Chapter 24

A Survey of Security Challenges and Existing Prevention Methods in FANET

Jatin Sharma and Pawan Singh Mehra
Delhi Technological University, New Delhi, India

24.1 Introduction

A drone is a small flying device that can be moved independently by remote control and can fly autonomously. Among the various applications of drones are disaster rescue, battlefield communication, photography, aerial delivery and device-to-device communication. The essential elements of drones are batteries, propellers and motors, flight controller, IMU and magnetometer. There are various type of drones such as quadrotor, multirotor drones, fixed wing UAS, fixed wing hybrid UAS (Figure 24.1).

The paper is organized as follows. Section 24.1 is an introduction to FANETs, Section 24.2 describes various FANET protocols, Section 24.3 explores various security attacks and Section 24.4 describes previous work. Section 24.5 provides a table of security solutions and conclusions are provided in Section 24.6.

DOI: 10.1201/9781003371380-24

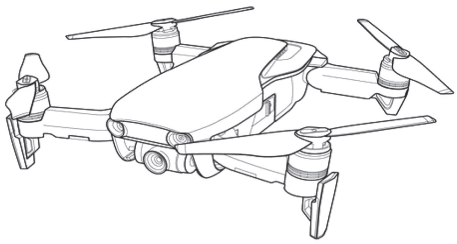

Figure 24.1 A single UAV drone.

24.2 FANET and Communication Protocols

Flying adhoc networks are networks that build on the fly without infrastructure. Their various advantages are [1]:

1. *Expense.* The expense of smaller UAVs is lower than larger UAVs.
2. *Survivable.* The failure of one node in FANETs cannot affect the UAV system as other nodes can play the same role as the failed one in an emergency.
3. *Speed.* The speed of a multi-UAV system is much faster as the number of UAVs can accomplish the task in minimum time.
4. *Expandability.* The multi-UAV system has the power to expand in case of mission requirement.
5. *Extended antenna range.* The multi-UAV system has the capability to cover a large area in reconnaissance and rescue operations.

Various kinds of communications are possible in FANETs:

- Inter-plane communication
- Intra-plane communication
- Ground station communication
- Ground sensor communication
- FANET–VANET communication

Figure 24.2 represent the A2G (air-to-ground) and A2A (air-to-air) communication.

The following sub-sections discuss various communication protocols.

24.2.1 Based on Physical Layer

- *FANET communication characterization.* Propagation model based on radio waves of FANET node-to-node links is identical to 2-ray ground schema.
- *Channel modeling.* The 2-state Markov model based on Rician fading is used to make the channel infrastructure-less among UAVs.

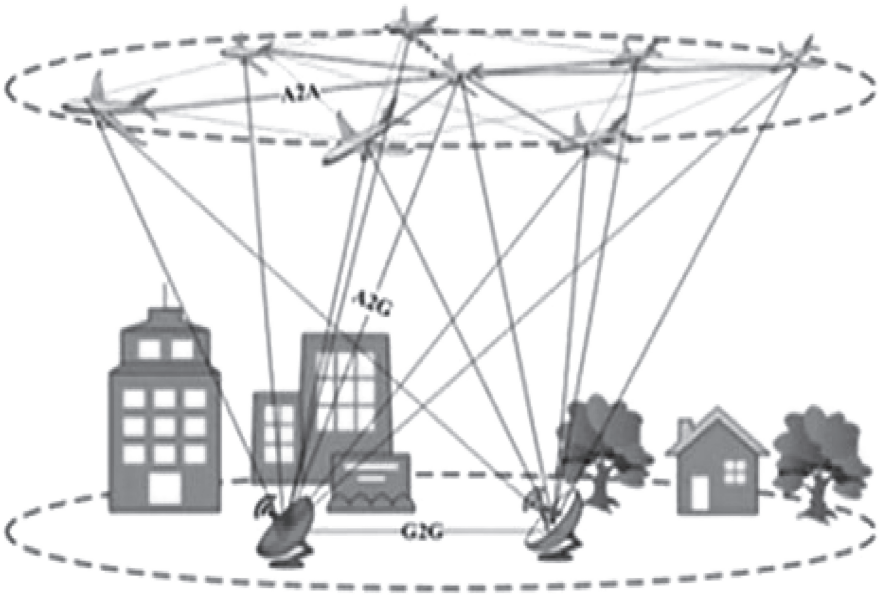

Figure 24.2 A2G and A2A communication.

- *Nakagami-based FANET radio propagation model.* In this model, the Nakagami-m fading channel was derived and a mathematical theorem evolved as output for link disconnection.
- *General link outage model.* In this model, the FANET node-to-node and UAV node-to-ground link disconnection over the defined fading channel was provided with the formula.
- *Many transmitters and receivers.* The packet transfer rate was improved in many receivers and transmitters for a longer time.

24.2.2 Based on MAC Layer

- *Adaptive MAC protocol approach for FANET nodes (AMUAV).* This approach delivers the controlling frames, i.e., CTS, RTS and ACK frames with its antennas propagating in every direction and DATA frame sent by antennas in a straightforward direction. This approach enhances E2E delay and error rate bit by bit in FANET UAVs.
- *Token-based MAC protocol.* This relies on the tokenization approach so as to modify link states and information on the link. The problem of code collision is resolved by the token-based approach. This approach enhances the number of bits per second using an MPR radio circuit and full duplex mode and also reduces latency.

24.2.3 Based on Network Layer/Routing Protocols

- *Proactive type.* For a limited time routing information is modified and kept in a 2D format such as DOLSR, in which the directed antenna concept is used so as to reduce latency and enhance packet delivery ratio.
- *Reactive type.* In this type of protocol, routing information is modified and kept only when the point or device finds a change in the network, such as on-demand routing based on a time slot which is used to eliminate collisions.
- *Hybrid Protocols.* In this type the functionality of two protocols – reactive and proactive – is joined together to achieve routing, for example, zone routing protocols.
- *Geographic type.* It predicts the movement of UAVs with the Gauss–Markov mobility model and uses this information to determine the next hop.
- *Position-based protocol.* This protocol determines the position of the particular UAV in the network. They are divided into two strategies, single path and multipath.
- *Swarm-based protocol.* This protocol is based on the behavior of animals.

24.3 Security Attacks and Issues

Attacks on the multi-UAV system can affect the whole network and, in such case, important information can be accessed by attackers while nodes are on the ground as well as on fly. There are two types of attacks.

24.3.1 Active Attacks

An active attack is used to modify data which affect operations or falsify statements. Active attacks include black hole and grey hole attacks [2], denial of service [3], and wormhole [4].

24.3.2 Passive Attacks

The purpose of a passive attack is to use the information without affecting resources, for example, monitoring UAV traffic and eavesdropping [5].

24.3.3 Other Types of Attack

- Spoofing attack based on GPS. The adversary sends a dummy GPS signal to the ground station which in turn forces navigation in a direction given by the adversary.
- Malware software installation attacks.

- Message alteration attacks.
- Distance-based attacks.
- Algorithmic-based attacks.
- Attacks based on integrity.
- Attacks based on confidentiality.
- Attacks based on privacy.
- Attacks based on availability.

The various security challenges are routing, UAV mobility and placement, scalability and reliability.

24.4 Literature Review and Related Works

Bekmezci et al. [1] cover various UAV design and protocol issues. They find security issues in omnidirectional antennas, location estimations and sharing of information, congestion avoidance, and flow control. The authors suggest various solutions but these are not relevant.

Cabuk et al. [6] describe SkyNet with manipulation of UAVs to collect information from individual nodes and desktops.

Khan et al. [7] describe threats between ground station and UAVs according to needs and types of assaults. and conclude that security is a significant issue.

Yaacoub et al. [8] examine information about a person's home, location, and behavior that can be found by aerial UAVs.

According to Youssef and Riham [6], there are risks when hackers use UAVs to make connection among internet of things (IoT) nodes. Adding FANET nodes to restricted areas in a no-fly-zone database is one way to protect yourself from these dangers.

Table 24.1 lists security requirements in the current scenario as represented by [1, 6, 8–12]. The security principles that are included, not included or partially included in these are labeled as covered, not covered and somewhat.

Existing security solutions proposed are the following.

In ref. [13], the OTP (one-time pad) technology was used to create secure communication between UAVs. In this approach, before encrypting the message, a replicated key is given and used with the message to obtain the cipher context with EX-OR operation, then to obtain the plain text, the cipher text and the replicated key were used with EX-OR. After successful decryption of the message the replicated keys were smashed. The performance was the best compared to AES-128.

In ref. [14], the enhanced frequency hopping technique was used to control UAVs. The authors of this paper have made the process complex by using passwords longer than 6 bytes.

In ref. [15], FANETs' systems are reviewed and their constraints analyzed. The authors present ECDSA digital signature algorithms based on elliptic curves and

Table 24.1 Requirements of Security

Ref.	*Authentication*	*Authorization*	*Confiden.*	*Integrity*	*Availability*	*Non Repud.*
[1]	Somewhat	Not covered	Somewhat	Not covered	Somewhat	Not covered
[6]	Covered	Somewhat	Covered	Covered	Covered	Somewhat
[8]	Covered	Covered	Covered	Covered	Covered	Covered
[9]	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered
[10]	Covered	Covered	Covered	Covered	Covered	Covered
[11]	Not covered	Not covered	Not covered	Not covered	Somewhat	Not covered
[12]	Covered	Covered	Covered	Covered	Covered	Covered

RSA to protect the UAVs from adversaries. Both algorithms have two keys, a secret key to keep communication strong and a public key. This method ensures the integrity of messages from the ground station.

In ref. [16], blockchain technology to secure and maintain data privacy is described. The blockchain system developed is so strong that it provides danger alerts to prevent unauthorized and unreliable access.

In ref. [17], the author proposes a Caesar cipher technique to keep MAVs (micro aerial vehicles) secure. This technique enciphers the data between MAV and ground control station. It is best suited for authentication and system reliability.

In ref. [18], the author proposes MAVLink security in terms of MAV-Sec and discusses various vulnerabilities. The four advanced encryption standard algorithms described are AES-CBC, ChaCha20, RC4, and counter mode. For secure communication between UAVs and ground station, ChaCha20 is used.

In ref. [19], the authors describe an IoT-based solution using the naive Bayes algorithm. The data captured from sensors on UAVs help detect threats with an accuracy of 97%.

In ref. [20], the author describes an intelligent system preventing encroachment activity on UAVs.

In ref. [21] proposes an eCLSC-TKEM communication security protocol technique that produces a unique key between UAVs and intelligent device by preserving the schedule.

In ref. [22], the author introduces cipher techniques and authentication to encrypt useful data using ChaCha20 and HIGHT encryption algorithms.

In ref. [23] a Raspberry pi system for reverting to the previous state if any UAV is attacked is described. For this purpose AES public keys are introduced before the sending process and authenticated during sending, which in turn enables self-destruction of UAVs in case of encroachment.

In ref. [24], the authors propose a hash function scheme for encryption. The system is validated with the help of Automated Validation of Internet Security Protocols and Application (AVISPA). Various security solutions are proposed.

In ref. [25], an adaptive trust strategy is proposed in the form of a lightweight mutual identity authentication scheme (ATSLIA). The proposed 2-way system involves authentication and elliptic curve cryptography between the ground station on the road and UAVs.

In ref. [26], physically unclonable functions (PUFs) and programmable packet-processing data planes are described. Hardware-based PUFs are used to provide authentication between UAVs and the ground control station which in turn provides ultra-low latency. [27] describes software-defined networking-based solutions such as adaptive SDN-based routing, QoS-based multipath routing protocol, Fuzzy C-means and GAP.

24.5 Security Solutions in Tabular Format

We present the various preventive measures to overcome vulnerabilities in the current system in the form of a table (Table 24.2). The table describes various proposed solutions, the year in which they were put forward, and comments.

Table 24.2 Proposed Solution in Survey

S.No.	*References*	*Duration*	*Proposed Solution*	*Remarks*
1	[13]	2019	OTP technology	Better encryption scheme and takes two or three milliseconds.
2	[14]	2018	eFHSS	Less time taken to detect attack.
3	[15]	2019	ECDSA and RSA algorithm	Ensures integrity.
4	[16]	2020	Blockchain	Ensures security with digital signature.
5	[17]	2015	Caesar cipher	This technique is best suited for authentication and system reliability.

(*Continued*)

Table 24.2 (Continued)

S.No.	References	Duration	Proposed Solution	Remarks
6	[18]	2019	MAVSec	For secure communication between UAVs and ground station, ChaCha20 algorithm is used.
7	[19]	2021	Naive Bayes algorithm	The data captured from sensors on UAVs helps in detection of threats with accuracy of 97%.
8	[20]	2020	K-nearest neighbor algorithm	Intelligent system to prevent intrusion and various attacks on UAVs.
9	[21]	2015	eCLSC-TKEM	Saves time needed to produce a key between UAV and intelligent device.
10	[22]	2021	ChaCha20 and HIGHT encryption	Proper UAV communication with fast execution of cipher technique.
11	[23]	2017	AES, Raspberry pi	To get back to the previous state if any UAV is attacked by any using Raspberry pi.
12	[24]		Hash function	Encryption scheme based on one-way hash functionality. AVISPA technique provides verification in this context.

(*Continued*)

Table 24.2 (Continued)

S.No.	References	Duration	Proposed Solution	Remarks
13	[25]	2022	ATS-LIA	Two-way system with authentication and elliptic curve cryptography approach between ground station on the road and UAVs.
14	[26]	2022	PUF-based UAV authentication	Provide authentication between UAVs and ground control station which in turn provides ultra-low latency.
15	[27]	2022	SDN-FANET	Software-defined networking-based solutions such as adaptive SDN-based routing, QoS-based multipath routing protocol, Fuzzy C-means and GAP

24.6 Conclusion

This chapter has described various vulnerabilities in the current system and discussed security solutions. Various FANET communication protocols and attacks have been defined. This paper can help researchers to identify techniques and solution to obtain secure communication between UAVs.

References

1. I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, May 2013, doi: 10.1016/J.ADHOC.2012.12.004.

2. J. Cai, J. Chen, and Z. Wang, "An adaptive approach to detecting black and gray hole attacks in ad hoc network," *2010 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, 2010, doi: 10.1109/AINA.2010.143.
3. J. P. Condomines, R. Zhang, and N. Larrieu, "Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation," *Ad Hoc Networks*, vol. 90, p. 101759, Jul. 2019, doi: 10.1016/J.ADHOC.2018.09.004.
4. E. E. Tatar and M. Dener, "Wormhole attacks in loT based networks," *Proc. - 6th Int. Conf. Comput. Sci. Eng. UBMK 2021*, pp. 478–482, 2021, doi: 10.1109/UBMK52708.2021.9558996.
5. X. Zhong, C. Fan, and S. Zhou, "Eavesdropping area for evaluating the security of wireless communications," *China Commun.*, vol. 19, no. 3, pp. 145–157, Mar. 2022, doi: 10.23919/JCC.2022.03.010.
6. R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones," *ACM Trans. Cyber-Physical Syst.*, vol. 1, no. 2, Nov. 2016, doi: 10.1145/3001836.
7. N. A. Khan, S. N. Brohi, and N. Jhanjhi, "UAV's applications, architecture, security issues and attack scenarios: A survey," pp. 753–760, 2020, doi: 10.1007/978-981-15-3284-9_81.
8. J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, Sep. 2020, doi: 10.1016/J.IOT.2020.100218.
9. A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Comput. Networks*, vol. 163, p. 106877, Nov. 2019, doi: 10.1016/J.COMNET.2019.106877.
10. "Scopus - Document details - Security issues in flying ad-hoc networks (FANETS) | Signed in." https://www.scopus.com/record/display.uri?eid=2-s2.0-85044241946&origin=inward (accessed Sep. 14, 2022).
11. A. Bujari, C. E. Palazzi, and D. Ronzani, "FANET application scenarios and mobility models", *Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, doi: 10.1145/3086439.3086440.
12. S. Rezwan and W. Choi, "A survey on applications of reinforcement learning in flying ad-hoc networks," *Electron*, vol. 10, no. 4, p. 449, Feb. 2021, doi: 10.3390/ELECTRONICS10040449.
13. S. Atoev, O.-J. Kwon, C.-Y. Kim, S.-H. Lee, Y.-R. Choi, and K.-R. Kwon, "The secure UAV communication link based on OTP encryption technique; the secure UAV communication link based on OTP encryption technique," *2019 Elev. Int. Conf. Ubiquitous Futur. Networks*, 2019, Accessed: Sep. 14, 2022. [Online]. Available: https://mavlink.io/en/protocol/overview.html
14. C. Bunse and S. Plotz, "Security analysis of drone communication protocols," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10953 LNCS, pp. 96–107, 2018, doi: 10.1007/978-3-319-94496-8_7.
15. M. J. Fernandez, P. J. Sanchez-Cuevas, G. Heredia, and A. Ollero, "Securing UAV communications using ROS with custom ECIES-based method," *2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS)*, 2019. doi: 10.0/Linux-x86_64.
16. R. Ch, G. Srivastava, T. Reddy Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.*, vol. 55, p. 102670, Dec. 2020, doi: 10.1016/j.jisa.2020.102670.
17. B. S. Rajatha, C. M. Ananda, and S. Nagaraj, "Authentication of MAV communication using Caesar Cipher cryptography," *2015 Int. Conf. Smart Technol. Manag. Comput. Commun. Control. Energy Mater. ICSTM 2015 - Proc.*, pp. 58–63, Aug. 2015, doi: 10.1109/ICSTM.2015.7225390.

18. A. Allouch, O. Cheikhrouhou, A. Koubaa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink protocol for Ardupilot/PX4 unmanned aerial systems," *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, pp. 621–628, Jun. 2019, doi: 10.1109/IWCMC.2019.8766667.
19. R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based cyber-security of drones using the Naïve Bayes algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 7, pp. 422–427, Sep. 2021, doi: 10.14569/IJACSA.2021.0120748.
20. S. M. Al-Abrez, K. M. A. Alheeti, and A. K. A. N. Alaloosy, "A hybrid security system for unmanned aerial vehicles," *J. Southwest Jiaotong Univ.*, vol. 55, no. 2, 2020, doi: 10.35741/ISSN.0258-2724.55.2.1.
21. J. Won, S. H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," *ASIACCS 2015 - Proc. 10th ACM Symp. Information, Comput. Commun. Secur.*, pp. 249–260, Apr. 2015, doi: 10.1145/2714576.2714616.
22. H. M. Ismael, Z. Tariq Mustafa Al-Ta, and A. Emails Mordasshani, "Authentication and encryption drone communication by using HIGHT Lightweight algorithm," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 11, pp. 5891–5908, May 2021, Accessed: Sep. 14, 2022. [Online]. Available: https://turcomat.org/index.php/turkbilmat/article/view/6875
23. K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on UAV network," *2017 First IEEE Int. Conf. Robot. Comput.*, 2017, doi: 10.1109/IRC.2017.56.
24. M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019, doi: 10.1109/JIOT.2018.2888821.
25. X. Du, Y. Li, S. Zhou, and Y. Zhou, "ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 4, pp. 1979–1993, 2022, doi: 10.1007/s12083-022-01330-7.
26. D. Pathak, P. Tammana, A. A. Franklin, and T. Alladi, "Accelerating PUF-based UAV authentication protocols using programmable switch," *2022 14th Int. Conf. Commun. Syst. NETworkS*, 2022, doi: 10.1109/COMSNETS53615.2022.9668481.
27. M. Abdelhafidh, N. Charef, A. Ben Mnaouer, and L. C. Fourati, "Software-defined networking for flying ad-hoc network security: A survey; software-defined networking for flying ad-hoc network security: A survey," *2022 2nd Int. Conf. Smart Syst. Emerg. Technol.*, 2022, doi: 10.1109/SMARTTECH54121.2022.00057.