International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-13 Issue-11, October 2024

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

Sandhya. S, Jeshik S, Prajwal Gajanan Hegde

Abstract: ***Unmanned Arial Vehicles (UAVs) can be applied to survey or for monitoring huge crowd where conventional monitoring systems fail. Even though UAVs is proven to be effective way for monitoring and surveying there present a threat of data getting leaked when it is being transferred to the user's device. To lessen these dangers a secure channel amid the user and the UAVs needs to be determined. There are multiple key agreement methods which is already present but they are either heavy authentication type or less secure to the attacks from the unscrupulous parties. In this paper, we provide an approach to mitigate such threats using a public key cryptographic method with a session-based authentication. The above-mentioned method is simulated using NS2 software and it's 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 well recognized, have become widely used in many different industries because of their adaptability, portability, and capacity to function in a variety of conditions. Unmanned aerial vehicles

(UAVs) hold great potential for crowd monitoring, as they can offer large-scale, real-time surveillance and data collecting.

Nevertheless, there are several security issues with using UAVs for crowd monitoring, especially when it comes to safe data sent between control centers and UAVs. Sensitive data collected by UAVs in a crowd surveillance system requires safe transmission to avoid interception or manipulation by unscrupulous parties. It is vital to safeguard the confidentiality, integrity, and validity of this information since breaches may result in dangers to public safety, privacy violations, and false information. Because UAVs are subject to special limitations, including limited computational resources, energy constraints, and the fluid character of UAV networks, conventional security precautions might not be immediately relevant.

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

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

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 makes data encryption possible being transferred over a network and prevent unauthorized access. To ensure that the resource constraints of the unmanned aerial vehicles (UAVs) are met, the key agreement process needs to be both effective and resilient against several 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, should possess the ability to manage the mobility and frequent changes in network topology that are typical of UAV systems, it needs to facilitate dynamic key creation and distribution. Finally, it should possess the ability to smoothly integrate with the current UAV communication protocols without adding an abundance of complexity or latency. Conclusively, the creation of 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 make use of one of the public key cryptographic method which is used for secure key sharing. Diffie Hellman secure key sharing mechanism is used. In this method, a pair of public keys are generated using individual parties secure private key. These public key is shared between them and finally and a final key is generated. If both parties generate same key the authentication is then valid else there might be a chance of potential attack.

II. RELATED WORK

[1] Addresses the security challenges in the Internet of Drones (IoD) environment, which is subject to a number of vulnerabilities such as unauthorized access and data interception. Here, they have utilized authenticated encryption, hashing and physical unclonable functions to secure IoD in case of attacks. Also computation, communication and energy overheads are optimized. Even though performance measured is addressed in [1] there is a chance that attacks takes place in between communication so in order to make UAVs secure from network attacks [2][20] 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 ground control station which is subsequently employed to create authentication while transmitting data.

Another way to secure the communication between consumer and 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 made use of channel estimation, feature extraction, quantization and information reconciliation and privacy amplification. Another use case of UAVs are in disaster recovery where existing infrastructure is compromised then need for multi-factor authentication combining biometric password and use of smart cards comes into picture. 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 of secure key getting leaked so as to address this issue a privacy-preserving authenticated key agreement a system that doesn't need secret key storage on devices is introduced in [5]. It make use of double PUF approach to ensure computational efficiency and security. When considering the connectivity of the UAVs there's a possibility that it isn't connectable to wireless network all the time. So in order 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 case of swarm of UAV systems use of 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 scheme there can be man in the middle attack which can compromise the existing system and make UAV generated data vulnerable. For the purpose of avoiding this issue literature [8][9][14][16][21][22][23][24][25] introduced random numbers and timestamps to ensure real time safety of the communication. Key generation and distribution is always a security issue when it comes to public key cryptography, so for the purpose of avoiding 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. For the purpose of adapting to dynamically changing topology a secure infrastructure is required. In paper [11] this is implemented using mutual authentication and ECC [12]. Another way to reduce computation overhead is to make group of closely placed UAVs. For this group a same session key is shared and each drones is validated. To address impersonation and DoS types of attacks on UAV network paper [13][17][18][19] made use of fuzzy extractor is used. Fuzzy extractor is utilized to use user biometric to generate secrete parameters and security of data is analyzed through BAN logic and RoR model. Another way of generating secure is to make use of chaotic systems to generate unpredictable and secure keys. A secure lightweight authentication technique designed for internet of drones which is suggested in [15] which employes authenticated key agreement and ProVerif software for analysing network security.

III. METHODOLOGY

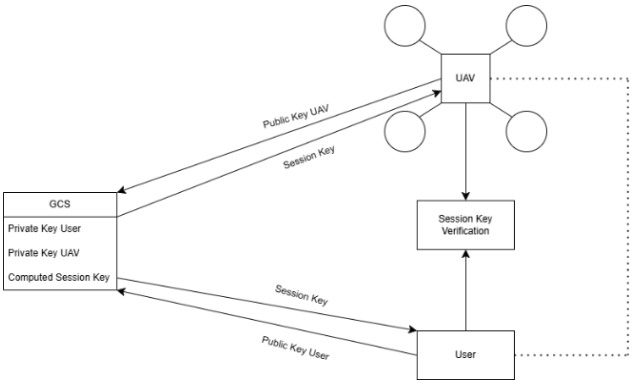

Fig. 1: Block Diagram of UAV System

To initiate secure communication between user and UAV we are making use of public key cryptography. Diffie-Hellman is a famous public key cryptography used in exchanging of keys.

We leverage this feature of Diffie-Hellan to generate public key at both UAV and User. When then each individual public key is shared to Ground Control System which holds the private keys of both UAV and User. GCS generates shared key. If shared key from both User and UAV is same a unique session key is generated. Drone and User communicate their session keys to session key verifier. If both session keys found to be same then direct connection between UAV and User is established. After particular duration of time a new session key is produced using the previous session key. By doing this we can prevent man in the middle attack from continuously listening to 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 primitives root modulo p, is a number whose powers generate all the integers from 1 to p-1. A random numbers chosen by each party and kept secret. There is also a public key which is computed from private keys using the formula g^a mod p (where 'a' is the private key). Shared key is generated at Ground Control Station (GCS) using user's and drone's private keys, resulting in same value if there is no corrupt value.

Steps for authentication is mentioned as 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)

© Copyright: All rights reserved.

A. Private Key Generation

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

B. Public Key Computation

Drone computes $\mathbf{A = g^a \bmod p}$ and forwards it to GCS, user computes $\mathbf{B = g^b \bmod p}$ and forwards it to GCS. GCS computes shared secret key using for formula $\mathbf{S1 = B^a \bmod p}$ and $\mathbf{S2 = A^b \bmod p}$. If both **S1** and **S2** are same then secured communication is achieved.

4. This key is used in generation of session key between drone and 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 a highly efficient performance. The iGCACS-IoD system has a time complexity of O(nlog n), balancing between complexity and efficiency. TAGKA for UANET exhibits a more variable complexity, ranging from $O(n^2)$ to O(nlog 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), while Our System achieves a time complexity of O(log n), indicating optimized 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 make a 4 node network.

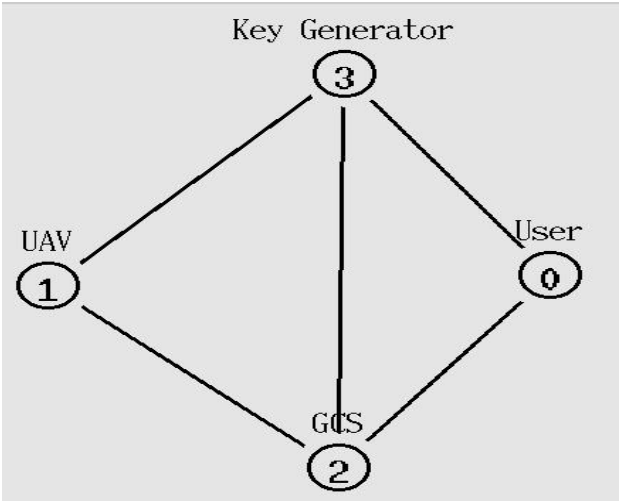

Fig. 2: Network Graph-1

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

Computed public keys are shared to GCS which holds private key of both node 1 and node 2. GCS computes session key for both UAV and User separately. After computing the session key is compared, if the session key is not equal then the connection request between UAV and User is denied by GCS else if the session keys of both UAV and User are equal, session key is shared to Session key generator, UAV and User. Only after that communication between the user and UAV happens through session key generator. After first session key generation GCS doesn't participate further between UAV and User.

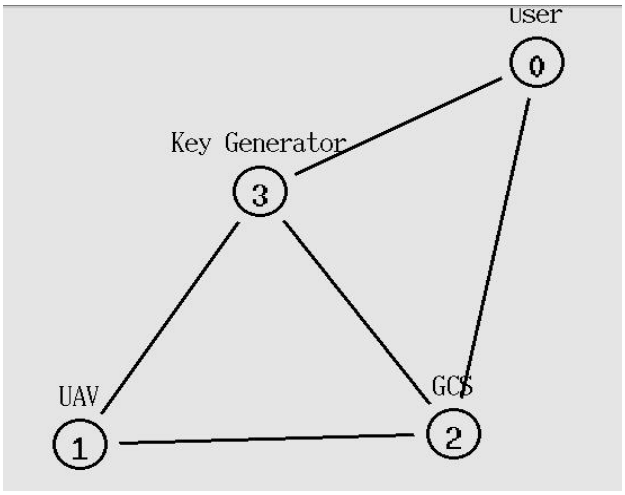

Fig. 3: Network Graph-2

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

V. RESULTS

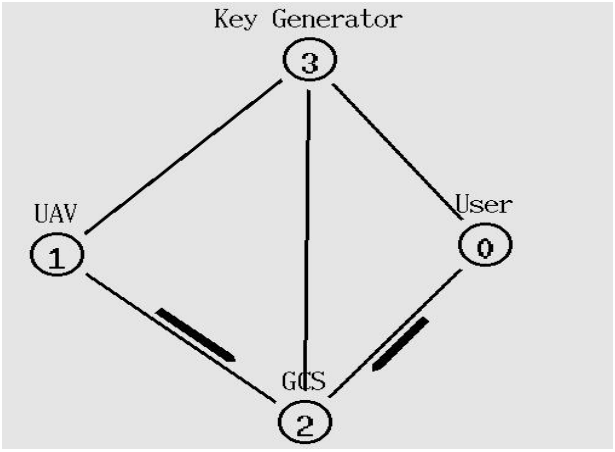

Fig. 4: Public Key Movement

In the above figure User and UAV send their public keys to GCS. This movement is indicated with dark color arrow mark (Fig.4) and GCS contains private key of both user and UAV.

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

After matched session is generated from GCS direct communication between us UAV and User happens. This is indicated in Fig.5 where movement of data between User and UAV is indicated in black arrow mark. By doing this secure and light weight communication between UAV and User is achieved using Diffie-Hellman and secure session key exchange.

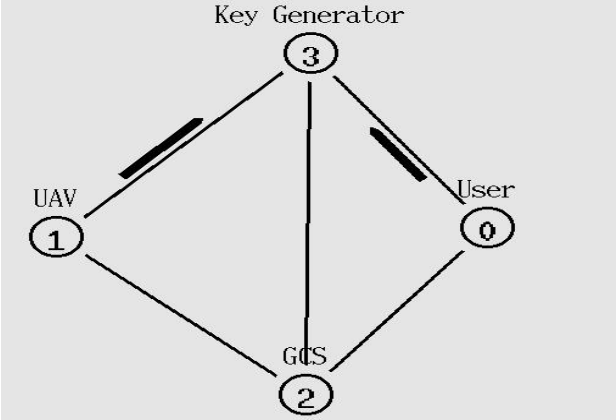

Fig. 5: Session Key Movement

VI. CONCLUSION

The secure key agreement scheme proposed for UAV-based crowd monitoring effectively balances lightweight computation with robust security through 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 has no 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 has been conducted without any external sway.
- **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.
- **Authors 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 June1, 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. Kumar, N., & Tomar, Dr. D. S. (2019). A Lightweight Authentication Method in Perception Layer of IoT Through Digital Watermarking. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 3, pp. 2937–2942). https://doi.org/10.35940/ijrte.c4793.098319
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 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
14. Tappari, S., & Sridevi, K. (2019). Resource Optimized Security Coding in Light Weight Security Protocol. In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 10, pp. 2645–2651). https://doi.org/10.35940/ijitee.j9393.0881019
15. 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

© Copyright: All rights reserved.

16. Shaharkar, B. B., & Pandit, D. P. (2022). ML Based Authentication Scheme for Data Storage in Cloud Based IoT. In International Journal of Engineering and Advanced Technology (Vol. 11, Issue 6, pp. 123–127). https://doi.org/10.35940/ijeat.f3767.0811622
17. Velani, J., & Patel, Dr. S. (2023). A Review: Fraud Prospects in Cryptocurrency Investment. In International Journal of Innovative Science and Modern Engineering (Vol. 11, Issue 6, pp. 1–4). https://doi.org/10.35940/ijisme.e4167.0611623
18. Zubir, Dr. A. S. H. M., Awi, Dr. N. A., Ali, Dr. A., Mokhlis, Dr. S., & Sulong, Dr. F. (2020). Cryptocurrency Technology and Financial Reporting. In International Journal of Management and Humanities (Vol. 4, Issue 9, pp. 103–108). https://doi.org/10.35940/ijmh.i0898.054920
19. Kaur, Dr. H., & Kaur, Prof. A. (2021). Cryptography in Cloud Computing. In Indian Journal of Cryptography and Network Security (Vol. 1, Issue 1, pp. 1–2). https://doi.org/10.54105/ijcns.a1402.051121
20. Baig, M. A. (2021). An Efficient Cluster Based Routing Protocol (ECCRP) Technique Based on Weighted Clustering Algorithm for Different Topologies in Manets using Network Coding. In Indian Journal of Data Communication and Networking (Vol. 1, Issue 2, pp. 31–34). https://doi.org/10.54105/ijdcn.b5011.041221
21. Raj, H., Duggal., A., M., A. K. S., Uppara, S., & S., S. M. (2020). Hand Motion Analysis using CNN. In International Journal of Soft Computing and Engineering (Vol. 9, Issue 6, pp. 26–30). https://doi.org/10.35940/ijsce.f3409.059620
22. Saroj, S. K., Yadav, M., Jain, S., & Mishra, R. (2020). Performance Analysis of Q-Leach Algorithm in WSN. In International Journal of Inventive Engineering and Sciences (Vol. 5, Issue 10, pp. 1–4). https://doi.org/10.35940/ijies.i0977.0651020
23. Murty, M. V. D. S. K., & Rajamani, Dr. L. (2023). Neighbour Node Ratio AODV (NNR-AODV) Routing Protocol for Wormhole Attack Detection in Manets. In International Journal of Emerging Science and Engineering (Vol. 11, Issue 4, pp. 1–9). https://doi.org/10.35940/ijese.d2547.0311423
24. Nixon, J. S., & Amenu, M. (2022). Investigating Security Issues and Preventive Mechanisms in Ipv6 Deployment. In International Journal of Advanced Engineering and Nano Technology (Vol. 9, Issue 2, pp. 1–20). https://doi.org/10.35940/ijaent.b0466.029222
25. Rajeev, H., & Chakkaravarty, Dr. M. (2023). Prediction of Cybercrime using the Avinashak Algorithm. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 4, Issue 1, pp. 5–10). https://doi.org/10.54105/ijainn.a1078.124123

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.

© Copyright: All rights reserved.