# Analysis of Routing Attacks in FANETs

Ozlem Ceviz[1,2(✉)], Pinar Sadioglu[2], and Sevil Sen[2]

[1] Department of Computer Engineering, Sivas University of Science and Technology, Sivas, Turkey
ozlemceviz@sivas.edu.tr

[2] WISE Laboratory, Department of Computer Engineering, Hacettepe University, Ankara, Turkey
{n19249120,ssen}@cs.hacettepe.edu.tr

**Abstract.** Nowadays, Unmanned Aerial Vehicles (UAV) are widely used in a variety of fields, especially in military and industrial applications. However, the usage of a single UAV has begun to be insufficient in most missions. A single UAV may not complete its mission in cases of rapid depletion of its batteries, limited field of view, long-term performance of a task, a fall or a malfunction in the system due to an external effect. In such cases, Flying Ad Hoc Networks (FANETs) that allow more than one UAV to participate in a common network and execute complex tasks in an organized manner is recommended. However, FANETS are target of attacks due to being used in critical applications. Moreover, they are vulnerable to a variety of attacks due to their very nature and the cooperative routing protocols they use. Moreover, FANETs requires new security solutions or adaptation of existing security solutions of Mobile Ad Hoc Networks (MANETs), since it has much higher mobility than MANETs. Since mobility could affect security in different ways, at first attacks against FANETs should be analyzed. This is the main aim of this study. In this paper, various attacks against FANETs, namely dropping, blackhole, sinkhole, flooding attacks are analyzed. This is the first study that presents a comprehensive attack analysis in FANETs by simulating realistic network scenarios, where UAVs move in 3D as in real life.

**Keywords:** FANET · UAV · AODV · Routing attacks · Blackhole attack · Flooding attack · Dropping attack

## 1 Introduction

Unmanned aerial vehicle (UAV) systems have started to be used in many areas with the rapid development of technology. They are already frequently used in military, industrial and civilian applications. Especially, UAVs being work as a group without human intervention has led to further expansion of their research areas. However, in order to work in groups, they need to set up a communication network among themselves at first. Ad hoc networks, which can be formed without the need of human intervention, resolve faults and organize


W. Bao et al. (Eds.): ADHOCNETS 2021/TridentCom 2021, LNICST 428, pp. 3–17, 2022.
https://doi.org/10.1007/978-3-030-98005-4_1

themselves, are suitable for providing network connectivity between UAVs [14]. However, high speeds and mobility of UAVs, in contrast to many other type of ad hoc networks, results in the topology to change very dynamically. Therefore, a new type of ad hoc networks called Flying Ad Hoc Networks (FANETs) has emerged and becomes one of the popular research areas [13]. FANETs have been used in many applications in order to execute specialized tasks such as monitoring, surveillance and reconnaissance, environmental surveillance. In such applications, nodes could report their findings to ground controller systems or designated nodes in the network [12,25].

FANETs are used in many applications, especially mission-critical ones, which make them the target of new attacks. First of all, the use of wireless links makes the network susceptible to eavesdropping and active interference attacks. Furthermore, routing protocols designed for ad hoc networks rely on the cooperativeness of nodes, which makes insider attacks to be very effective in such networks. Although AODV protocol is a popular routing protocol for FANETs, it is vulnerable to attacks [10]. High mobility of such networks could also affect security in different ways. On the one hand, mobility allows attackers to evade from security solutions while damaging the network. On the other hand, the effect of attacks could be limited on highly mobile targets. Controller systems in the network can be the target of attacks such as Denial of Service (DoS) attacks, and hence the availability of the network can be compromised.

New security solutions should be improved for FANETs. While there are many security proposals for MANETs in the literature, they are not directly applicable to FANETs due to their high level mobility. Furthermore, the existence of ground controller systems allows to use such nodes in security solutions. On the other hand, there is no central points in typical MANETs and all data are distributed in MANETs. Furthermore, UAVs move in 3D contrary to nodes in MANETs and VANETs. Moreover, they might have different mobility models than other type of ad hoc networks. For example, in order to complete some missions, they might fly together in one direction as a group and move periodically towards to the controller ground system. Therefore, new security solutions and architectures should be developed for FANETs or the existing solutions proposed for ad hoc networks should be adapted to FANETs. This requires attacks against FANETs to be thoroughly analyzed, which is the main aim of the current study.

In this study, the effects of various routing attacks against FANETs are analyzed. AODV, which is one of the most popular routing protocols for ad hoc networks, are used. AODV is also a popular protocol in FANETs due to its simplicity and low overhead [23]. Attacks, namely dropping, flooding, blackole and sikhole are analyzed on networks with varying percentage of attackers from 5% to 20%. The 3D Gaussian Markov Model is used as the mobility model in order to simulate flying nodes. While studies in the literature still use 2D mobility models such Random Waypoint Mobility Model and low node speeds such as 20 m/s that is suitable for MANETs applications [17,21], here realistic network scenarios for FANETs are simulated by using Ns-3 [16]. To the best of the authors' knowledge, this is the first study that rigorously analyze attacks against FANET

on realistic network scenarios. The effects of attacks on simulated networks are evaluated by using packet delivery ratio, overhead and end-to-end delay.

The rest of this paper is organized as follows. Section 2 summarizes the related studies in the literature. Section 3 makes a brief introduction to the AODV protocol at first, then introduces the mobility model and attacks simulated in this study. Section 4 gives details about the experimental settings, and presents the attack analysis results. Finally, Sect. 5 concludes the paper.

## 2 Related Work

Although there are many studies on MANETs security in the literature, research on FANETs security is still immature even though they have been started to use in many applications. There are quite a number of studies that analyze attacks against AODV on mobile ad hoc networks in the literature [9,11,15,19]. In [15], both atomic and composite attacks against AODV are systematically presented. Jain et al. [11] and Dokurer et al. [9], not only analyze blackhole attacks, but also propose solutions for blackhole attacks by improving AODV. Both approaches show similarity since they ignore the firstly arrived RREP message to the source node based on the assumption this reply packet is from the attacker node. In [19], again, the effect of blackhole attacks are evaluated on networks using different routing protocols, AODV and OLSR. The results show that the AODV protocol shows better performance than the OLSR protocol. However if there is no attack in the network, OLSR provides higher throughput on small networks.

UAVs can be a potential target for attackers, whether they are part of a group as in ad hoc networks or single, in order to damage the device and/or access the data it contains. The impact of such threats targeting its privacy, security and physical integrity can severely affect both for the mission of UAV or to the network it is included in [2,3]. Moreover, multi-UAV communication is exposed to additional threats for trust establishment and secure communication mechanisms. FANETs have higher levels of node mobility and hence more frequent changes in network topology than traditional MANETs. In [4,20], authors discuss the unique characteristics of FANETs and their challenges. Bekmezci et al. [5] address security requirements of FANETs and possible threats against these highly networks. Furthermore, the authors present well-known ad hoc network attacks and discuss security solutions for such attacks on FANETs.

There are a few security solutions proposed for FANETs in the literature. Some studies [6,24] propose solutions for sybil attacks. Walia et al. [24] proposes a mutual authentication technique in order to detect sybil attack. In this method, each node checks its neighbor nodes and if there are different neighbors with the same ID, the node is marked as malicious and monitored. If this marked node changes its identity, it is assumed to be malicious. The proposed method has maximum throughput, minimum overhead and packet loss compared to other methods. Another proposed solution from Bhatia et al. [6] consists of monitoring, detection and isolation steps to identify malicious nodes triggering the sybil attack. In another study [8], a hybrid intrusion detection system is proposed.

The proposed method consist of two steps. Firstly, the spectral analysis is used to generate a specific traffic signature which offers a basic degree of knowledge regarding the type of intrusion in the network. Secondly, with the output of the first step, the controller/observer-based estimation step evaluates the level of attack observed in the network.

To sum up, even though routing attacks against AODV are extensively studied in the literature, different characteristics of FANETs such as having nodes with higher speeds, moving in 3D requires a new analysis of attacks on these highly mobile networks. The lack of such an analysis also negatively impacts the development of security solutions for FANETs.

## 3 Background

### 3.1 Routing Protocol: AODV

AODV is widely used in ad hoc networks, where FANETs are no exception. Since there is high mobility in FANETs, routing protocols proposed for them seek to establish and maintain communication between end points in such dynamic topologies. AODV is a reactive and multi-hop routing protocol that responds to this request. AODV enables the rapid discovery of routes to a new destination and cancels out inactive routes [18]. Due to high speeds of UAVs, FANETs experience frequent link breakages and disconnection problems.

AODV has two main mechanisms: route discovery and route maintenance. In the route discovery phase, the source node, who does not have a valid route to the destination node in its routing table, broadcasts route request (RREQ) packets. Any node having a valid route to the destination could send a unicast route reply (RREP) packet to the source node. The source node selects the freshest and the shortest path (having minimum number of hops) to the destination. In the route maintenance mechanism, locally detected broken links are announced to other nodes by using route error (RERR) packets. These packets are frequently broadcast to the whole network.

### 3.2 Attacks

Four type of attacks against AODV are analyzed in this study.

**Sinkhole Attack.** In this attack scenario, the malicious node aims to attract network traffic to itself by advertising a better route to the destination. This attack often lays the foundation for further attacks such as selective dropping, modification attacks.

In this study, when the attacker receives a RREQ message, it replies with a fake RREP that claims that it is one hop away from the destination node, hence it increases its chance to be selected as the shortest path. Moreover, it advertises itself as the freshest route to the destination by increasing the destination sequence number, hence in this case it guarantees to be selected as the route to

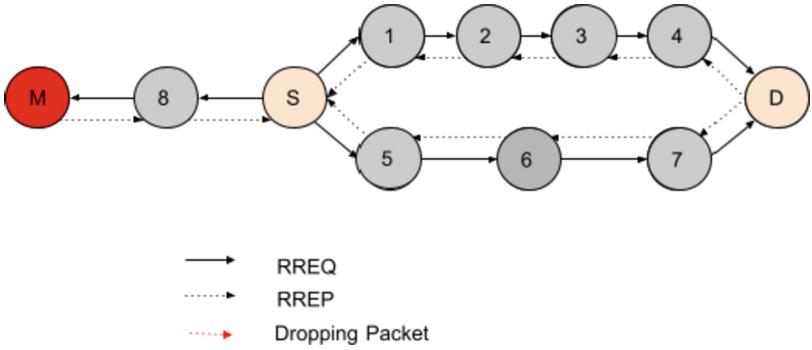


**Fig. 1.** Blackhole attack

the destination. When this route is selected, the attacker listens to all communication between the source and the destination nodes, therefore it is called as the sinkhole attack.

**Dropping Attack.** In this simple attack scenario, the attacker simply drops packets it received. It could selectively drop packets such as packets destined to a particular destination. Or he could randomly drop some packets in order to be more evasive, however in this case the effect of the attack is expected to be more limited. Besides data packets, the attacker could also drop routing control packets. In this case, active routes might not be built or inactive routes might not be announced in time. Such cases result in re-initiating the route discovery mechanism, which might consume network resources, cause congestion and delays. In this study, the attacker drops all data packets it received.

**BlackHole Attack.** Blackhole attack is a composite attack that performs sinkhole and dropping/modification attacks consecutively. Firstly it directs the network traffic to itself by advertising it has the best route to the destination, then it performs other attacks on the network traffic it receives such as modification, dropping, fabrication attacks. In the simulations here, in the first phase of the attack, the sinkhole attack is carried out as defined above, then only the dropping attack is performed in the second phase of this attack.

In Fig. 1, a blackhole attack is demonstrated. The source node (S) wants to discover a route to the destination node (D) by broadcasting a RREQ message. When the malicious node (M) receives one of these RREQ messages, it replies with a fake RREP. As shown in the figure, even M is not in the route to the destination, it receives data packets sent from S to D, since it claims itself to be in the shortest path to the destination.

**Ad Hoc Flooding Attack.** In this attack scenario, the attacker takes the advantage of high number of messages sent in the route discovery mechanism

in order to overwhelm the network. In this DoS attack, malicious nodes send a large number of RREQ messages for the selected nodes. This attack results in increasing the network traffic, consuming network and nodes resources, breaking the connection between nodes, and interrupting data transmitting. In the simulations, a random destination node is selected and 20 new RREQ messages are sent to discover routes to this destination node. The attack is repeated every 3 s for another destination node that is randomly selected.

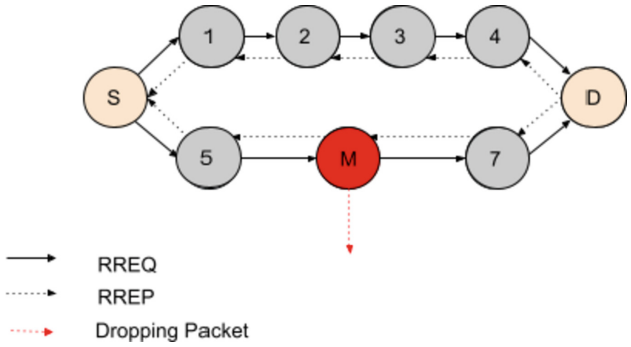


**Fig. 2.** Dropping attack in AODV protocol

### 3.3 Gauss-Markov (GM) Mobility Model

In order to simulate the mobility of UAVs in a realistic way, a three-dimensional mobility model should be used in the experiments. For that reason, 3D Gauss-Markov (GM) Mobility Model, which is a time-based mobility model designed with a single adjustment parameter to prevent sharp motion changes and to integrate various randomness adaptations [22] is used in this study. Since the movements of a node between its consecutive positions must be harmonious [7], the model keeps the previous movements in its memory. The mobility behaviour of nodes are adjusted by the $\alpha$ parameter, which takes values between zero and one. While $\alpha$ is 0, it corresponds to a memory-free model (i.e. random mobility). While it gets closer to 1, the motion becomes more predictable.

## 4 Attack Analysis

The main purpose of this study is to analyze routing attacks against FANETs. Therefore, a number of networks is simulated firstly without attacks, and then with the attacks described above. Finally, the performance of all simulated networks is analyzed. Here, the simulation environment is introduced below at first, then the effect of attacks on these simulated networks are discussed in the subsequent sections.

### 4.1 Simulation Settings

In this study, the well-known network simulator, Ns-3 [16] is employed to simulate networks and attacks against FANETs. In order to see the multi-hop characteristics of AODV, each network consists of 25 nodes, where one of them is a mobile server node. Each network is run without attacks, then run with blackhole, sinkhole, dropping and ad hoc flooding attacks separately. Different ratios of attackers are applied from 5% to 20% and the position of attackers are selected randomly five times for each network topology. Hence 70 (14×5) network topologies are executed for each attack type and ratio, and the average of performance metrics on these 70 networks are given in the results. As noted above, 3D Gaussian Markov Model is used in order to represent nodes' mobility in 3D. $\alpha$ value is started from 0.495 in order to keep the balance between random mobility and predictable mobility and, each time it is increased by 0.001 for simulating a different network topology. The speeds of nodes are set to 720 km/h as in real life. In order to be compatible with FANETs, the 802.11n MAC protocol is used at 5 GHz [1]. The transmission range of the nodes is determined as 250 m for the given network area. Each node sends 1024-byte 15 UDP packets to the server node every 0.5 s. All simulation parameters are summarized in Table 1.

The following performance metrics are employed in order to see the effects of attacks on networks: packet delivery ratio, end-to-end delay, and overhead metrics. Packet delivery ratio (PDR) is the average of the ratio of the total number of packets received by all nodes in the network to the total number of packets destined for the same nodes. End-to-end (E2E) delay is the measurement in seconds, of the average of all delays that occur in the network during data transmission between end communication points. Overhead is the ratio of the total control packets generated by the routing protocol to the received data packets.

### 4.2 Experimental Results

In the experiments, firstly 14 networks with varying network topologies are executed without no attacker. Then, different attack types are applied to the same topologies with different ratio of attackers. Firstly, the effects of sinkhole attack is given in Table 2 and Fig. 3. Table 2 shows the average values of performance metrics on networks with different attack ratios. Figure 3 emphasizes on PDR by using the box plot representation. As defined above, the attacker does not drop data packets deliberately in this attack scenario. However, due to the attacker of building inactive routes, the data packets might not be reached to the destination as shown in the results. The attacker might not be even in a route between the source and the destination.

**Table 1.** Simulation parameters used in Ns-3

| Parameter | Value |
|---|---|
| Routing protocol | AODV |
| MAC protocol | IEEE 802.11n |
| Frequency band | 5 GHz |
| Simulation time | 900 s |
| Area | 1700 m × 1700 m × 1500 m |
| Number of nodes | 25 |
| Node speed | 720 km/h |
| Transmission range | 250 m |
| Traffic type | UDP |
| Packet size | 1024 bytes |
| Packet count | 15 |
| Bandwidth | 6 Mbps |
| Ratio of malicious node | No attack, 5%, 10%, 15%, 20% |
| Mobility model | GM model |
| Bounds for GM | X: [−70; 70], Y: [−70; 70], Z: [0; 70] |
| $\alpha$ for GM | [0.495–0.509] |

**Table 2.** Average performance metrics of networks under sinkhole attack

| Attackers (%) | PDR (%) | E2E delay (s) | Overhead |
|---|---|---|---|
| 0% | 91,43 | 0,0253 | 12,5 |
| 5% | 84,94 | 0,031 | 6,98 |
| 10% | 84,01 | 0,036 | 11,04 |
| 15% | 70,11 | 0,018 | 42,16 |
| 20% | 56,60 | 0,017 | 111,14 |

The effect of dropping attack is given in Table 3 and Fig. 4. Even though the attacker positions are selected randomly, the same set of attackers are used in each topology for different attack scenarios. Therefore, the same data packets pass through attackers in each attack scenario. In addition, more data packets could be directed to the malicious node in sinkhole attack. Please also note that the attacker size is increased by covering already existing attacker nodes on networks with less number of attackers for each topology. As shown in the results, as the number of attacker increases, its effect becomes more evident in the network.

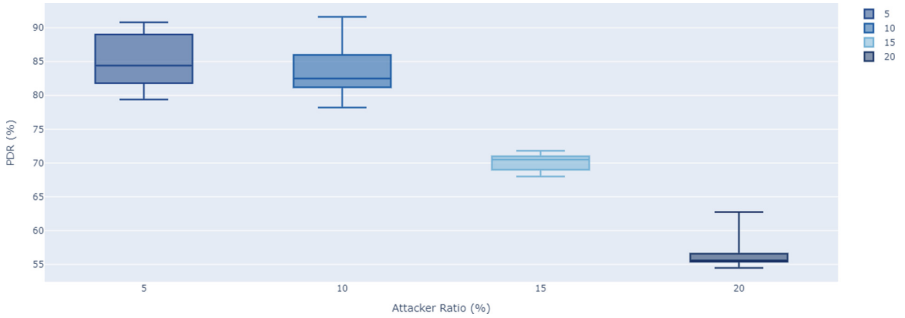


**Fig. 3.** PDR of networks under sinkhole attack

**Table 3.** Average performance metrics of networks under dropping attack

| Attackers (%) | PDR (%) | E2E delay (s) | Overhead |
|---|---|---|---|
| 0% | 91,43 | 0,0253 | 12,29 |
| 5% | 88,47 | 0,024 | 5,61 |
| 10% | 81,84 | 0,036 | 11,87 |
| 15% | 70,14 | 0,023 | 42,17 |
| 20% | 56,72 | 0,018 | 110,02 |

Table 4 shows the average of performance metrics on simulated networks under blackchole attack. In order to see PDR more closely, Fig. 5 shows the box plot for this performance metric. As shown in the results, the network is affected worse as the number of attackers increases. Especially when the attacker ratio reaches to 15%, PDR decreases down to approximately 70%. When the attacker rate is 20%, PDR reaches to an unacceptable level. However such attacks are not very effective on networks having a lower density of attackers due to high mobility. Since all the attacks analyzed so far causes data packets to drop, and hence the route discovery mechanism is re-initiated, the number of routing control packets on networks increases with the number of attackers.

Blackhole attack reduces PDR slightly more than sinkhole attack on networks where more than 5% of nodes are attackers. Even though both attacks take control of the route to the destination node, in some cases the attackers could be in a route between the source and the destination nodes. In such cases only, data packets are forwarded in sinkhole attacks, which explains the small differences between PDR of networks under sinkhole and blackhole attacks.

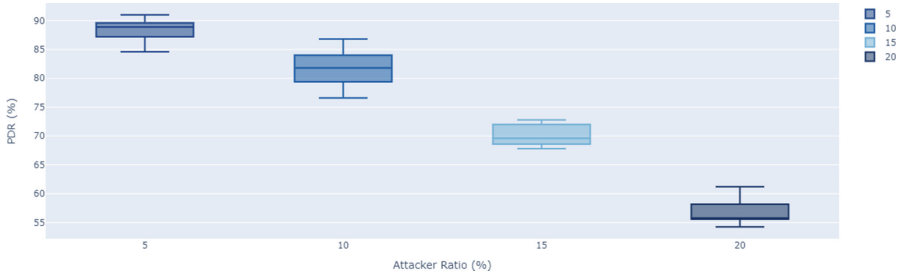


**Fig. 4.** PDR of networks under dropping attack

**Table 4.** Average performance metrics of networks under blackhole attack

| Attackers (%) | PDR (%) | E2E delay (s) | Overhead |
|---|---|---|---|
| 0% | 91,43 | 0,0253 | 6,64 |
| 5% | 88,04 | 0,0254 | 5,91 |
| 10% | 82,53 | 0,0334 | 11,68 |
| 15% | 69,34 | 0,0191 | 43,58 |
| 20% | 56,81 | 0,0170 | 72,77 |

Finally, a DoS attack type is analyzed. The performance results of networks under ad hoc flooding attacks is given in Table 5 and Fig. 6. As expected, the overhead increases considerably. The high number of routing control messages also cause data packets to drop due to network congestion.

The effects of attacks are compared with each other by using PDR, E2E delay, and overhead in Figs. 7, 8, 9 respectively. As shown in Fig. 7, even though blackhole attack is a combination of sinkhole and dropping attacks, the difference between the effects of those attacks is not very notable, not as much as being expected. Hence, the attackers could decrease PDR considerably even by only performing the simplest attack in these small networks, dropping, so it does not need even need to attract the traffic through itself. This may be due to other factors analyzed in depth in the ongoing study. On the other hand, ad hoc flooding attack causes more packets to drop than dropping attacks due to congestion it has created in the network. Even in the presence of one attacker (5%), ad hoc flooding attack shows a considerable decrease in PDR.

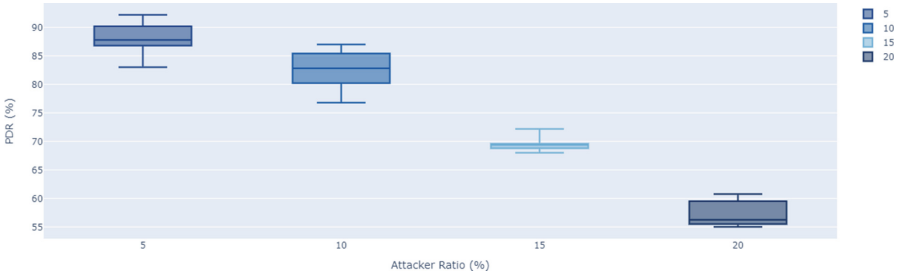


**Fig. 5.** PDR of networks under blackHole attack

**Table 5.** Average performance metrics of networks under ad hoc flooding attack

| Attackers (%) | PDR (%) | E2E delay (s) | Overhead |
|---|---|---|---|
| 0% | 91,43 | 0,0253 | 12,29 |
| 5% | 76,53 | 0,065 | 5,59 |
| 10% | 76,46 | 0,063 | 5,00 |
| 15% | 69,30 | 0,028 | 40,66 |
| 20% | 57,01 | 0,018 | 107,76 |

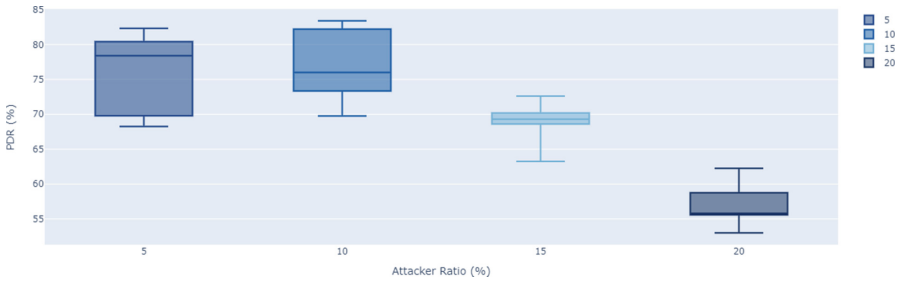


**Fig. 6.** PDR of networks under ad hoc flooding attack

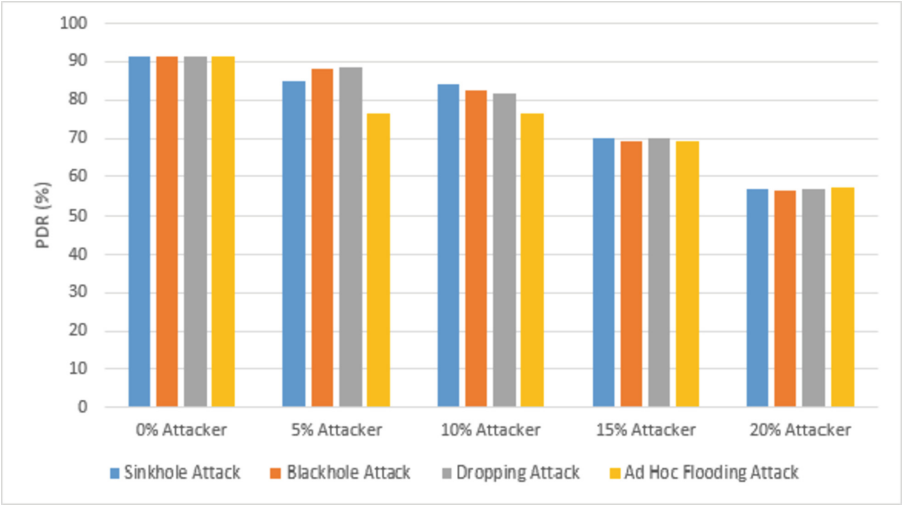


**Fig. 7.** Comparison of PDR on networks under different attack types

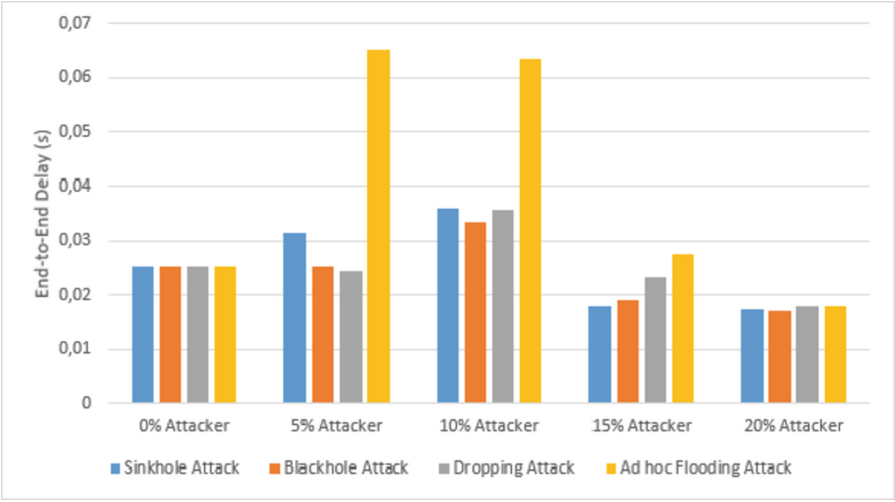


**Fig. 8.** Comparison of E2E delay on networks under different attack types

As shown in Fig. 8, E2E delay increases until the density of attackers reaches to 10% of nodes. Since the network resources are still available until this point, packet delay increases proportionally to the increase in the number of attackers. However, as the number of attackers in the network continues to increase, the overhead also increases considerably due to re-initiating of the route discovery mechanism as shown in Fig. 9. This increase is very dramatic for ad hoc flooding attacks as expected. Because of the overhead, and so the network congestion,

packets have started to be dropped. Moreover, since data packets in shorter routes have higher chance to be forwarded than data packets in longer routes, this might still affect the E2E delay positively on networks under high number of attackers.

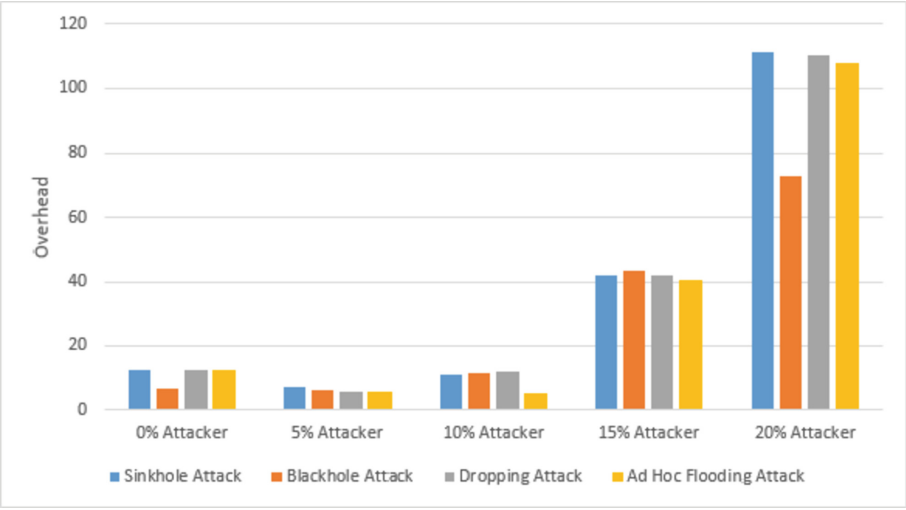


**Fig. 9.** Comparison of overhead on networks under different attack types

## 5 Conclusion

This paper analyzes how various attacks against FANETs affect network performance. Particularly routing attacks targeting AODV, namely sinkhole, dropping, blackhole and ad hoc flooding attacks are taken into consideration. The experimental results show that all attacks degrade the performance of the network, especially when the ratio of attackers has exceed 15%. When the density of attackers below that, the network can still run smoothly. In such cases, the effects of such attacks might be limited due to high mobility. Furthermore, it is shown sinkhole, dropping and blackhole attacks affect the network in a similar way when the attackers are placed in the same positions. Hence, the attackers could decrease the PDR by performing the simplest attack, dropping, so it does not need even need to attract the traffic through itself in small networks. Only ad hoc flooding attack could results in a sharper decrease in PDR even in the existence of one attacker (5%) due to its very nature.

To the best of the authors' knowledge, this is the first attack analysis on FANETs with realistic simulation parameters. The studies in the literature still use the 2D mobility models. Hence, it is believed that this study could accelerate studies on FANETs security. Researchers could use the network parameters here

in order to simulate attacks that could really affect FANETs, so they could propose solutions for mitigating/detecting such attacks. In the future, more complex attack scenarios in larger networks are planned to be analyzed.

## References


1. Abraham, S., Meylan, A., Nanda, S.: 802.11n MAC design and system performance. In: IEEE International Conference on Communications, vol. 5, pp. 2957–2961. IEEE (2005). https://doi.org/10.1109/icc.2005.1494932
2. Akram, R.N., et al.: Security, privacy and safety evaluation of dynamic and static fleets of drones. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), pp. 1–12 (2017). https://doi.org/10.1109/DASC.2017.8101984
3. Altawy, R., Youssef, A.M.: Security, privacy, and safety aspects of civilian drones: a survey. ACM Trans. Cyber-Phys. Syst. **1**(2), 1–25 (2016). https://doi.org/10.1145/3001836
4. Bekmezci, I., Sahingoz, O.K., Temel, S.: Flying AD-HOC networks (FANETS): a survey. AD Hoc Networks **11**(3), 1254–1270 (2013). https://doi.org/10.1016/j.adhoc.2012.12.004
5. Bekmezci, I., Şentürk, E., Türker, T.: Security issues in flying AD-HOC networks (FANETS). J. Aero. Space Technol. **9**(2), 13–21 (2016). http://jast.hezarfen.msu.edu.tr/index.php/JAST/article/view/32
6. Bhatia, V., Walia, E., Singla, P.: VANET and FANET under the impact of the security attack. Int. J. Innov. Technol. Explor. Eng. **8**(9), 390–397 (2019). https://doi.org/10.35940/ijitee.I1062.0789S19
7. Broyles, D., Jabbar, A., Sterbenz, J.P.: Design and analysis of a 3-D gauss-markov mobility model for highly dynamic airborne networks. In: Proceedings of the International Telemetering Conference, p. 46 January 2010
8. Condomines, J.P., Zhang, R., Larrieu, N.: Network intrusion detection system for UAV AD-HOC communication: from methodology design to real test validation. Ad Hoc Networks **90**, 101759 (2019). https://doi.org/10.1016/j.adhoc.2018.09.004
9. Dokurer, S., Erten, Y.M., Acar, C.E.: Performance analysis of ad-hoc networks under black hole attacks. In: Conference Proceedings of IEEE SOUTHEASTCON, pp. 148–153 (2007). https://doi.org/10.1109/SECON.2007.342872
10. El-Semary, A.M., Diab, H.: BP-AODV: blackhole protected AODV routing protocol for MANETs based on chaotic map. IEEE Access **7**, 95197–95211 (2019). https://doi.org/10.1109/ACCESS.2019.2928804
11. Jain, A.K., Tokekar, V.: Mitigating the effects of Black hole attacks on AODV routing protocol in mobile AD Hoc networks. In: 2015 International Conference on Pervasive Computing ICPC 2015 (2015). https://doi.org/10.1109/PERVASIVE.2015.7087174
12. Ladosz, P., Oh, H., Chen, W.H.: Optimal positioning of communication relay unmanned aerial vehicles in urban environments. In: 2016 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1140–1147 (2016). https://doi.org/10.1109/ICUAS.2016.7502562
13. Mahmud, I., Cho, Y.Z.: Adaptive hello interval in FANET routing protocols for green UAVs. IEEE Access **7**, 63004–63015 (2019). https://doi.org/10.1109/ACCESS.2019.2917075
14. Maxa, J.a., Mahmoud, M.s.B., Larrieu, N.: Extended Verification of Secure UAANET Routing Protocol To cite this version : HAL Id : hal-01365933 Extended Verification of Secure UAANET Routing Protocol (2016)

15. Ning, P., Sun, K.: How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Ad Hoc Networks **3**(6), 795–819 (2005)
16. The ns-3 network simulator (2021). http://www.nsnam.org/
17. Ochola, E.O., Mejaele, L.F., Eloff, M.M., Van Der Poll, J.A.: Manet reactive routing protocols node mobility variation effect in analysing the impact of black hole attack. SAIEE Africa Res. J. **108**(2), 80–92 (2017). https://doi.org/10.23919/saiee.2017.8531629
18. Perkings, C., Belding-Royer, E., Das, S.: Ad hoc On-Demand Distance Vector (AODV) Routing. Ietf Rfc 3561 (2003)
19. Praveen, K.S., Gururaj, H.L., Ramesh, B.: Comparative analysis of black hole attack in Ad Hoc network using AODV and OLSR Protocols. Proc. Comput. Sci. **85**, 325–330 (2016). https://doi.org/10.1016/j.procs.2016.05.240
20. Sahingoz, O.K.: Networking models in flying AD-HOC networks (FANETS): concepts and challenges. J. Intell. Robot. Syst. **74**(1), 513–527 (2014). https://doi.org/10.1007/s10846-013-9959-7
21. Sen, J., Koilakonda, S., Ukil, A.: A mechanism for detection of cooperative black hole attack in mobile AD Hoc networks. In: Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011, pp. 338–343 (2011). https://doi.org/10.1109/ISMS.2011.58
22. Shumeye Lakew, D., Sa'Ad, U., Dao, N.N., Na, W., Cho, S.: Routing in flying Ad Hoc networks: a comprehensive survey. IEEE Commun. Surv. Tutorials **22**(2), 1071–1120 (2020). https://doi.org/10.1109/COMST.2020.2982452
23. Tan, X., Zuo, Z., Su, S., Guo, X., Sun, X.: Research of security routing protocol for UAV communication network based on AODV. Electronics **9**(8), 1–18 (2020). https://doi.org/10.3390/electronics9081185
24. Walia, E., Bhatia, V., Kaur, G.: Detection of malicious nodes in flying Ad-HOC networks (FANET). Int. J. Electron. Commun. Eng. **5**(9), 6–12 (2018). https://doi.org/10.14445/23488549/ijece-v5i9p102
25. Xu, Z., Huo, J., Wang, Y., Yuan, J., Shan, X., Feng, Z.: Analyzing two connectivities in UAV-ground mobile AD HOC networks. In: 2011 IEEE International Conference on Computer Science and Automation Engineering, vol. 2, pp. 158–162 (2011). https://doi.org/10.1109/CSAE.2011.5952445