Hindawi
Applied Computational Intelligence and Soft Computing
Volume 2022, Article ID 3330168, 9 pages
https://doi.org/10.1155/2022/3330168

Research Article

AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks

Sadoon Hussain[1], **Ahmed Sami**[2], **Abida Thasin**[1] and **Redhwan M. A. Saad**[3,4]

[1]*Department of Physic, College of Science, University of Mosul, Mosul, Iraq*
[2]*Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq*
[3]*Department of Electrical Engineering, Faculty of Engineering, Ibb University, Ibb 70270, Yemen*
[4]*Department of Computer Engineering, Faculty of Engineering, Cairo University, Giza 12613, Egypt*

Correspondence should be addressed to Sadoon Hussain; sadosbio113@uomosul.edu.iq

Received 13 August 2022; Accepted 5 September 2022; Published 16 September 2022

Academic Editor: Agostino Forestiero

Artificial intelligence has recently been used in FANET-based routing strategies for decision-making, which is a unique paradigm. For effective communication in flying vehicles that use routing protocols to accomplish tasks collectively, aerial vehicles are used in both civic and military applications. Aerial ad hoc networks are wirelessly connected, and designing routing schemes is difficult due to the rapid mobility. Ground base stations and satellites are frequently used to interconnect UAV ad hoc networks. This paper developed a novel routing protocol with a focus on ant behavior routing, which assists in end-to-end security. For the first time in flying networks, the column mobility model is used to evaluate the performance of routing protocols. While merging with aerial ad hoc networks, AI-based networking is a relatively new field. In simulation results, AntHocNet shows better results in comparison with other contemporary routing algorithms. Pheromone update process is used for data encryption in AntHocNet. This research study is performed on network simulator-2.

1. Introduction

The most important requirement for any AI-based network should be security. However, there are two types of security threats that are widely used: passive and active. Passive attacks are sometimes used by intruders to get around heavily secured data. Whenever active attacks are utilized, data can be easily accessed and changed. To encrypt plain text, the AES and DES methods use secret keys. Heuristic function is reinforced to use repeatedly artificial ants for new solutions. Binary ant colony optimization has been used to secure data from security attacks [1]. Hash functions, asymmetric keys, and symmetric keys are three types of cryptography techniques that encode and modify the security of information. Particle swarm optimization (PSO) based key generation algorithm is designed to make use of character code table to secure data, while ant colony optimization (ACO) algorithm produces unique keys and strategies to ensure proficiency in communication [2].

The topological scenario of wireless sensor network nodes is static. To counter security attacks, routing protocols is the optimal solution which can easily overcome on data transmission vulnerabilities. Intruder makes use of security attacks which include blackhole, grey-hole, and false routing updates; also, hello data packet attacks are utilized to disturb the transmission channels. The mentioned countermeasure can be easily tackled by using appropriate routing protocols. Multihop communication within network bio-inspired technique called ant colony optimization is used to work on path selection and adaptive security nature. In addition, graph theory and artificial neural networks will be quite helpful in routing techniques for securing communication standards. In addition, routing techniques can be used in smart grids [3, 4].

In this research study, routing performed well in comparison with i-ACO and LEACH in terms of end-to-end delay, overhead, and data forwarding [5]. Existing routing protocols have several security flaws. This research focuses

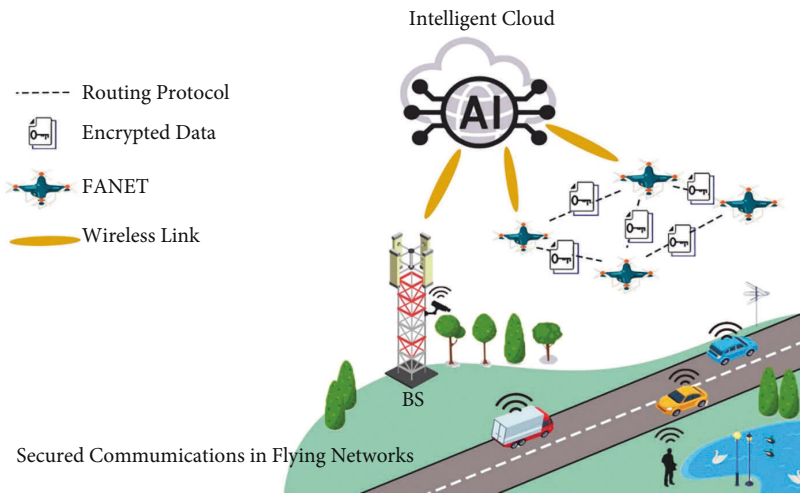

Figure 1: AI-enabled secure communication in flying networks.

on finding vulnerabilities in distributed hash table routing approaches. Security risks from the attacker's perspective include destination LID tempering, neighborhood attack, node joining, and authentication. This study has used digital signatures in order to swap logical identifiers and establish a trust between nodes [6]. The network life-time, on the other hand, is essential in any system. This research discusses a unique approach that focuses on energy efficiency, clustering, and fog nodes. The goal of this study is to develop a procedure based on the distance and residual energy associated with the network's cluster head [7].

The notion of AI-assisted routing in flying networks is visualized in Figure 1. Only encryption techniques can ensure the security of communication between aerial vehicles. Wireless communication channels connect unmanned aerial vehicles (UAV) to the base station. The information is stored using AI-based intelligent cloud computing. Using modern routing algorithms, secure communication in any network is achievable. The implementation of any algorithm is the most difficult task due to the dynamic movement of aerial vehicles. However, Table 1 illustrates the security techniques used in the area of aerial ad hoc networks.

AI-based flying network is designed to overcome on the issues related with real world applications of aerial vehicles. The technique of evolutionary computing is introduced in this research study which works on the basic principle of heuristic analysis. As drones need lightweight algorithms to secure communication medium in Internet of flying vehicles, a hybrid cryptographic security approach with high level of computing to ensure encryption using AES-256, ECC, and SHA256 is utilized for authentication [13]. For scaling up the network, convergence is the main issue which affect the energy level of every node. Enhanced pheromone method is considered to increase the life-line and path length [14].

The main contribution of this paper is as follows:

(i) AI-based heuristic routing protocol is designed for Internet of flying vehicles

(ii) Column mobility pattern is used to check the performance of secure routing schemes in the flying networks

(iii) Network throughput, bandwidth utilization, packet drop rate, and quality of experience is used in this research study

(iv) Aerial ad hoc networks are utilized in the field of information security and artificial intelligence

(v) IoT based flying vehicles are used as a real-life application

The organization of the rest of the paper is as follows: Section 2 discusses the literature review, followed by explanations of the proposed scheme in Section 3. Then, Section 4 presents the simulation environment. Lastly, Sections 5 and 6 presents results and concludes the paper and suggests future work.

2. Literature Review

Secure communication scheme in aerial vehicles have to maintain and manage specific area to employ hierarchical identity-based broadcast encryption. Packet transmission using the HIBBE technique is broadcasted as preassigned key to encrypt data. Mutual communication of UAVs uses the signcryption method to verify and authorize every flying node. This technique is utilized for master drones to give resistance towards denial-of-service attacks [15]. On the military side, the employment of aerial vehicles is very popular.

Between the UAVs and the base station, a secure protocol is implemented. BAN-logic, on the other hand, tested that the suggested protocol is valid. The protocol outperforms and responds to denial-of-service attacks, man-in-the-middle attacks, and UAV-to-UAV security [16]. Unmanned aerial systems are either having connection with the ground station and satellite or store the information on memory chips. Key negotiation approach in cryptography is used to develop security protocol which encrypt the data stored in

Table 1: Security techniques for FANETs.

Author	Used technique	Description
Atoev et al. [8]	One-time pad (OTP) encryption technique	This technique enables a secure link between the drone and the ground control station (GCS), with improved accuracy and execution time in comparison with other systems
He et al. [9]	Encryption bridging technique between IBE and ABE	A new encrypted data switching protocol was introduced that minimizes client computation and communication costs, especially when the client's data are encrypted and outsourced to a faraway cloud
Deng et al. [10]	An identity-based encryption transformation (IBET) model	Using identity-based encryption (IBE) and identity-based broadcast encryption (IBBE) for high-efficiency flexible sharing of encrypted data in the public cloud
Puthal et al. [11]	Selective encryption (SEEN) method	Secure data streams were developed by encrypting data using a symmetric key block cipher with multiple shared keys to protect data confidentiality and integrity from malicious attackers
Islam and Shin [12]	BUS: a block chain-enabled data acquisition scheme	Data acquisition scheme for IoT networks with the help of UAV swarm was designed, where the BUS technique is utilized to filter malicious devices. Simulation results illustrate the success of the technique and reduced energy consumption of IoT devices.

the system. The proposed implementation is installed on the FPGA boards which is utilized in a prototype [17].

The main problem with flying vehicles is network lifetime. To address this, a novel routing protocol is introduced in a dynamic pattern that can save one-third of the energy. Khan et al. worked on the ant colony optimization and incorporated energy stabilizing parameter to conserve energy. This is the first ever routing protocol in FANETs for energy efficiency which is named E-AntHocNet [18]. Due to mobile movement of aerial vehicles, wireless communication technology is used as a backbone. For indoor and open-air communication in flying vehicles, path loss model and machine learning classifier called decision tree is used to improve signal power. 3D centroid algorithm is used for node localization to find the actual location and also calculate the estimated location [19].

Routing protocols can be employed in flying networks to reduce end-to-end delays by employing a random way point mobility model that pauses until a path is randomly selected. AnHocNet is employed with other routing techniques which shows better results in comparison with other routing schemes [10]. However, ACO-based routing protocol can be employed in many real-time applications which include searching, monitoring, and rescue operations using aerial vehicles [20]. FANET network is infrastructure-less and nodes move in three dimensions. Software defines networks integration with FANET makes STFANET [21]. UAV-network can also be used in smart grid [22].

For efficient communication, routing protocol plays an important role in health care and sports using Internet of drones [23]. Therefore, maintaining the security level of IoT-networks intrusion detection system filters queue length packets to minimize false alarm and missed detection probabilities [24]. Figure 2 illustrates how data encryption is used in cloud computing to protect information transmitted by UAVs. The diagram also depicts the mechanics of attacks such as denial of service. However, Table 2 describes the detailed survey of security-based routing protocols.

ACO algorithm is a multipath method that can be quite useful in aerial networks for secure routing. A multiobjective function can be utilized to save residual energy while assuring low-cost routing. Ant-based heuristic computation relies on the pheromone update process to improve and solve security attacks regarding networks [34].

3. Proposed Scheme

AntHocNet is a routing technique for securing communication between nodes in aerial networks. This method is based on ant colony optimization, which is a hybrid methodology that combines reactive and proactive techniques. The three processes that make up the main working strategy are as follows:

(1) Evaporation

(2) Concentration

(3) Reinforce learning

The basic working of AntHocNet is explained in Figure 3, where the process of evaporation and concentration directly connects with pheromone update. If the concentration of pheromone will be high, then solution will be optimal. The term concentration is related with the evaporation of pheromone. The proposed technique easily overcomes coverage, packet drop rate, throughput, and bandwidth utilization. Also, due to quality of service, this routing protocol easily improves the overall life-time of flying network. However, reinforcement learning is used to train the aerial vehicles from environment which gives best results. This novel routing easily improves aerial vehicles performance in many applications which include forest monitoring, surveillance of border areas, filming, and criminal catching. Due to the dynamic pattern of flying vehicles, deployment of every new technique is a very tough task to perform. AntHocNet is compared with other advance techniques like ZRP, M-DART, DSR, and DSDV; in addition, AOMDV is utilized.

Column mobility pattern is used as the mobility model in aerial ad hoc networks for scanning and searching the network environment. Mobile node has a proper reference point which easily moves UAVs in the forward direction.

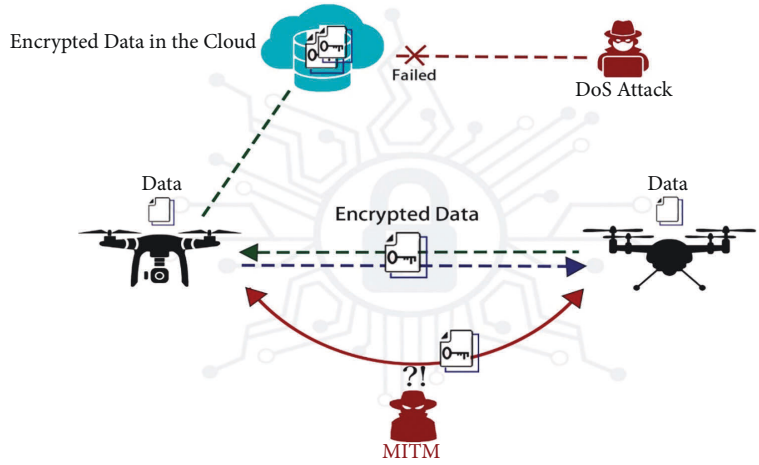

Figure 2: Data encryption and security attacks in aerial networks.

Table 2: Security based routing protocols.

Authors	Used protocol	Used environment	Attack type	Routing table	Encryption	Filtering malicious nodes	Privacy protection	Light weight
Shin et al. [25]	RO_INIT and RO_HO-based protocol	IoT	Exhaustion attack	No	Yes	No	Yes	No
Bujari et al. [26]	ESMR protocol	IoT	—	Yes	Yes	No	Yes	Yes
Shi et al. [27]	TDL-based protocol	WSN	Packet dropping attacks	Yes	No	Yes	No	Yes
Wang et al. [28]	TUE-OLSR protocol	MANET	Black hole and grey-hole attack	Yes	No	Yes	No	No
Kojima et al. [29]	ISDSR + protocol	Ad hoc	Active attacks	No	Yes	No	No	No
Ahutu and El-Ocla [30]	Multihop routing protocol	WSN	Wormhole attack	Yes	No	No	No	Yes
El-Semary and Diab [31]	BP-AODV protocol	MANET	Black hole attack	Yes	No	Yes	No	No
Stute et al. [32]	LIDOR protocol	IoT	DoS and wormhole attack	No	Yes	Yes	No	Yes
Velusamy et al. [33]	A cross-layer trust evaluation protocol	Smart grid	Cross-layer attacks	No	No	Yes	No	No

Also, at each time interval, a new reference point is calculated in account with the old reference point [26].

4. Simulation Environment

The simulation environment consists of thirty aerial vehicles and one base station which is distributed in ad hoc manner. Network simulator-2 is used to perform the evaluation of routing protocols. Topological scenario contains three-dimensional structure in flying vehicles which include x, y, and z. However, 1000 m is used for each dimension; also, the experimentation is performed in 180 seconds. Figure 4 elaborates the topological structure of aerial vehicles connected with the base station. Deployment of routing techniques in network simulator 2 is a very tough task. Also, the physical structure of the UAV-network is properly presented in Figure 4.

5. Results and Discussion

AntHocNet is a heuristic computing method that is inspired by ant behavior. When it concerns to evaluating routing algorithms, ant-based routing exhibits the most diversity in terms of throughput. Figure 5 shows how routing techniques monitor network performance to see how many data packets are received per unit time.

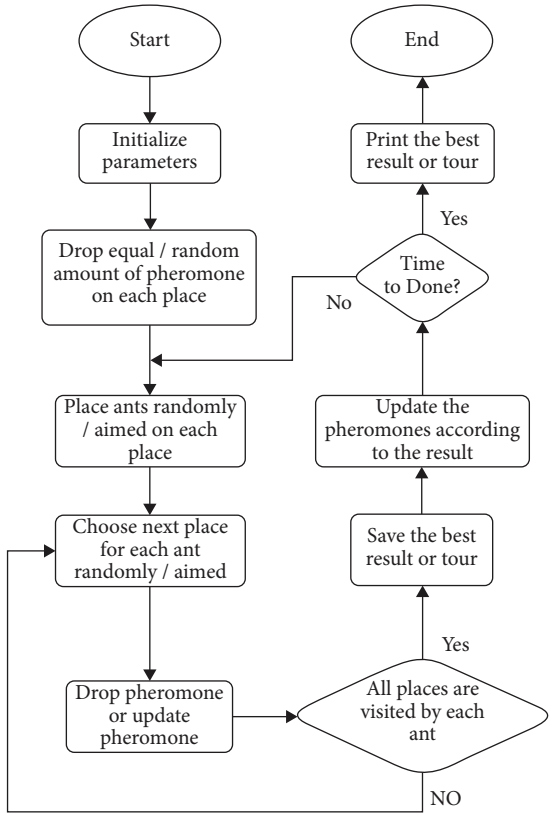

Figure 3: AntHocNet routing in aerial networks.

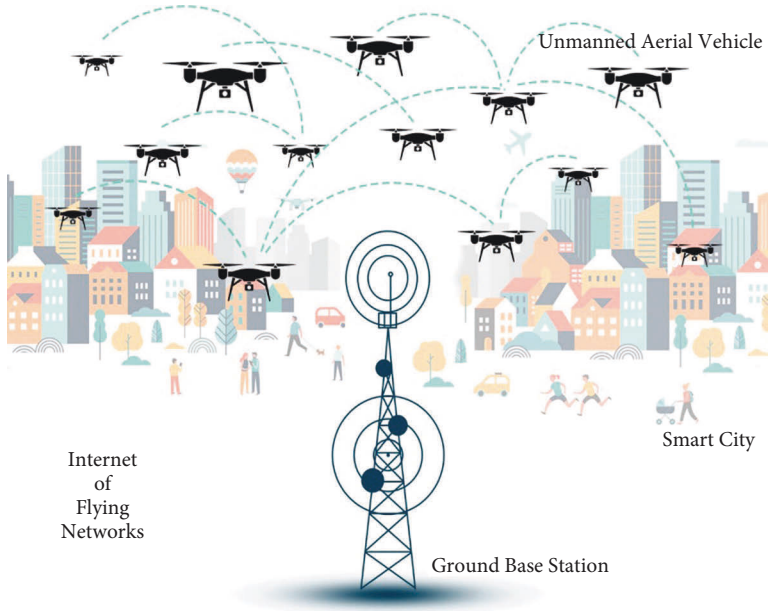

Figure 4: Secure communication using Internet of flying networks.

Figure 6 illustrates bandwidth utilization to sense the transmission capacity of the flying network. However, AntHocNet shows optimal results in terms of network/bandwidth in comparison with dynamic source routing and other routing schemes.

Packet drop rate is visualized in Figure 7, where bio-inspired scheme called AntHocNet shows less packet drop analysis on 40 to 140 seconds and 160 to 180 seconds. In comparison with other techniques, packet drop is very much reduced.

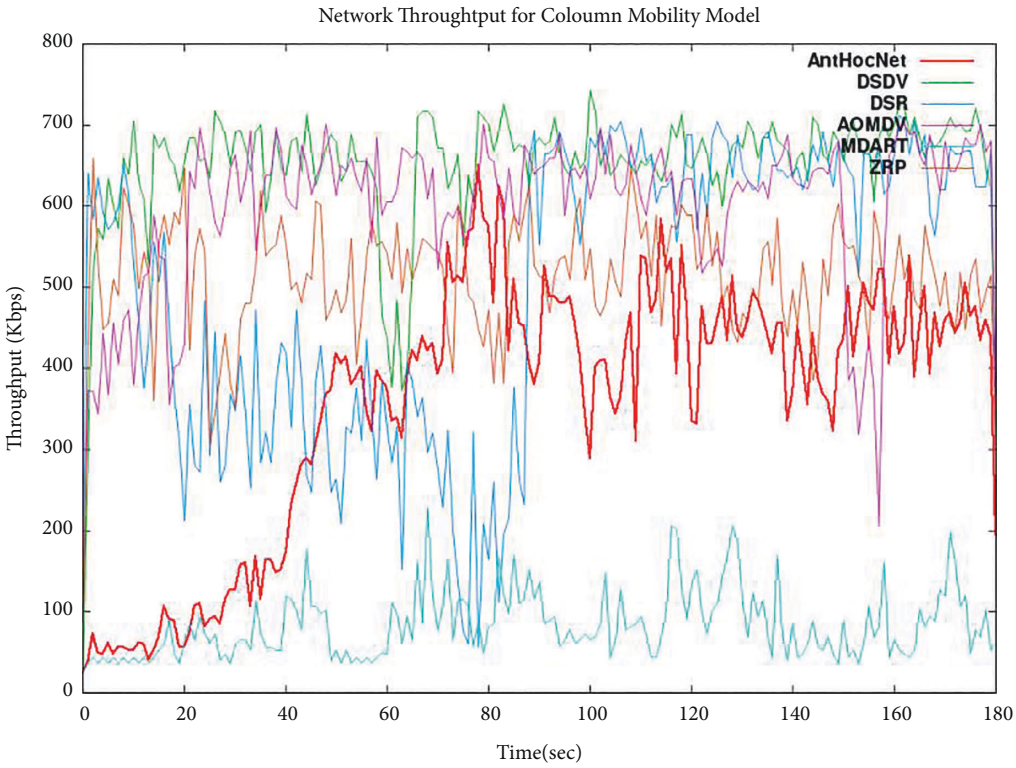

Figure 5: Network throughput for column mobility model using routing protocols.

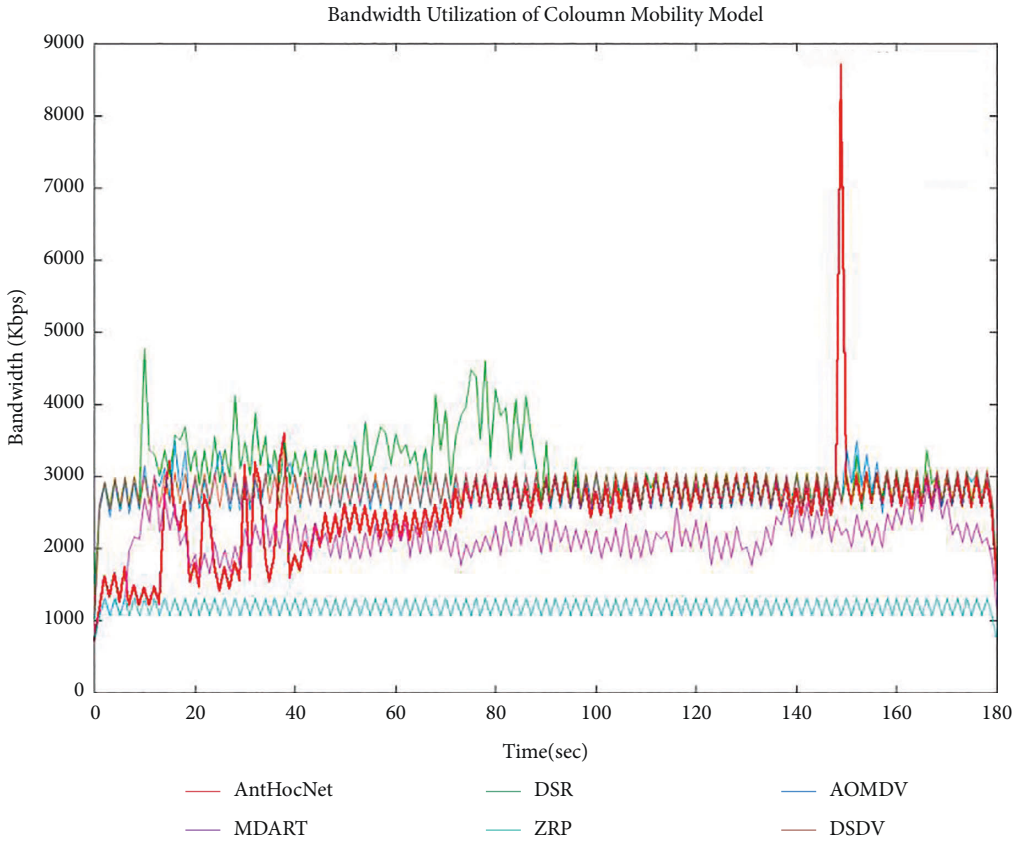

Figure 6: Bandwidth utilization for column mobility using AntHocNet, DSR, AOMDV, M-DART, ZRP, and DSDV.

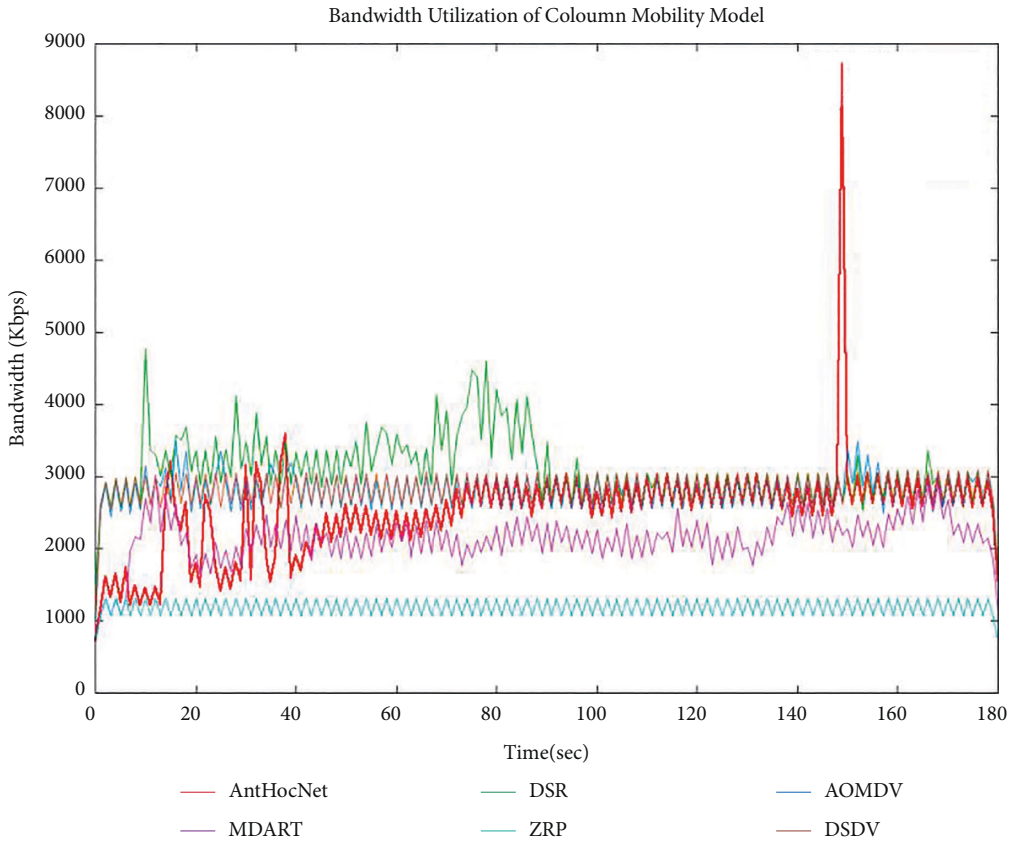

Figure 7: Packet drop rate for column mobility pattern.

6. Conclusion

AI-enabled flying networks are a newly emerged area that provides a better understanding of artificial intelligence and UAVs. There exist many applications such as rescue operations, disaster, searching, and monitoring. However, routing protocols are quite helpful, especially in optimal and secure communication. In this paper, the ant colony optimization-based routing technique is introduced which is used to secure communication standards within the network. Drone networks are regularly changing physical structure which is quite vulnerable. Therefore, a comparative analysis of routing protocols is properly discussed where AntHocNet performed well in terms of packet drop rate, throughput, and bandwidth utilization. Around 93% of packet drop analysis is optimized due to AntHocNet. Also, bandwidth utilization is improved by 90% in comparison with other routing techniques. Moreover, throughput is used to check the number of received data packets with respect to time. Therefore, the throughput level is enhanced by more than 95% in comparison with traditional routing techniques. The topology of flying vehicles is dynamic. However, to address this problem, security is a key consideration. Ant behavior routing is based on heuristic computing to secure communication between flying nodes. Thus, this research proposed a novel routing protocol with a focus on ant behavior routing, which assists in end-to-end security. The proposed algorithm is compared with other legacy protocols which include DSR, AOMDV, M-DART, ZRP, and DSDV. The simulation results illustrated that AntHocNet has shown better performance in accordance with throughput, network utilization, and packet drop analysis. The experience is evaluatedby combining the parameters quality to finalize the aerial network life-line. Column mobility model is deployed in the aerial networks.

In the future, particle swarm-based routing should be introduced to secure communication among aerial vehicles. Also, hybrid mobility models need to be designed for FANETs. In addition, artificial intelligence, machine learning, and computational intelligence will be the optimal solution to improve communication standards in FANETs.

Data Availability

This research study was performed on network simulator-2.

Disclosure

This paper has been removed from SSRN.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Khan, W. Shahzad, and F. A. Khan, "Cryptanalysis of four-rounded DES using ant colony optimization," in *Proceedings of the 2010 International Conference on Information Science and Applications*, pp. 1–7, Seoul, Republic of Korea, April 2010.

[2] P. Baliyan, P. Chandra, S. Srivastava, and I. Kaur, "Survey paper key generation using ant colony optimization technique," in *Proceedings of the 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 809–811, Greater Noida, India, December 2020.

[3] A. Forestiero, C. Mastroianni, and G. Spezzano, "A multi-agent approach for the construction of a peer-to-peer information system in grids," *Self-Organization and Autonomic Informatics (I)*, vol. 135, pp. 220–236, 2005.

[4] A. Forestiero, "Heuristic recommendation technique in internet of things featuring swarm intelligence approach," *Expert Systems with Applications*, vol. 187, Article ID 115904, 2022.

[5] N. A. Alrajeh, M. S. Alabed, and M. S. Elwahiby, "Secure ant-based routing protocol for wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 9, no. 6, Article ID 326295, 2013.

[6] R. Kousar, M. Alhaisoni, S. A. Akhtar, N. Shah, A. Qamar, and A. Karim, "A secure data dissemination in a DHT-based routing paradigm for wireless ad hoc network," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–32, 2020.

[7] A. P. Abidoye, E. O. Ochola, I. C. Obagbuwa, and D. W. Govender, "An improved ant colony optimization algorithm: a technique for extending wireless sensor networks lifetime utilization," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, 2020.

[8] S. Atoev, O. Kwon, C. Kim, S. Lee, Y. Choi, and K. Kwon, "The secure UAV communication link based on OTP encryption technique," in *Proceedings of the 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 1–3, Zagreb, Croatia, July 2019.

[9] K. He, Y. Mao, J. Ning et al., "A new encrypted data switching protocol: bridging IBE and ABE without loss of data confidentiality," *IEEE Access*, vol. 7, pp. 50658–50668, 2019.

[10] H. Deng, Z. Qin, Q. Wu et al., "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3168–3180, 2020.

[11] D. Puthal, X. Wu, N. Surya, R. Ranjan, and J. Chen, "SEEN: a selective encryption method to ensure confidentiality for big sensing data streams," *IEEE Transactions on Big Data*, vol. 5, no. 3, pp. 379–392, 2019.

[12] A. Islam and S. Y. Shin, "BUS: a blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019.

[13] F. Ronaldo, D. Pramadihanto, and A. Sudarsono, "Secure communication system of drone service using hybrid cryptography over 4g/lte network," in *Proceedings of the 2020 International Electronics Symposium (IES)*, pp. 116–122, Surabaya, Indonesia, September 2020.

[14] X. Li, B. Keegan, and F. Mtenzi, "Energy efficient hybrid routing protocol based on the artificial fish swarm algorithm and ant colony optimisation for WSNs," *Sensors*, vol. 18, no. 10, p. 3351, 2018.

[15] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y.-N. Li, "Secure communications in unmanned aerial vehicle network," in *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 601–620, Melbourne, Australia, December 2017.

[16] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, "Drone secure communication protocol for future sensitive applications in military zone," *Sensors*, vol. 21, no. 6, p. 2057, 2021.

[17] J. A. Steinmann, R. F. Babiceanu, and R. Seker, "UAS security: encryption key negotiation for partitioned data," in *Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS)*, pp. 1E41–1E47, Herndon, VI, USA, April 2016.

[18] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access*, vol. 8, pp. 56371–56378, 2020.

[19] I. U. Khan, R. Alturki, H. J. Alyamani et al., "RSSI-controlled long-range communication in secured IoT-enabled unmanned aerial vehicles," *Mobile Information Systems*, vol. 2021, Article ID 5523553, 11 pages, 2021.

[20] I. U. Khan, S. Z. Nain Zukhraf, A. Abdollahi, S. A. Imran, I. M. Qureshi, and M. A. Aziz, "Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles," in *Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, pp. 1–6, St. Petersburg, Russia, November 2020.

[21] T. Dapper e Silva, C. F. Emygdio de Melo, P. Cumino, D. Rosário, E. Cerqueira, and E. P. De Freitas, "STFANET: SDN-based topology management for flying ad hoc network," *IEEE Access*, vol. 7, pp. 173499–173514, 2019.

[22] A. Forestiero, C. Mastroianni, and G. Spezzano, "Building a peer-to-peer information system in grids via self-organizing agents," *Journal of Grid Computing*, vol. 6, no. 2, pp. 125–140, 2008.

[23] I. U. Khan, M. A. Hassan, M. D. Alshehri et al., "Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing," *Journal of Healthcare Engineering*, vol. 2021, Article ID 1686946, 11 pages, 2021.

[24] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in IoT networks," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2057–2070, 2020.

[25] D. Shin, K. Yun, J. N. Kim, P. V. Astillo, J. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019.

[26] A. Bujari, C. T. Calafate, J.-C. Cano, P. Manzoni, C. E. Palazzi, and D. Ronzani, "Flying ad-hoc network application scenarios and mobility models," *International Journal of Distributed Sensor Networks*, vol. 13, Article ID 155014771773819, 10 pages, 2017.

[27] P. Shi, C. Gu, C. Ge, and Z. Jing, "QoS aware routing protocol through cross-layer approach in asynchronous duty-cycled WSNs," *IEEE Access*, vol. 7, pp. 57574–57591, 2019.

[28] X. Wang, P. Zhang, Y. Du, and M. Qi, "Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network," *IEEE Access*, vol. 8, pp. 47675–47693, 2020.

[29] H. Kojima, N. Yanai, and J. P. Cruz, "ISDSR+: improving the security and availability of secure routing protocol," *IEEE Access*, vol. 7, pp. 74849–74868, 2019.

[30] O. R. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020.

[31] A. M. El-Semary and H. Diab, "BP-AODV: blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019.

[32] M. Stute, P. Agarwal, A. Kumar, A. Asadi, and M. Hollick, "LIDOR: a lightweight DoS-resilient communication protocol for safety-critical IoT systems," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6802–6816, 2020.

[33] D. Velusamy, G. Pugalendhi, and K. Ramasamy, "A cross-layer trust evaluation protocol for secured routing in communication network of smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 193–204, 2020.

[34] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks," *Applied Soft Computing*, vol. 77, pp. 366–375, 2019.

[35] I. U. Khan, S. B. H. Shah, L. Wang, M. A. Aziz, T. Stephan, and N. Kumar, "Routing protocols & unmanned aerial vehicles autonomous localization in flying networks," *International Journal of Communication Systems*, Article ID e4885, 2021.

[36] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.