Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution

Hichem Sedjelmaci, Sidi-Mohamed Senouci

Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution

Hichem Sedjelmaci[1], Sidi Mohamed Senouci[2]

Abstract Aerial vehicle networks (AVNs) compose a large number of heterogeneous aerial nodes, such as unmanned aerial vehicles, aircrafts and helicopters. The main characteristics of these networks are the high mobility of aerial nodes and the dynamic network topology. AVNs represent attractive targets for attackers due to the fact that aerial nodes could be connected to an untrusted network and hence lead the attackers to launch lethal threats, e.g., aircraft crash. Therefore, the security of AVNs is mandatory. In this article, we examine the challenges of cyber detection methods to secure AVNs and review exiting security schemes proposed in the current literature. Furthermore, we propose a security framework to protect an aircraft (SFA) against malicious behaviors that target aircrafts communication systems. Numerical results show that SFA achieves a high accuracy detection and prediction rates as compared to the current intrusion detection for aircrafts communication system.

Keywords Aerial vehicle networks · Intrusion monitoring · Intrusion prevention and detection · Attacks

1 Introduction

Aerial vehicles network (AVN) can be any aerial vehicles that communicate together such as an UAV to UAV (U2U), aircraft to aircraft (A2A), and UAV to aircraft (U2A)

✉ Hichem Sedjelmaci
hichem.sedjelmaci@irt-systemx.fr

Sidi Mohamed Senouci
Sidi-Mohammed.Senouci@u-bourgogne.fr

1 IRT SystemX, 8 avenue de la Vauve, 91120 Palaiseau, France

2 DRIVE EA1859, Univ. Bourgogne Franche Comt, Besançon, France

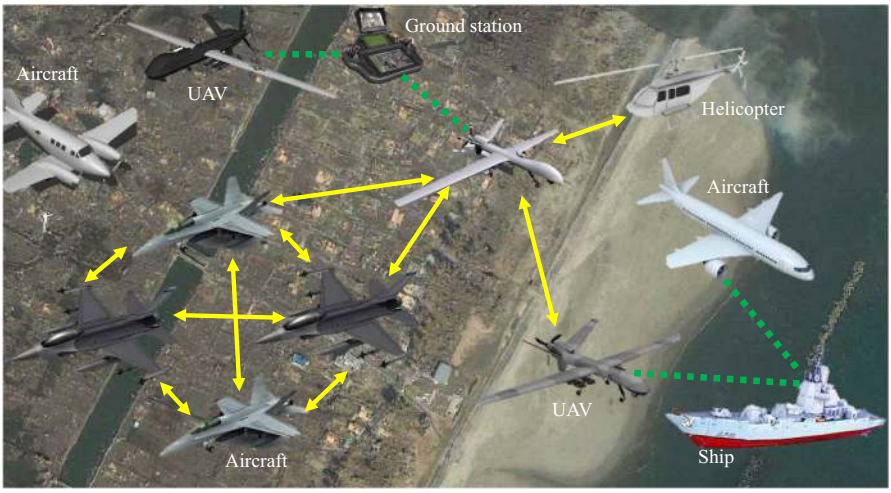

Fig. 1 Synoptic scheme for aerial vehicle network (AVN)

or with static infrastructure like an aircraft to traffic control tower (A2T) and UAV to ground station (U2G), as shown in Fig. 1. Due to the sensitive information that aerial vehicles handle, AVNs are subject to a variety of cyber-threats. In [1], the authors present a number of cyber-threats that target the air traffic communication systems. They analyze the impact of attacks in the cyber-aviation context based on their resources, expertise and motivation. In the taxonomy, they classify cyber-threats into five classes: passive attacker, hobbyist hacker, cyber menace, cyber terrorism and cyber state. For more details on the definitions of these threats, we refer the readers to [1]. According to [2], the main factors that motivate a group of attackers to hack the air traffic communication systems are the high number of wireless systems and the wide variety of sensitive data. For example, more than a dozen of wireless systems are used by the aircraft and traffic control tower during the aircraft takeoff and landing [2]. Therefore, panoply of systems could be targeted by the attackers. The aircraft information is available and easily accessible through the plane-spotting websites and forums. This leads the attacker to track the target aircraft and launch lethal attacks when he is within its radio range. No defense-in depth approaches are discussed in [1,2] to secure the AVN against malicious threats. While in [3], a lightweight cryptography mechanism to resist against a denial-of-service (DoS) attack in civilian UAV is proposed. This mechanism aims to ensure communication privacy and UAV identity and hence prevent the external attack to hack the communication system. However, this cryptography mechanism cannot prevent the internal attackers, i.e., attackers that are aware of the cryptography keys. Hence, attackers could hack the communication system without being detected.

Contributions from academic and industrial communities demonstrate the robustness and efficiency of cyber detection methods to secure the wireless network against malicious behaviors (i.e., internal and external threats). These methods are based on intrusion detection system (IDSs) and intrusion prevention systems (IPSs). These sys-

tems rely on a set of detection and prediction techniques to analyze, detect and predict the misbehavior of a monitored node. Based on these insights, some cyber detection frameworks [4–8] are developed and conceived to secure the AVN against lethal attacks. Cyber detection methods could be categorized into two main categories [5,8]: (i) rule-based specification detection, which is based on comparing the behavior of a monitored device against a set of rules specifications, defined by a security expert [9]. Despite the fact that such technique generates a low number of false alarms, a certain number of threats could not be detected specifically when this number increases over time, and (ii) bio-inspired detection, which is based on biological systems like evolutionary biology system such as game theory and genetic algorithms, and bio-inspired artificial intelligence systems such as neural networks (NN) and support vector machine (SVM) [10]. The advantage of this technique consists on its ability to detect almost of threats launched by attackers. However, it is not suitable of low resource devices since it is based on heavy algorithms to model the abnormal cyber-attack patterns. Current intrusion detection and prevention mechanisms are based on these detection techniques to secure mobile ground nodes, Mobile Ad hoc Networks (MANETs) and Vehicular Ad Hoc Networks (VANETs). However, these detection and prevention mechanisms cannot be reused directly to AVN, due to the following requirements:

- *Mobility model* The mobility model in AVN differs from that of ground vehicles since an aerial vehicle cannot change frequently its speed and direction and make sharp turns as mobile ground nodes do [11]. Therefore, IDS (IPS) agents should react promptly when the speed and direction change frequently; as it could be under attack.
- *Cyber-threat* Launching cyber-attacks against an AVN is hard compared to launch them against ground nodes. This is due to the large number of interconnected black-box systems within aerial vehicle (e.g., aircraft). To attain their objectives, hackers need a sophisticated material in order to reach a remote target and hack its system. Recently, scientists from University of Texas [12] have developed a spoofer material to hack a remote UAV. This material aims to jam communication, alter the UAVs GPS coordinates and force the UAV to crash with another UAV or ground station.
- *Hybrid detection (and prevention)* A centralized detection (and prevention) mechanism in AVN is not efficient, owing to sparse communication [4,5]. Thereby, the most appropriate solution is a distributed approach where each aerial vehicle and ground node activate their monitoring process to observe the behavior of their neighbors. Furthermore, making a final decision about a suspected device (i.e., normal node or attacker) based only on a local observation is not accurate. In fact, this decision should be made by a centralized trusted node based on recommendation of the set of suspected devices neighbors.
- *Resource constraints* Some aerial vehicles, such as UAVs, have a constraint in energy, and it is not appropriate to embed heavy detection methods used in VANET in such kind of energy-constraint nodes. Therefore, a dilemma between a high level of security and low energy consumption should be considered for designing intrusion detection and prevention mechanisms.

– *Independency* The IDS and IPS in aerial vehicle should be independent of the embedded systems where they are activated. This is due to the large number of interconnected complex systems. In addition, they should run transparently for the pilot (e.g., drone pilot) without time-consuming overhaul of the embedded systems [2].

Therefore, a new detection and prevention mechanism should be proposed to secure the AVN against the most lethal attacks that target such kind of attractive networks. This new mechanism could be inspired from the ones developed for ground nodes by taking into account the requirements cited above. Furthermore to predict and detect the attackers with high accuracy, we use the hybrid security approach, i.e., the combination between a bio-inspired detection and rule-based specification detection methods. This security approach has the ability to get high attacks detection rate and low false alarms.

In this research work, we present a careful review of different cyber detection schemes in AVN and highlight a couple cyber-attacks that could occur in this network. Additionally, we propose a security framework, SFA to detect and prevent threats occurrence that target aircrafts communication systems.

2 Cyber-attacks and security countermeasures

This section is organized into two sub sections: cyber-attacks that target the AVN and a taxonomy of cyber detection schemes to protect the AVNs, respectively.

2.1 AVN-sophisticated cyber-attacks

The basic security of AVNs includes integrity, availability, authenticity and confidentiality, as explained in [13] for UAVs network. Figure 2 lists a couple of cyber-attacks that could target AVNs:

– *Injection/modification attack* This kind of attacks aims to alter the sensitive information of a legitimate aerial vehicle, by injecting wrong data, modifying the content of transmitted packets or dropping the received ones from aerial vehicle. It is also known as integrity attack [14]. False data injection is a kind of integrity attack where the goal is to affect, for instance, the aircraft in order to transmit false information to traffic control tower. A selective forwarding is another kind of injection/modification attack, in which the malicious device selects most attractive packets and drops them.
– *Denial-of-service (DoS) attack* This attack targets the availability of aerial vehicle by exhausting the network bandwidth, jam the wireless communication or disturb network operation and communication protocol. Jamming attack is one of the most lethal DoS attacks where the goal is to jam the communication between legitimate aerial vehicles or between aerial vehicles and the ground station. As a result, an aerial vehicle crash could easily occur. Spoofing attack is another kind of DoS in which the malicious device spoofs the GPS coordinates of aircraft or UAV leading to a false estimation of aerial vehicle position [12,14].

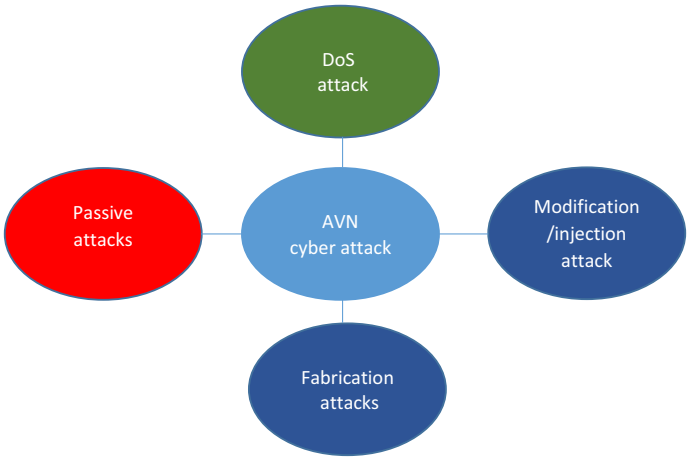

Fig. 2 AVN cyber-attack

– *Fabrication attack* This threat is an attack on authenticity [13], where it gains the privilege to access in the aerial vehicle components to provide a false information. For instance, the intruder replaces aerial vehicles identities by false identities. In this case, the legitimate aerial node receives false packets from the sender. Therefore, the node that sends the packets will be suspected as an attacker, and hence, the false-positive rate (i.e., claiming a normal node as an attacker) will increase in the network.
– *Passive attack* The malicious device overhears the packets that pass through its radio range, investigates the most relevant data and determines the most attractive node, i.e., hot-point (e.g., aircraft or ground station). Afterward, the attacker switches from a passive mode to an active mode in order to launch a cyber-attack, e.g., DoS against this attractive node.

2.2 Cyber detection schemes to secure AVN against lethal attacks: a taxonomy

Here, we review cyber detection schemes proposed in the current literature to secure AVN against attackers. We classify these schemes according to their detection methods, described in the previous section, into two classes.

2.2.1 Rule-based specification detection schemes

Mitchell and Chen [4] proposed an intrusion detection scheme to secure the UAV nodes against malicious threats. This security scheme relies on a set of attacks signatures to detect whether the monitored device is an intruder or not. To ensure a high level of robustness, an update of attacks signatures is required. According to their simulation results, their scheme detects almost of cyber-threats that attack the UAV networks. However, a high number of false alarm could be raised by the IDS agents.

Sedjelmaci et al. [5] aim to address the issues of false positive and false negative generated by the IDS and IPS agents in an UAVs network. In this security scheme, they model the behavior of a suspected device by a threat level (TL) function. This latter is based on a belief approach that aims to define a set of rules specification to classify accurately the monitored device in the following categories: Normal, Suspect or Malicious. According to their simulation, they prove that a belief approach helps on a decrease in the false-positive and false-negative rates. However, an update of rules is required.

In [6], Strohmeier et al. developed a rule-based intrusion detection scheme to protect the communication between aircraft and ground station on the ground. Specifically, the scheme aims to detect false data injection attack. The external cyber-threat injects a wrong data into Automatic Dependent Surveillance-Broadcast (ADS-B) and could lead to a catastrophic scenario, e.g., aircraft crash. ADS-B is an embedded system used by the aircraft for broadcasting sensitive information, such as position, speed, and collision avoidance. The main feature to detect such kind of cyber-threat is signal strength. The authors propose a detection technique to monitor the behavior of signal strength and define a set of detection rules to categorize the monitored devices signal into normal or malicious patterns. According to their simulation results, the authors prove that almost of attackers are detected within 40 seconds.

Kacem et al. [15] proposed an ADS-B intrusion detection framework to secure the aircraft against cyber-attacks that target the ADS-B messages. Their framework is based on a signature detection techniques that analyze the GPS position of an aircraft. In their evaluation, they analyze the sending and receiving time of ADS-B messages, when cyber-attacks are occurring. According to their experiment results, they claim that even when attacks are occurring their approach requires a low overhead and a negligible jitter. However, the authors did not evaluate their performance of ADS-B detection framework in terms of security metrics, such as attacks detection rate.

2.2.2 Bio-inspired detection schemes

Casals et al. [7] developed a bio-inspired detection scheme to detect cyber-attacks that target airborne networks. The bio-inspired technique is based on a machine learning algorithm. The authors choose to use SVM algorithm for the learning and classification process. This choice lies in the fact that SVM is a lightweight algorithm and does not require a high computational complexity as compared to NN. The authors do not provide any simulation or experimental results to analyze the performance of their detection scheme.

Sedjelmaci et al. [8] aimed to secure the UAV-aided VANET against malicious threats. The main contribution of their work is summarized as follows: (i) How an IDS activates optimally the monitoring process to detect the malicious node in order to ensure a dilemma between a high detection rate and low energy consumption. (ii) When the IDS agents should eject the suspected device from the network to ensure a trade-off between the detection and false-positive rates. The performance of their detection scheme is analyzed through simulation and the obtained results were satisfying.

Rani et al. [16] proposed an anomaly detection scheme based on a learning algorithm to protect UAV nodes against a network attacks such as a distributed denial-of-service

(DDoS) attacks. The authors described how to use NN and fuzzy learning algorithms to detect accurately such kind of cyber-threats. However, they did not detail the monitoring and detection process carried out by the IDS agents. In addition to that, the authors did not evaluate the detection efficiency of their security scheme.

Sedjelmaci et al. [14] proposed an intrusion detection and response framework (IDRF) to secure the UAVs network against the attacks that target data integrity and network availability. As far as we know, this is the only framework that developed a hybrid detection technique (i.e., combine between rule-based detection and anomaly detection techniques) for UAVs network, while taken into account the energy constraints of UAV node. According to simulation results, they prove that their framework exhibits a high attack detection rate and low false- positive rate. In addition its requires a low communication overhead to respond promptly against detected attack.

2.2.3 Discussion

Table 1 highlights a taxonomy of current cyber detection schemes developed to protect the AVN against malicious threats. The anomaly detection techniques based on machine learning (artificial intelligence system or game theory concept) are robust against cyber-threats and scalable. However, according to security experts, these techniques tend to yield a certain number of false positives. Furthermore, machine learning is not suitable to be executed in low resource device such civilian drone, since it requires a high computational complexity to detect malicious threats. In other side, a rule-based detection is a lightweight technique used to reduce the number of false positives. However, this technique is not robust, specifically when the behavior of cyber-threat varies over time, i.e., launches a set of misbehavior patterns. In order to handle both issues, robustness and false positives, it is imperative to combine between a machine learning detection and rule-based specification detection methods. Moreover, in order to address the computation complexity issue, machine learning should be executed in a powerful node, e.g., aircraft or mobile ground station.

Table 1 Comparison between cyber detection schemes for AVN

Security schemes	Detection techniques	Robustness	Complexity
[4]	Rule-based detection	Medium	Medium
[5]	Rule-based belief approach detection	Medium	Medium
[6]	Rule-based detection	Medium	Low
[15]	Rule-based detection	Medium	Low
[7]	Anomaly detection based on SVM	Medium	Medium
[8]	Anomaly detection based on game theory	High	High
[14]	Rule-based detection and anomaly detection based on SVM	High	Low
[16]	Anomaly detection based on NN and fuzzy learning	High	High

3 A case study on cyber-attacks targeting aircrafts communication system with security countermeasures

This study concerns the security against attackers targeting the communication between the aircraft and its ecosystem of Internet of Things (IoT), such as UAV, ground vehicles and air traffic control. The aircraft is equipped with communication systems to communicate with IoT objects; we cite Aircraft Communications Addressing and Reporting System (ACARS) and ADS-B. ACARS could be used to exchange messages between aircraft and ground node (e.g., vehicle and air traffic control) via radio or satellite. Such kind of messages could contain the following sensitive information: amount of fuel, crew and weather information, flight origin and destination. ADS-B system broadcasts critical information, such as position, heading, and velocity to air traffic control or/and other aircraft for collision avoidance purpose. Due to the sensitive information handled by both ACARS and ADS-B systems, the aircraft communication systems are an attractive target for the attackers [17]. Here, the hacker targets the aircraft during its takeoff and landing since it is easier to reach the aircraft by using, for instance, a spoofer material. Some attack scenarios that target these communication systems are summarized as follows:

- The attacker eavesdrops the messages exchanged between aircraft and air traffic control (since the messages that ACARS delivers and receives are unencrypted) and hence leads the attacker to know what is in the air and when. In this case, the attacker chooses an appropriate time to jam the communication and could create wrong environment information with the false information injection to the air traffic control [17], e.g., provide a false aircrafts position.
- With the help of ADS-B and GPS components, the aircraft can locate all objects within its area. Here, the attacker can hack the aircrafts GPS; by spoofing its coordinates [18,19]. This will lead to a false estimate of the aircraft position. In addition, the attacker could attack every IoT device which is located in the proximity of the aircraft and spoof their GPS signals simultaneously.

3.1 Security architecture

Figure 3 illustrates the aircraft security framework, SFA that aims to monitor, detect and prevent cyber-attacks that target ACARS and ADS-B communication systems, where the pseudocode of attacks detection and prediction is illustrated in Algorithm 1. SFA is embedded in an aircrafts communication system and is composed of three modules:

- *Intrusion monitoring and modeling (IMM)* This module monitors the behavior of a target device by collecting a set of features related to the attacks that the framework aims to detect. For instance, the signal strength is one of the jamming attacks feature [2] that is monitored to detect the cyber-threat that jams communication between aircraft and air traffic control. Table 2 highlights some features related to cyber- threats that could target the aircraft communication systems [2,4,14]. In order to detect the attacks with a high accuracy, other features could be added

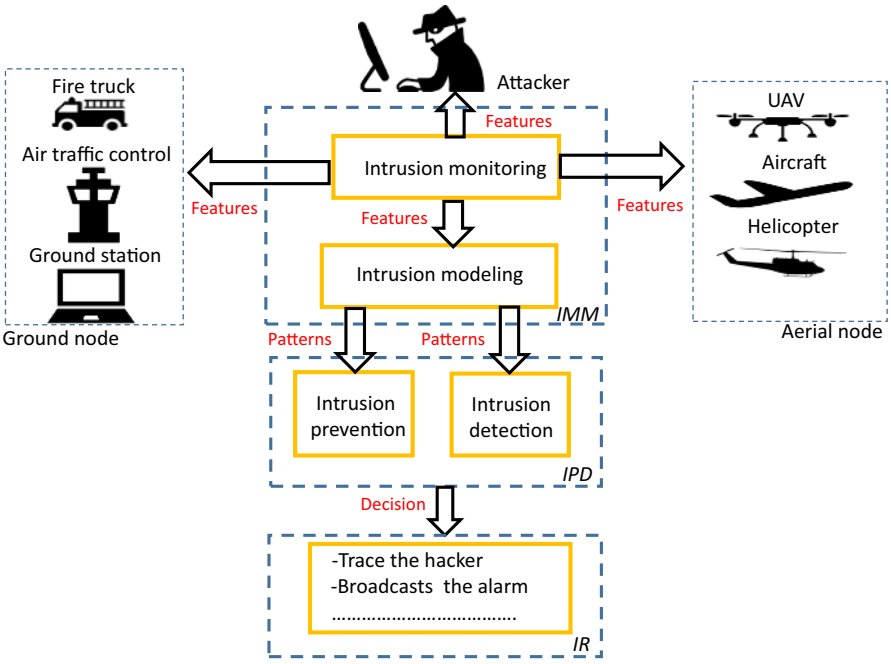

Fig. 3 SFA

Table 2 Cyber-threats features

Cyber-threats	Features
Wormhole and Black hole	Data injection rate
Jamming	Signal strength intensity
Resource exhaustion	Number of requests
Man-in-the-middle	Messages modified rate and signal strength intensity
False information injection	Messages modified rate
GPS spoofing	Signal strength intensity

in addition to those of Table 2. Machine learning algorithm based on NN is used to detect unknown malicious behavior [20]. The NN algorithm relies on a training and classification process to model the malicious behaviors of threats. In the training phase, SFA collects the features from trusted IoT devices that communicate with aircraft such as vehicle, UAV and air traffic control, and model normal behaviors of features related to each IoT device. In the classification process, the framework classifies the new incoming features according to the normal patterns, determined during the training phase. In case when a misbehavior is detected it will be stored and used by intrusion detection module for further detection. This process is updated over time and depends on the panoply of misbehaviors that cyber-threats could launch.

– *Intrusion prevention and detection (IPD)* This module aims to prevent and detect lethal attacks that hack the aircraft communication system. In the prevention system, game theory approach is used to predict the future misbehavior of an intruder. Game theory is perceived as a mathematic tool to analyze the interactions among multiple players; in our case, the players are SFA and attackers. Each player has a set of strategies and chooses the best strategy to achieve its own goals. The equilibrium defined as a Nash equilibrium (NE) solution is reached when the players do not change their strategy, i.e., the hackers attack the communication system and SFA monitors the suspected IoT device [21]. Our security game is modeled as $\mu(S, Q)$ and $\mu^{'}(S^{'}, Q^{'})$. The strategies of SFA and attackers can be defined, respectively, as: $S_j = \{S_i; \forall \text{ i} \in (1 \triangleq \text{monitor}, 2 \triangleq \text{does not monitor})\}$ and $S^{'}_j = \{S^{'}_i; \forall \text{ i} \in (1 \triangleq \text{hack}, 2 \triangleq \text{does not hack})\}$. $Q\{S_i\}$ and $Q^{'}\{S^{'}_i\}$ are the utility functions of SFA and attackers, respectively; which increase and decrease, depend on the strategies carried out by the players. The goal of this distributed game is to predict the future misbehavior of a hacker and detects it. The intrusion detection system is based on a rule-based detection technique to identify the attackers. This technique relies on a set of signatures (i.e., patterns) to verify whether the behavior of a suspected IoT device matches one of the attacker signatures. In case when a match occurs, the intrusion reaction module is launched. The attacker signatures related to each attack behavior are defined by the machine learning algorithm as explained in the intrusion modeling module. It is noted that the future misbehavior that is detected by the game theory system is also compared with attack patterns (determined by machine learning algorithm) before the decision making, i.e., categorizes the node as an attacker or legitimate node. By combing between a rule-based specification detection and machine learning detection techniques, a high level of cyber security could be ensured, i.e., high detection and low false-positive rates [4,9].
– *Intrusion reaction (IR)* This module proposes different services airport to react smartly and promptly against a hacker or a group of hackers. These services could be, for instance, trace the hacker and broadcasts the alarm to the security staff in the airport.

Algorithm 1: *Attack detection and prediction*

```
1   Begin
2     Monitor the device T_i
3     Extract the features F_j
4     if(F_j !=0) then
5       Model the detected misbehavior with attack's
        signatures S_k
6       if(S_k !=0) then
7         IPD module is launched
8           if (attack detection == True && attack prediction
          == True )
9             IR is activated
            Else
              Compute the new F_j
10  End
```

4 Experiment and security analysis of SFA

In this section, we evaluate the performance of SFA using NS (Network Simulator)-3 simulator [22] by analyzing the accuracy detection and prediction rates. Afterward, we provide a security analysis against cyber-attacks that could target the aircrafts communication systems.

4.1 Simulation results

In this section, we analyze the security performance of SFA under the two attack scenarios (described in Sect. 3). These attacks are categorized into denial of service (DoS) and false information injection attacks. The main purpose of these attacks is to target the communication systems of an aircraft by injecting wrong information, jamming the communication and altering the aircrafts GPS coordinates. In our simulation, we use NS 3 simulator [22], which could be used as a simulator for large-scale airborne network as explained in [23]. The aircraft which is defined as a node in the simulator communicates with a set of heterogeneous ground nodes (e.g., vehicles), where the mobility model of an aircraft is defined by its position, velocity and flight plan information (departure, destination and trajectory) [23]. In the simulations, we vary the number of ground nodes from 100 to 400 nodes, where the number of aircraft varies from 10 to 30% of overall ground nodes and the number of attackers varies from 5 to 20% of overall aircraft nodes. Specifically, we compute the following security metrics: (i) Accuracy detection rate is the expected detection rate—false-positive rate. (ii) Accuracy prediction rate is the attacks prediction rate—false prediction rate. The detection and prediction rates are, respectively, the number of detected and predicted DoS and false information injection attacks over the total number of attackers. False positive is the percentage of legitimate ground nodes that are categorized as an attacker. False prediction is the percentage of a future honest nodes that are categorized as future attackers. We compare the performance of SFV with IDS frameworks developed for aircraft and UAVs, ADS-IDS [15] and IDRF [14], respectively. As indicated in the related work section, ADS-IDS framework relies on a signature-based detection technique to detect a false information injection attacks such as GPS spoofing. Note that ADS-IDS does not have the capability to detect DoS attacks. Thereby, we add to this framework the DoS features (described in Table 2) into its signature-based detection technique to enable it to detect such attacks. In the simulation, we inject the same number of DoS and false information injection attacks against the communication between the aircraft and ground node (A2G). We assume that the attackers target the A2Gs communication only during the takeoff and landing of an aircraft since it is easier for a hacker to reach its target. The main simulation attributes are summarized in Table 3.

The most important results are summarized below.

4.1.1 Accuracy detection rate

As illustrated in Figs. 4 and 5, we inject separately the DoS and false information injection attacks and analyze the security performance of SFV, ADS-IDS [15] and

Table 3 Simulation attributes

Attribute	Value(s)
Scenario time	15 min
Ground nodes#	[100, 400]
Aircraft#	10, 15, 25 and 30% of overall ground nodes
Link data rate of A2G	15 Gbps
UDP flow rate of A2G	1 Mbps
Packet size	512 bytes
Aircrafts velocity during its takeoff	120 km/h
Aircrafts velocity during its landing	250 km/h
Attackers#	5 and 20% of overall aircraft nodes
Radio range of attackers	25 km

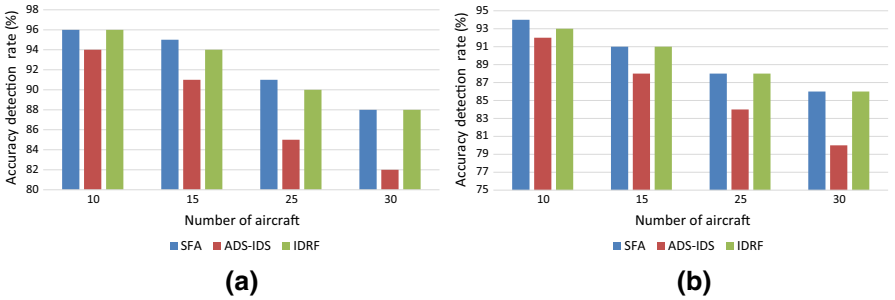

Fig. 4 Accuracy detection rate under DoS attacks. **a** Number of attackers is equal to 5% of overall aircraft. **b** Number of attackers is equal to 20% of overall aircraft

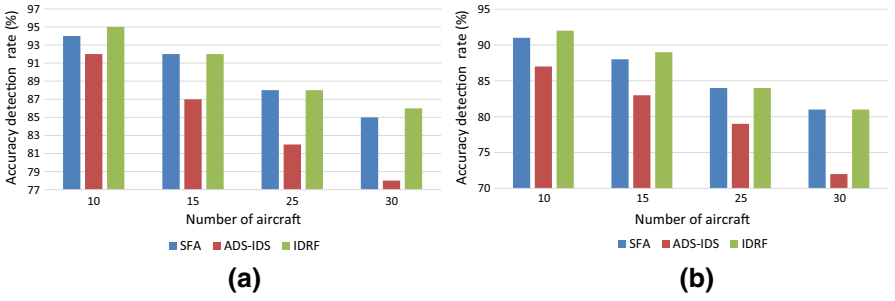

Fig. 5 Accuracy detection rate under false information injection attacks. **a** Number of attackers is equal to 5% of overall aircraft. **b** Number of attackers is equal to 20% of overall aircraft

IDRF [14] frameworks by computing the expected detection and false-positive rates. As shown in Fig. 5, it is apparent that it is difficult for these cyber security frameworks to detect false information injection attacks, since the main purpose of a group of hackers when it executed such misbehavior (e.g., spoofing attack) is to cause an attack

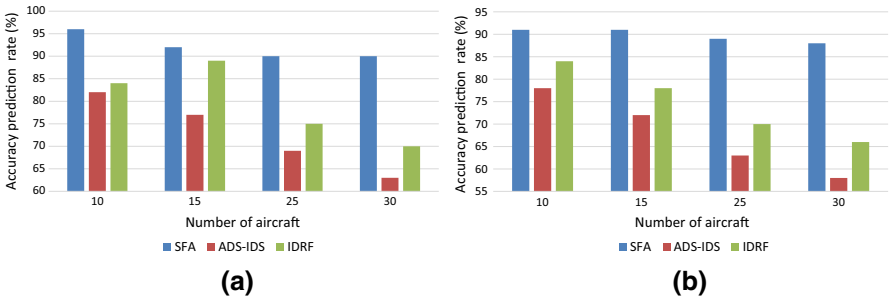

Fig. 6 Accuracy prediction rate under DoS attacks. **a** Number of attackers equal to 5% of overall aircraft. **b** Number of attackers equal to 20% of overall aircraft

without raising any alarms on the targeted aircrafts component [24]. Furthermore, the hacker can choose judiciously the right time and target component to launch remotely their malicious software. As shown in Figs. 4 and 5, we analyze two scenarios, the number of attackers equal to 5 and 20% of overall aircraft nodes. We found out that SFV and IDRF outperform ADS-IDS in terms of expected detection and false-positive rates, since they have the capability to prevent accurately the execution of DoS and false information injection attacks. In worst case, i.e., when the number of attackers is equal to 20%, the accuracy detection rate of SFV when DoS and false information injection attacks occur is almost equal, respectively, to 80 and 72%, as shown in Figs. 4b and 5b. Hence, the excellent performance of SFV framework is achieved due to an efficient collaboration between intrusion monitoring and modeling module and intrusion detection module. These modules model the current misbehavior of an intrusion and use a rule-based specification detection to detect the intrusion that executes an attack.

4.1.2 Accuracy prediction rate

From Figs. 6 and 7, it is apparent that ADS-IDS and IDRF cannot predict efficiently the future attacks. This is due to the fact that there is no intrusion prevention mechanism in these IDS frameworks. From Figs. 6b and 7b, the false prediction rate of SFV increases and has a negative impact on the prediction of a future attack. This increase is due to the communication noise within aircrafts range, which degrades the reliability of monitoring the behavior of a suspected node. Despite the number of false prediction alerts that generated by SFV, it has the capability to predict the future expected attacks behavior with a high accuracy. However, in worst case the accuracy prediction rate of SFV when DoS and false information injection attacks occur is almost equal to 88 and 85%, respectively, as shown in Figs. 6b and 7b. This result is achieved due to an efficient combination between an attack modeling and intrusion prevention modules. The attack modeling aims to define the main distinguish features related to DoS and false information injection attacks, and intrusion prevention module uses a mathematic tool, game theory [25] to predict the future attacks behavior.

Before to discuss the security analysis of SFA against cyber-attacks, in the following we discuss how SFA deals with the requirements cited in introduction section:

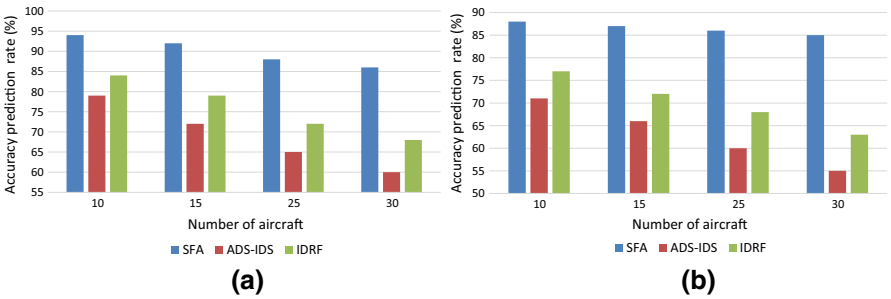

Fig. 7 Accuracy prediction rate under false information injection attacks. **a** Number of attackers equal to 5% of overall aircraft. **b** Number of attackers equal to 20% of overall aircraft

(i) cyber-attacks. SFA relies on a couple of security rules to detect the specific attacks that target the aircraft. For instance, the intrusion monitoring, detection and prevention modules use security rules based on signal strength to detect the GPS spoofing attacks. (ii) Hybrid detection (and prevention). The decision about the suspected IoT node (i.e., normal or attack) is made by a trusted entity, air traffic control. This latter gathers the intrusion alerts from the detection and prevention modules and makes a final decision by broadcasting an alarm to the security staff when the suspected node is qualified as an attacker. (iii) Resource constraints. The ACARS and ADS-B communication systems of an aircraft have not the constraints of energy; this is unlike the ADS-B communication system used by the civilian UAV as explained in [4,14]. Thereby, the proposed SFA could be embedded in these communication systems without degrading their performances. (iv) Independency. SFA is flexible and its modules is independent of the communication systems where they are activated. (v) Mobility model: The aircraft cannot change frequently its speed and direction as vehicle do [11]. The detection and prevention modules report an alert to air traffic control when the speed and direction change frequently.

4.2 Security analysis

We analyze our aircraft security framework to prove that the aircraft is secured against the following attacks: Jamming, GPS spoofing, injection/modification, sybil, wormhole, black hole and passive attacks.

- *Jamming and GPS spoofing attacks* As explained in Sect. 3, these threats aim, respectively, to jam and alter the communication systems and GPS coordinates of an aircraft. These internal attacks could not be prevented by the cryptography mechanisms and only the IDS and IPS can identify them. The SFA monitors the feature, signal strength intensity (SSI) related to each suspected IoT device, and launches its intrusion detection and prevention systems to identify the malicious devices that jam and/or alter the communication and aircrafts GPS coordinates, respectively.
- *Injection/modification attack* Cryptography mechanisms are used to authenticate the external node and prevent the malicious device from injecting false messages in

ACARS and ADS-B components. Therefore, we can prevent the injection attack to inject wrong data. However, these mechanisms cannot prevent internal attackers that are aware about the cryptographic keys. To detect them, SFA activates its intrusion detection and prevention systems and analyzes the feature, Messages Modified Rate; related to each suspected IoT device.

- *Fabrication attack* The Sybil attack is the most dangerous attack that fabricates a set of identities with providing false positions, when it communicates with legitimate aerial node. To identify the Sybil device, a position verification algorithm could be used, such as the one used in [14] to identify the GPS spoofing attack. This algorithm is based on a hybrid detection (rule-based and SVM detection techniques) to monitor the signal strength intensity and detection of a malicious signal.
- *Wormhole and black hole attacks* The main features of these cyber-threats are to drop the relevant data that are exchanged between the aircraft and its ecosystem of IoT objects (e.g., air traffic control) [26]. To prevent the occurrence of these threats, the intrusion prevention and detection module analyzes the number of false data that are injected, and when an anomaly is detected [14] it informs the security staff to localize the source of attack.
- *Passive attack* ACARS and ADS-B messages that are exchanged between the aircraft and its IoT ecosystem (e.g., air traffic control) are unencrypted and the attacker can overhear all the messages that pass through its radio range. Therefore, the use of elliptic curve cryptography (ECC) [27] to ensure the external nodes authentication and the communication privacy is required. The elliptic curve digital signature algorithm (ECDSA) is used to authenticate the IoT node that wants to communicate with the aircraft. Therefore, ECDSA prevents the external threat to launch an attack against the aircraft. To preserve the anonymity, the elliptic curve integrated encryption scheme (ECIES) is used to encrypt the messages that are exchanged between the aircraft and its ecosystem of IoT nodes. Therefore, by using ECIES scheme the passive attack cannot overhears the exchanged messages.

5 Conclusion

Security for aerial network is a challenging issue since cyber-threats that target such kind of network become more sophisticated and could cause a lethal attack, e.g., aircraft crash. In this research work, we focus in reviewing various cyber detection schemes by highlighting their drawbacks and advantages. According to our investigation, we conclude that there is a need to address several weaknesses that the current detection schemes exhibit. These schemes suffer either from a low robustness or/and high complexity. To address these weaknesses, we propose a security framework that could be used to secure an aircraft against malicious threats. Our framework is based on intrusion monitoring and modeling to monitor the behavior of targets IoT devices and models accurately the malicious behaviors. The intrusion detection and prevention systems are used to prevent and detect promptly the malicious intent. The simulation results show that SFV exhibits a high attack prediction and detection rates as compared to the contemporary detection frameworks [14,15]. In addition, we found out

that false information injection threat is the most difficult attack to detect. However, an efficient combination between the attack modeling and intrusion detection (and prevention) modules leads the prevention of this smart attack to occur.

References

1. Strohmeier M, Schfer M, Smith M, Lenders V, Martinovic I (2016) Assessing the impact of aviation security on cyber power. In: 8th IEEE International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, pp 223–241
2. Strohmeier M, Schfer M, Pinheiro R, Lenders V, Martinovic I (2017) On perception and reality in wireless air traffic communication security. IEEE Trans Intell Transp Syst 18(6):1338–1357
3. Sparrow RD, Adekunle AA, Berry RJ, Farnis RJ (2016) A novel block cipher design paradigm for secured communication. In: IEEE Annual Systems Conference (SysCon), Orlando, Florida, USA
4. Mitchell R, Chen IR (2014) Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE Trans Syst Man Cybern Syst 40(5):593–604
5. Sedjelmaci H, Senouci SM, Messous MA (2016) How to detect cyber-attacks in unmanned aerial vehicles network? IEEE Globecom, Washington DC, USA
6. Strohmeier M, Lenders V, Martinovic I (2015) Intrusion detection for airborne communication using PHY-layer information. In: SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), Milan, Italy
7. Casals SG, Owezarski P, Descargues G (2013) Generic and autonomous system for airborne networks cyber-threat detection. IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC), New York, USA, pp 1–14
8. Sedjelmaci H, Senouci SM, Ansari N (2017) Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology. IEEE Trans Intell Transp Syst 18(5):1143–1153
9. Callegari C, Vaton S, Pagano M (2010) A new statistical method for detecting network anomalies in TCP traffic. Trans Emerg Telecommun Technol 21(7):575–585
10. Meisel M, Pappas V, Zhang L (2010) A taxonomy of biologically inspired research in computer networking. Comput Netw 54(6):90116
11. Namuduri K, Wan Y, Gomathisankaran M, Pendse R (2012) Airborne network: a cyber-physical system perspective. In: Proceedings of the First ACM MobiHoc Workshop on Airborne Networks and Communications, South Carolina, USA, pp 55–60
12. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA (2012) Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: Proceedings of the ION GNSS, Meeting Nashville, USA
13. He D, Chan S, Guizani M (2017) Drone-assisted public safety networks: the security aspect. IEEE Commun Mag 55(8):218–223
14. Sedjelmaci H, Senouci SM, Ansari N (2017) A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. IEEE Trans Syst Man Cybern Syst 1–13
15. Kacem T, Wijesekera D, Costa W, Barreto A (2016) An ADS-B intrusion detection system. IEEE TrustCom-BigDataSE-ISPA, Tianjin, China, pp 544–551
16. Rani C, Modares H, Sriram R, Mikulski D, Lewis FL (2016) Security of unmanned aerial vehicle systems against cyber-physical attacks. J Def Model Simul Appl Methodol Technol 13(3):331–342
17. Polstra P (2014) Cyber-hijacking airplanes. DEFCON, Las Vegas, USA
18. He D, Chan S, Guizani M (2017) Communication security of unmanned aerial vehicles. IEEE Wirel Commun Mag 24(4):134–139
19. Shepard DP, Bhatti JA, Humpherys TE (2012) Spoofing attack demonstration on a civilian unmanned aerial vehicle. GPS World Mag 30–33
20. Moon D, Im H, Kim I, Park JH (2015) DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. J Supercomput 73(7):2881–2895
21. Nezarat A, Shams Y (2017) A game theoretic-based distributed detection method for VM-to-hypervisor attacks in cloud environment. J Supercomput 73(10):4407–4427
22. Network simulator (ns-3) (2018). http://www.nsnam.org
23. Newton B, Aikat J, Jeffay K (2014) Simulating large-scale airborne networks with ns-3. ACM Workshop on ns-3, Barcelona, Spain, pp 32–39

24. Chen H, Howard FH (2016) A Kalman filter based method for GPS spoofing detection. In: Proceedings of the 2016 International Technical Meeting of the Institute of Navigation, Monterey, California, pp 151–159
25. Garnaev A, Baykal-Gursoy M, Poor HV (2016) Security games with unknown adversarial strategies. IEEE Trans Cybern 46(10):22912299
26. Maxa JA, Mahmoud MS, Larrieu N (2016) Extended verification of secure UAANET routing protocol. In: 35th IEEE/AIAA Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, pp 1–16
27. Qiu Q, Xiong Q (2004) Research on elliptic curve cryptography. In: IEEE 8th International Conference on Computer Supported Cooperative Work in Design Proceedings, Xiamen, China, pp 698–701