (GCS) poses potential risks, such as single points of failure, particularly in high-traffic scenarios.

Although NS2 simulations demonstrate the scheme’s efficiency, real-world testing is crucial to verify the system’s performance under various scenarios. To enhance system resilience, future work could explore decentralized key management approaches and integrate advanced cryptographic techniques. Overall, this scheme represents a significant advancement in securing UAV-based crowd monitoring, with opportunities for further refinement.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Badshah et al., "USAF-IoD: Ultralightweight and Secure Authenticated Key Agreement Framework for Internet of Drones Environment," in IEEE Transactions on Vehicular Technology, https://doi.org/10.1109/TVT.2024.3375758
2. V. O. Nyangaresi et al., "Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges," 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2021, pp. 1-6, https://doi.org/10.1109/ICECET52533.2021.9698744
3. S. Jangsher, A. Al-Dweik, Y. Iraqi, A. Pandey and J.-P. Giacalone, "Group Secret Key Generation Using Physical Layer Security for UAV Swarm Communications," in IEEE Transactions on Aerospace and Electronic Systems, vol. 59, no. 6, pp. 8550-8564, Dec. 2023, https://doi.org/10.1109/TAES.2023.3307092
4. D. Wang, Y. Cao, K. -Y. Lam, Y. Hu and O. Kaiwartya, "Authentication and Key Agreement Based on Three Factors and PUF for UAV-Assisted Post-Disaster Emergency Communication," in IEEE Internet of Things Journal, vol. 11, no. 11, pp. 20457-20472, 1 June 1 2024, https://doi.org/10.1109/JIOT.2024.3371101
5. P. Gope and B. Sikdar, "An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones," in IEEE Transactions on Vehicular Technology, vol.. 69, no. 11, pp. 13621-13630, Nov. 2020, https://doi.org/10.1109/TVT.2020.3018778
6. R. Ma, J. Cao, S. He, Y. Zhang, B. Niu and H. Li, "A UAV-Assisted UE Access Authentication Scheme for 5G/6G Network," in IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 2426-2444, April 2024, https://doi.org/10.1109/TNSM.2023.3341829
7. E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan and N. Kaabouch, "A Secure Blockchain-based Communication Approach for UAV Networks," 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 2020, pp. 411-415, https://doi.org/10.1109/EIT48999.2020.9208314
8. Chandran and K. Vipin, "A Robust PUF-Based Mutual Authentication and Key Agreement Protocol Using FPGA to Secure UAV Networks," 2023 IEEE Engineering Informatics, Melbourne, Australia, 2023, pp. 1-7, https://doi.org/10.1109/IEEECONF58110.2023.10520358
9. M. Yahuza, M. Y. I. Idris, A. W. A. Wahab, T. Nandy, I. B. Ahmedy and R. Ramli, "An Edge Assisted Secure Lightweight Authentication Technique for Safe Communication on the Internet of Drones Network," in IEEE Access, vol. 9, pp. 31420-31440, 2021, https://doi.org/10.1109/ACCESS.2021.3060420
10. S. U. Jan, I. A. Abbasi and F. Algarni, "A Key Agreement Scheme for IoD Deployment Civilian Drone," in IEEE Access, vol. 9, pp. 149311-149321, 2021, https://doi.org/10.1109/IEEECONF58110.2023.10520358
11. J. Liu, L. Yuan, Z.-S. Feng, X. Chen and Z.-C. Hang, "A Lightweight Key Agreement Scheme for UAV Network," 2022 IEEE 8th International Conference on Computer and Communications (ICCC), Chengdu, China, 2022, pp. 731-735, https://doi.org/10.1109/ACCESS.2021.3124510
12. Ayad and Y. Hammal, "An Efficient Authenticated Group Key Agreement Protocol for Dynamic UAV Fleets in Untrusted Environments," 2021 International Conference on Networking and Advanced

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Systems (ICNAS), Annaba, Algeria, 2021, pp. 1-8, https://doi.org/10.1109/ICNAS53565.2021.9628966

13. H. Dogan, "Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme," 2023 7th International Conference on Cryptography, Security and Privacy (CSP), Tianjin, China, 2023, pp. 13-21, https://doi.org/10.1109/CSP58884.2023.00010

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.