Towards a Multi-Agent based Network Intrusion Detection System for a Fleet of Drones

Said OUIAZZANE[1], Fatimazahra BARRAMOU[2], Malika ADDOU[3]
ASYR Team - LaGeS Laboratory, Hassania School of Public Works
Casablanca, Morocco

***Abstract*—The objective of this research work is to propose a new model of intrusion detection system for a fleet of UAVs deployed with an ad hoc communication architecture. The security of a drone fleet is rarely addressed by the scientific community, and most research has focused on routing protocols and battery autonomy, while ignoring the security aspect. The multi-agent paradigm is considered the most adequate and appropriate solution to model an effective intrusion detection system capable of detecting intrusions targeting a drone fleet. Multi-agent systems can perfectly address the security problem of a drone fleet, given the mobility, autonomy, cooperation and distribution characteristics present in the network linking the different nodes of the fleet. The proposed model consists of a set of cooperative, autonomous, communicating, learning and intelligent agents that collaborate with each other to carry out intrusion and suspicious activity detection missions that can target the network of a fleet of drones. Our system is autonomous and can detect known and unknown cyber attacks in real time without the need for human experts, who generally design the signatures of known attacks for conventional intrusion detection systems.**

Keywords*—*Fleet of drones; drone; intrusion detection; multi agent system; security; intrusion detection system; autonomy; distribution; UAV; unmanned aerial vehicle; unknown attacks; known attacks

I. Introduction

Drones play a major role in the everyday life of individuals, given their extensive use in several areas of expertise, and will now be the trend worldwide. According to a study conducted on the prospects for European UAV (Unmanned Aerial Vehicle), the UAV market will be the trend in the coming years in various fields: agriculture, energy, public safety, e-commerce/delivery and mobility and transport [1]. The author in [2] highlights some applications of drones as illustrated by Fig. 1. As shown in the table (Fig. 1), UAVs are generally used respectively in the military sector, in the professional civilian sector and for leisure activities. In our work, we will focus mainly on the use of drones in the civilian professional field, given the important use of drones to solve human problems.

Drones have limited resources in terms of battery life and the geographical area they can cover. As a result, a single drone cannot perform all the missions it is assigned, especially when it has to cover a large geographic area. To overcome these limitations, a fleet of drones [3] is needed, which consists of connecting several drones via a network, so that they can cooperate and collaborate with each other to accomplish more complex tasks.

In spite of the important research carried out in the scientific community on drones, the problem of security of UAV networks is still an issue, as these networks have not yet received much attention from researchers [4]. Moreover, the only security system implemented on UAVs is the Anti-collision system, which is insufficient to ensure the security of the drone against cybercrime [5]. Therefore, security issues need to be addressed and should be a major concern given the criticality of the information that transits in the network and which may be subject to various attacks.

The security issue is necessary for several reasons:

- Firstly, because the architecture of the Mobile Adhoc Network is generally vulnerable to various attacks due to the lack of a central entity monitoring the activities in the network.
- Secondly, this is due to the routing protocols used in an ad hoc network, which involve all nodes in the network in the routing operations without thinking about the presence of malicious nodes that can falsify the paths taken by the packets.
- Thirdly, because we can't distinguish between a malicious action undertaken by an attacker and another caused by the loss of linkage due to the mobility of the drones.

Fourthly and finally, we must take into consideration the problem of the drones's limited resources in terms of memory, bandwidth and energy.

Sector	Examples of applications	Roles
Law enforcement surveillance	Search and rescue	Drone are equipped with cameras
Public safety communications	Voice communications in case of disaster	Aerial base stations
Environmental applications	Climate change	Information gathering via sensors
Logistics	Goods shipping and delivery in urban areas	Drones are used as a transportation medium
Military	Searches for lost or injured soldiers	Drones use live streaming communications to send videos to ground troops, they can also be equipped with weapons
Medical field	Delivering aid packages, medicines and vaccines to remote zones	Drones are used as a transportation medium
Photography	Events such as social gatherings, sport games and competitions	Drones are used to capture videos by using cameras
Agriculture	Crop monitoring and soil and field analysis	Sensors can be placed on drones to capture the information required by the agriculture field

Fig. 1. Summary Table of the Fields of Application of UAVs [1] [2].

In light of these observations, it is necessary to ensure the security of a UAV network to detect intrusions that could affect the security principles summarized by the CIA triad (Confidentiality, Integrity and Authentication).

The flow of applications through the UAV network is of acritical importance not only for the mission requirement, but also for civilians (the critical risk would be, for example, the hijacking of a drone). The application flow is very sensitive and must be protected against illegitimate access that could corrupt the viability of the drone system [6].

A UAV network is a spontaneous environment that raises several security issues. First of all, the use of wireless links which are intrinsically vulnerable to eavesdropping attacks or denial of service. Secondly, because of the absence of message and node authentication services, knowing that it is possible to inject forged packets into the network to disrupt the proper functioning of the routing algorithm. This kind of attacks can corrupt the communication or decrease the network performance [7].

The rest of the document is organized as follows: Section 2 highlights the context of the study to define some concepts related to our work. Section 3 highlights the state of the art of the multi-agent paradigm and its use for handling complex problems. Section 4 discusses the proposed architecture of IDS, its components and its operating principle. Section 5 concludes the paper.

II. Related Work

In this section, we will highlight some of the concepts related to our research work. First, we're going to talk about drones, a fleet of drones, and the different communication architectures of a fleet of drones. Next, we'll look at the security aspects of a UAV network, while identifying the various vulnerabilities and attacks to which the UAVs in the fleet are exposed. Finally, we will close this part by defining the multi-agent paradigm, while citing the different types of agents that exist and that can deal with the security issue in a UAV network.

A. Drone Definition

A drone is an unmanned aircraft with no pilot on board, remotely controlled by a ground station. It can fly autonomously according to a programmed flight plan or by controlling it via a smartphone or tablet connected to its network [8].

Examples of the use drones for different purposes are numerous in the literature. Notably, in [9] the author proposes to use a drone to capture multispectral images and to detect the difference in terrain in the field of agriculture. In [10], the authors propose to use drones to carry an X-ray camera, an IR camera and metal detectors. For e-commerce and delivery, applications are still in their early stages given the strong impact of weight on battery life and therefore on the distance to be travelled by the drone, knowing that the delivery of small objects is already a reality. In [11], a service for transporting small medicines and blood in Africa using a winged drone is proposed. For e-commerce, several proposals have been made by large technology companies, namely Amazon's Prime Air service [12].

B. Fleet of Drones

A UAV fleet consists of several drones that cooperate and collaborate with each other to accomplish more complex tasks [3]. In a UAV fleet, each drone execites its task to participate in achieving the mission objective for which the fleet is created. A UAV fleet can be designed according to three possible communication architectures: the centralized communication architecture, the cellular communication architecture, the satellite communication architecture and the adhoc communication architecture.

C. Possible Communication Architectures of a UAV Fleet

1) Centralized communication architecture: A centralized UAV fleet communication architecture [13] is characterized by a direct wireless link between a centralized node (e.g. ground station) and the surrounding drones (Fig. 2). In this architecture, each drone is directly connected to the ground station to transmit payload data and to receive the command and control flow. UAVs are not directly connected to each other and the information can be sent between neighboring UAVs via the ground station. In this case, the ground station acts as a relay node.

2) Cellular communication architecture: This type of communication architecture is used in the field of telephony and is based on a base station infrastructure. Cells are deployed according to the density of the network sought and the geographical perimeter to be covered. Each cell includes a subset of UAVs and a ground station that manages the group [13] and communication between the members of a group must pass through the ground station (Fig. 3). Direct communication between UAVs belonging to the same cell can take place. This architecture is expensive and requires much more investment for its proper deployment.

3) Satellite communication architecture: Another communication architecture can be envisaged and it is based on the deployment of a satellite to make the different UAVs communicate with each other. In this architecture (Figure 4), the satellite plays the role of a communication relay [13]. The satellite's receiving antennas receive signals from the ground station; these signals undergo amplification and frequency conversion operations before they are retransmitted to the drones. However, this architecture requires the presence of a central entity which is the satellite to ensure routing between the control station and the drones. Given the real-time nature of the application traffic exchanged between the nodes of a fleet of UAVs, this could lead to significant latencies in exchanges between the nodes. In addition, in the presence of obstacles around the ground station (a building, for example), communication to the satellite can be partially attenuated or completely blocked.

4) Adhoc communication architecture: A wireless adhoc network consists of connecting several mobile drones equipped with one or more radio interfaces to weave a short-duration communication network to achieve the fleet's mission

objective [41]. The drones belonging to this network can enter or exit the network at any time. The adhoc communication architecture (Fig. 5) is decentralized and capable of self-organizing without the need for a fixed infrastructure. If a transmitting UAV, for example, is located outside the perimeter of coverage of the receiving UAV, the application flow is transmitted step by step to the destination point and the routing table is kept up to date by the network in case of a change in the network topology. The adhoc network enables two nodes that are out of direct reach of each other to communicate. [3].

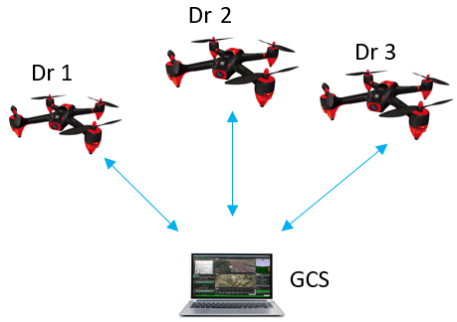

Fig. 2. Centralized Communication Architecture [13].

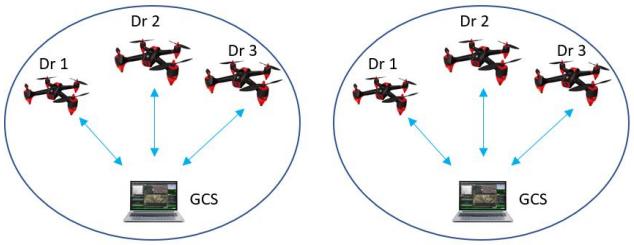

Fig. 3. Cellular Communication Architecture [13] [3].

Fig. 4. Satellite Communication Architecture [3].

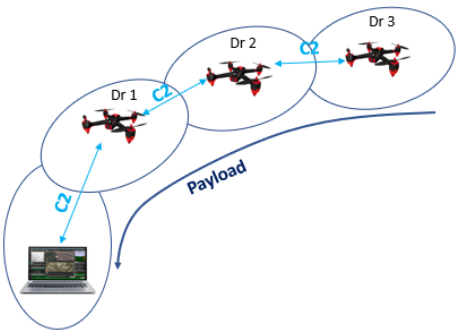

Fig. 5. Adhoc Communication Architecture [3].

D. Security in an Adhoc Network

The use of drones is becoming widespread, and that what is motivating Hackers to learn much more about drone vulnerabilities in order to exploit them and thus touch on the security principles summarized in the CIA triad (Confidentiality, Integrity and Availability). Consequently, it is imperative to ensure network security against cyber attacks to protect application flows and sensitive network data.

1) Vulnerabilities in an adhoc network: The adhoc mobile network architecture is generally vulnerable to various attacks due to the lack of a central entity monitoring the activities in the network. In addition, the routing protocols in an Adhoc network involve all nodes of the network in the routing operations and assume the absence of malicious nodes that can falsify the paths taken by packets [3].

UAV vulnerabilities can be related to the physical architecture of the nodes [14], to the different communication links, to the condition of the UAV fleet deployment (the need for cooperation between nodes) and to the possibility of malicious nodes presence in the network [15]. Radio links are often equipped with very low bandwidth and this is exactly what an attacker can exploit by saturating the network via packet broadcasting and thus succeeding in breaking the communication between the drones in the network [16].

The environment of an adhoc wireless network is uncontrolled due to its distribution and dynamic characteristics. That is, communication is shared and opportunistic between the nodes participating in the routing operations. As a result, it is very difficult to control the entry and exit of nodes into and out of the network. As a result, a malicious node could connect to the network and thus participate in the transfer of packets. It can also use the identity of a legitimate node (Identity Theft) to tamper with the routing mechanism while broadcasting incorrect information or replaying outdated information. This is notably the case of the rushing attack [17].

Drones can move at a very high speed (for example, DT18 type UAVs can reach a speed of 80 km/h), what leads to a continuous change of the network topology according to the commands issued by the ground station or those imposed by the UAV flight plan. The mobility of drones poses a security problem since a routing protocol cannot distinguish between a communication failure caused by UAV movements and an attacker trying to interrupt communications in the network [18].

An adhoc network works with the assumption that all nodes are cooperative and non-malicious in nature and the assumption that a malicious node can connect to the network is not taken into account. In this case, the authenticity of the identity of the nodes is not guaranteed since the possibility of the existence of malicious nodes is always present and they can publish routes with better metrics and thus participate in the routing operations.

Drones are very limited in termes of CPU and RAM capacities. In this case, the limited resources can be exhausted by the attackers while applying, for example, sleep deprivation

attacks [19] whose principle is the unlimited distribution of control messages to the network nodes. As a result, once these resources are exhausted, drones can be, for example, captured or hijacked by an attacker.

2) Attacks in an adhoc network: A fleet of drones relies on the wireless network to send and receive signals between nodes. The wireless network in turn relies on radio links that can be targeted by various attacks, namely eavesdropping and active interference [20].

The presence of an attacker using a high-gain antenna within range of a UAV can present a significant risk of eavesdropping on the entire network that supports the communication of the UAV fleet.

Ad hoc networks are generally targeted by different types of attacks, and drones are a new target for hackers given the importance of the application flows they carry. For example, the Eavesdropping on an adhoc network consists of placing a malicious node between two or more communicating nodes. Attackers can also explore the vulnerabilities of drone systems which can be the result of misconfiguration of UAV networks, a fault implementation, flawed designs and/ or protocols [21]. To listen to the whole network, the attacker can act on the routing protocols while trying to generate false packets or modify the routing packets.

The presence of an attacker using a high-gain antenna within range of a UAV can present a significant risk of illicit eavesdropping on the entire network constituting the communication medium of the UAV fleet.

Fig. 6 and 7 highlight possible attacks on an ad hoc network of UAVs. These intrusions can target both layers of the OSI model, the physical layer and the network layer. For example, attacks aimed at exploiting the physical layer can attack the wireless modem in use. Such attacks do not require any prior knowledge of the network topology. These attacks can take the form of eavesdropping on application flows, active interference to overlap transmission channels or jamming attacks.

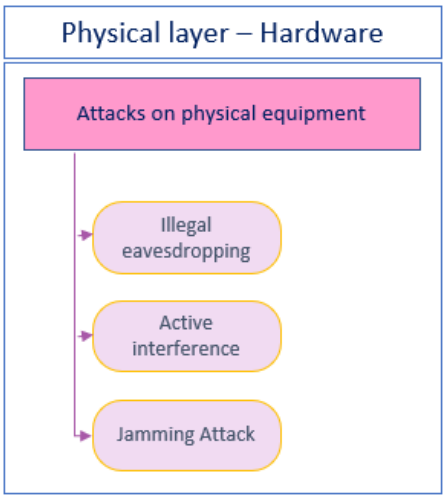

Fig. 6. Attacks Targeting the Physical Layer of a UAV [20].

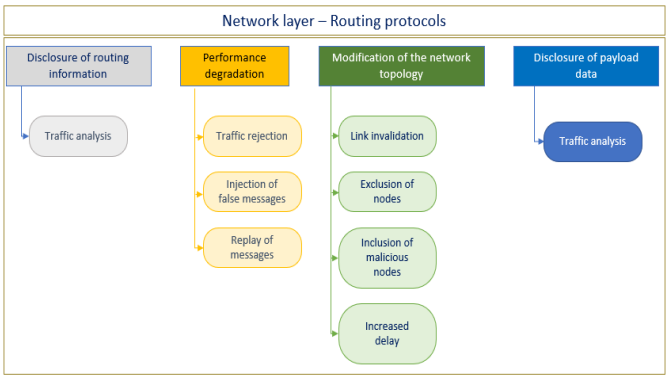

Fig. 7. Attacks that can Target the Network Layer [21][22].

Attacks aimed at attacking the network layer generally consist of disclosing routing information through traffic analysis, degrading network performance through traffic rejection, injecting false messages and replaying messages, and modifying the network topology while invalidating links, including or excluding malicious nodes, and increasing the delay of exchanges. And finally, these attacks can disclose payload data through sniffing and network traffic analysis.

E. Multi-Agent Paradigm (MAS)

1) Agent: According to [23], an agent is a physical or virtual entity that has the following characteristics:

- It must be able to act in its environment,
- It can communicate and interact with other agents,
- It seeks to achieve and optimize its individual goals, satisfactions and survival,
- It has its own resources,
- It is able to perceive its environment in a limited way,
- It has only a partial representation of this environment (Or any),
- It has skills to offer services,
- It is capable of reproducing itself when needed,
- It behaves in such a way that it satisfies its objectives within the limits of its resources and skills and this, according to its perception, its representations and the communications it receives from other entities in the system.

In the field of computer science, an agent is any computer program that has some or all of these characteristics [24][25]:

- It is capable of perceiving the environment to which it belongs in order to act appropriately.
- An agent is independent, i.e. it can act alone without human intervention (or by other agents).
- An agent is flexible, i.e. it can react quickly to changes in its environment and always tries to take advantage of opportunities to achieve its goals.

According to the Muli-agent paradigm, There are four main types of agents [23] [24] [26] [25]:

- Reactive agent that responds to changes in its environment while acting appropriately to accomplish its missions.
- Deliberative agent which can conduct deliberations to accomplish its missions and thus achieve its objectives.
- Hybrid agent that performs both the tasks of a reactive agent and those of a deliberative agent.
- A learning agent which is able to learn through the perception of its environment in order to improve its ability to act in the future without any human intervention or by other agents.

2) Multi-Agent system: A Multi-Agent system can be defined as a set of autonomous entities that interact in a given environment to achieve objectives and deal with very different problems [27]. Multiagent Systems mainly aim to achieve the following objectives:

- Multi-agent systems aim to carry out their missions according to the phenomena and problems to be dealt with. There are different types of MAS that are:
  - Cooperative SMA (MAS) where each agent sets its own objective. The agents in this SMA trust each other and can make decisions together to achieve their common goal.
  - Competitive SMA: Each agent in this type of system sets its own objective relying on simulation by agents to reproduce a phenomenon external to the system.

III. State of the Art

A. UAV Security and Mutliagent Paradigm

1) UAV security: The security of UAV networks has not yet received much attention from researchers. Most of the research conducted by the scientific community has focused on routing protocols and optimizing UAV autonomy, while ignoring the security aspect, which has been of major importance lately and is now attracting the attention of manufacturers.

Several research projects have dealt with the safety aspect of UAV systems. Notably, in [28], the author carried out an audit of the behavior and vulnerability of UAVs used in the IoT as an intermediate communication medium. In [29], the authors proposed to use the Blockchain technology to transmit signals between the controller and the UAV. The author of [30] gave a secure routing protocol for UAV Ad hoc NETworks (UAANETs). In [4], a rule-based IDS is proposed to detect GPS Spoofing, Jamming and False information attacks. In [31], the focus was on the security of the physical layer to counter jamming, eavesdropping and spoofing attacks that can target UAV systems. The author in [32] proposed an IDS for the UAV using behavior rule specifications knowing that most existing IDS for UAV use behavior based detection mechanisms [33].

From the above literature survey, we can identify that a simple framework based IDS is only designed for UAV against different types of attacks with major limitations.

2) Multiagent paradigm for computer security: The MAS (Multi-Agent System) paradigm is widely used by researchers to address complex problems that are difficult or impossible to address with traditional methods. Agent technology is already used to address the security aspect in traditional information systems. For example, in [34], the author considers the network as a set of nodes and opts for a multi-agent system as a solution to detect suspicious activities at the level of all nodes. The author in [35] highlights a hybrid intrusion detection system called MOViCAB IDS which is based on artificial neural networks and multi-agent architecture. In [36], a distributed intrusion detection system architecture is proposed and it is based on mobile agents allowing decision making and agent replication. The author of [37] gave a model of a PAID intrusion detection system using multi-agent technology. The proposed model is based on several agents capable of sharing their beliefs (Soft findings) and measuring values (Hard findings). This model allows to analyze the information contained in the system and to estimate the probability of intrusion according to its agents.

In [38], a framework named SPIdER is proposed, based on a set of autonomous agents with heterogeneous processing models. The author of [39] proposed the IA-NSM (Intelligent Agents for Network Security Management) system to detect intrusions by relying on intelligent agent technology. This architecture is hierarchical and is based on a set of agents that communicate and cooperate with each other in order to perform intrusion detection missions efficiently and with optimal processing performance. The author in [40] develops an approach for network intrusion detection based on multi-agent systems and the artificial immune system (AIS). The AIS system is based on autonomous, mobile, collaborative, adaptive and learning agents. The MAIS-IDS (Multi-agent Artificial Immune System - Intrusion Detection System) is a hybrid IDS by anomaly detection that is capable of analyzing system configurations to detect activities that may be real intrusions that threaten the security of the system.

B. Discussion

Based on the study of the state of the art conducted to better understand what is done in the literature regarding the security of drones. The security of a UAV fleet is rarely addressed, despite the fact that these fleets represent the future trend in the use of UAVs for civilian missions. Most of the work cited in the state of the art has focused on routing protocols, autonomy optimization, communication architectures... while ignoring the security aspect, which is receiving much more attention given the disastrous damage that can occur if the security principles of a UAV fleet are circumvented.

Research work in the field of the adhoc UAV network generally focuses on improving on-board ground communication between a drone and a ground station and optimizing inter-drone communication, and does not address the safety aspect of UAVs. The scientific community is opting for multi-agent systems to deal with complex problems affecting different fields. This technology is very effective in simplifying the most complex problems. The network of a fleet of UAVs is in turn very complicated due to the continuous modification of the network topology and the increased speed of the UAVs. As a result, dealing with the safety of an UAV fleet is a very difficult mission to accomplish.

The computer security of a UAV fleet based on an adhoc communication architecture is very complex to address due to the continuous change in the network topology and the rapid mobility of the nodes. In this case, opting for the multi-agent paradigm proves to be the most appropriate solution to address the security gaps in an adhoc UAV network.

In our work, we will propose a more efficient intrusion detection architecture allowing to detect intrusions in an adhoc UAV network in real time without any network latency or depletion of limited UAV resources (CPU, RAM, Storage...).

IV. Proposed Approach

A. General View

In a fleet of UAVs, all the nodes communicate with each other and generate very sensitive application flows. These flows include very critical information, which can be routing information, payload traffic (images, videos, sounds, etc.), control and command traffic (C2), GPS coordinates, etc. It is therefore necessary to secure these application flows against malicious persons who can exploit the vulnerabilities of the wireless ad hoc networks to impact the smooth operation of the UAV fleet.

Fig. 8 gives a brief description of the ad hoc communication most used in the deployment of UAV fleets. Indeed, the ad hoc network is a sub-category of the Manet mobile networks. This mode of communication consists of connecting a set of cooperative mini drones that have an enormous mobility speed. In an ad hoc UAV fleet network, we find exchanges of routing data and payloads. Therefore, we need to think about security to secure the data flow that passes through it.

B. Proposed Model

To fill the security gaps in adhoc UAV networks, we thought of designing and developing an intrusion detection system to detect intrusions targeting UAV fleets based on ad hoc networks. The IDS will be placed at the level of the adhoc network so that it captures all traffic circulating at the level of the UAV network including the control station. It will then proceed by comparing the captured traffic with the normal reference profile to determine whether it is an attack or not. Our system is designed to fully comply with the security principles of data confidentiality, integrity, availability and authenticity (Fig. 9).

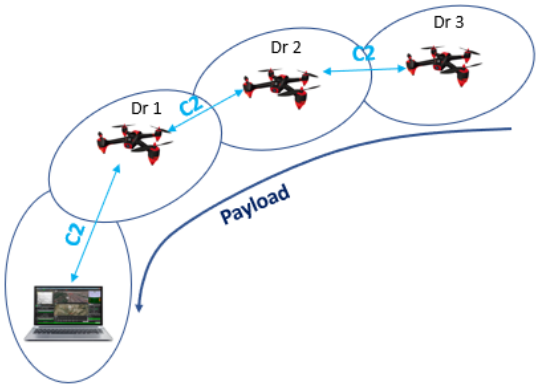

Fig. 8. Adhoc Architecture of a UAV Fleet [3].

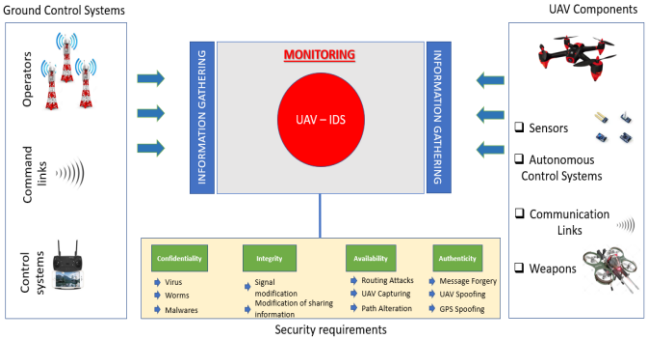

Fig. 9. General Overview of the Intrusion Detection System in an adhoc UAV Network.

Our approach, to detect intrusions and attacks targeting a fleet of drones based on an adhoc network, is to propose an intrusion detection system model based on the multi-agent paradigm. Indeed, the proposed system is distributed and includes a set of autonomous, learning, cooperative and communicating agents to undertake actions to detect attacks in an adhoc network of drones.

The proposed IDS model will be deployed in such a way that it receives all traffic from the UAV fleet's, including the ground station. Our IDS will be based on machine learning techniques while learning the normal operation of the UAV ad hoc network to model the normal reference profile, and from there any deviation from this profile is considered as an intrusion while notifying the fleet owner. Fig. 10 gives an overview of the location of our system in an UAV fleet ad hoc network.

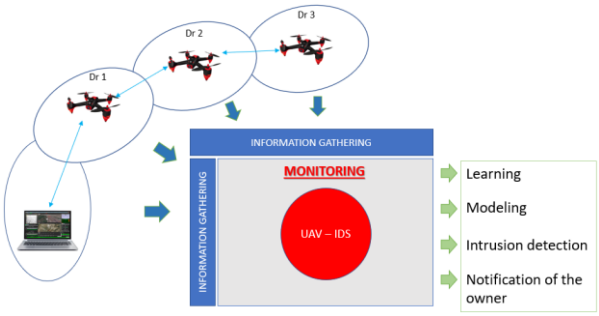

Fig. 10. General Overview of the Proposed IDS to Capture Attacks Targetting adhoc Networks.

The diagram (Fig. 11) illustrates our proposed IDS model. This system is composed of a set of cooperative and communicating agents that collaborate with each other to carry out intrusion detection missions.

Our model consists mainly of a total of seven agents which are: Sniffer Agent (SA), Filtering Agent (FA), Feature Selection Agent (FSA), Decision Maker Agent (DMA), Reporting Agent (RA), Alert Manager Agent (AMA) and Taking Action Agent (TAA). Each agent in the system is responsible for carrying out specific tasks to help achieve the system's strategic objectives, which are to detect intrusions in an efficient manner without impacting the resources of the drones belonging to the fleet.

C. Components of the Proposed System

Our approach is based on the multi-agent paradigm given the complexity of adhoc UAV networks in terms of node mobility and the continuous change in the network topology of the fleet. To simplify the system, multi-agent technology proves to be the most appropriate solution to address the problem of intrusion detection in this type of network. The proposed intrusion detection system consists of the following components:

- Sniffer Agent (SA): This agent represents the entrance of our system; it takes care of capturing all the network traffic that transits in the adhoc network. To do so, this agent will be equipped with a high gain antenna that will be placed in a location so as to cover the entire perimeter of the fleet.
- Filtering Agent (FA): This is a reactive agent that checks the packet match against a knowledge base of all signatures of all known attacks and intrusions. If it finds a match, a notification will be generated to alert the user and if the packet is not recognized by the signature database, it will be sent to the Storage Cluster for processing.
- Feature Selection Agent (FSA): This agent is intelligent and relies on machine learning techniques to extract the features that best describe network packets. In addition, it uses size-reduction techniques to select only the relevant parameters that can characterize and distinguish network packets.
- Decision Maker Agent (DMA): This is a learning agent that uses machine learning techniques to model different types of attacks and normal traffic. It is based on the calculated values of the attributes extracted by the FSA.
- Alert Manager Agent (AMA): This agent is responsible for correlating the various alerts and alarms generated by the system in order to reduce their number and to keep only those that are true alerts and not false positives. It also allows the user, via the GUI interface, to intervene to mark alerts as true or false alarms. This allows the administrator's expertise to be exploited and leveraged to improve the accuracy of the IDS and reduce the false positive rate.
- Reporting Agent (RA): It allows reports to be developed according to the needs of administrators. The user can generate dashboards and reports so that he has more visibility on the security KPIs that need to be more meaningful through the use of graphs.
- Taking Action Agent (TAA): This agent allows to take actions in case of attack or intrusion. The user via its graphical interface can neutralize an attack by isolating the UAV concerned, for example, it can also ensure the RTH (Return To Home) of the drone before it is lost or captured by hackers and malveillant persons. The TAA communicates with the AMA and can be programmed according to the alerts generated. For example, it can trigger the landing of a legitimate drone as soon as a malicious UAV is detected trying to enter its adhoc network.
- Knowledge Base Module: This is a knowledge base that includes all known attack signatures. This base will be enriched by new signatures of attacks detected by the IDS.
- Storage Cluster: The traffic coming from the adhoc networks is very voluminous and transits with an increased speed. Therefore, choosing HDFS storage is more appropriate and allows for very fast processing without any latency or performance degradation.

D. Principle of Operation of the Proposed System

The operating principle of the proposed model is illustrated in Fig. 12.

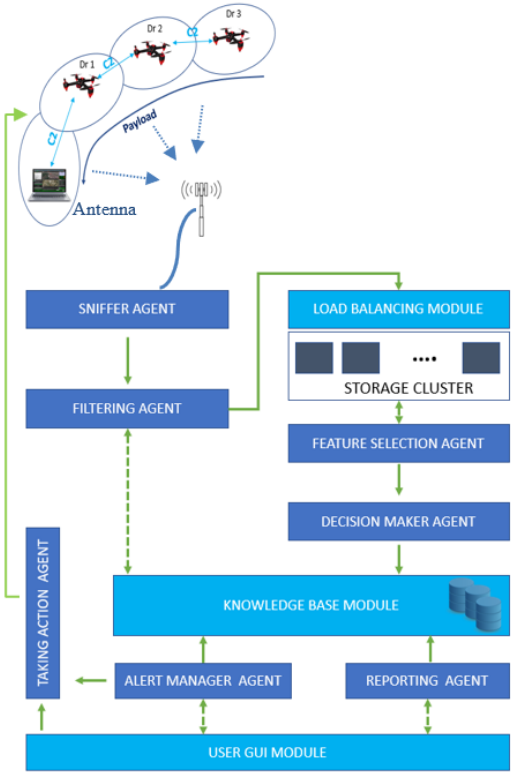

Fig. 11. The Proposed Model of IDS.

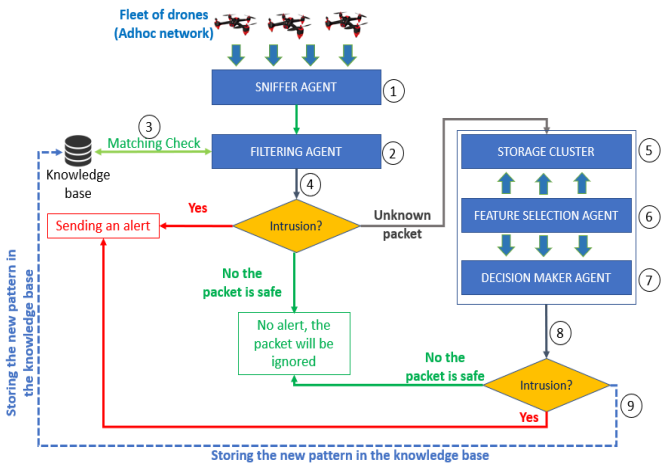

Fig. 12. Operating Principle of the Proposed Model.

As we can see in the diagram above, the intrusion detection mechanism at the level of an adhoc network of a UAV fleet is done according to nine steps which are:

- Step 1: In this step, the system, via its SA agent, captures all network traffic circulating in the UAV fleet, based on a high-gain antenna that can cover the entire perimeter of the fleet.
- Step 2: The captured traffic is sent to the next agent, which is the FA.
- Step 3: The FA opts for a matching check against a knowledge base containing all known attack and intrusion signatures.
- Step 4: Depending on the result of the matching verification, there are three possible scenarios:
    - Either the packet matches an attack signature already known by the knowledge base, in which case the FA alerts the system administrator to see the intrusion details,
    - Either the network packet is normal and does not represent any risk for the fleet network and in this case the packet will be ignored and will not undergo any further processing,
    - And finally, if the package is not recognized by the signature database, then in this case it will be sent to the following agents to undergo the necessary treatments to identify its nature.
- Step 5: Then, as we said in the previous step, if the packet is not recognized, it will automatically be stored in a HDFS (Hadoop Distributed File System) storage cluster to undergo the necessary treatments.
- Step 6: In this step, the FSA chooses to extract the characteristics and attributes that best describe the behavior of the packet. It also ensures dimension reduction through the use of machine learning algorithms in order to obtain good detection accuracy.
- Step 7: The DMA agent uses the attribute values calculated by the FSA and a model of normal traffic to detect deviations from normal traffic. The DMA uses machine learning techniques and must be trained beforehand on a training dataset so that it can recognize the nature of network packets.
- Step 8: Depending on the result of the processing, there are two scenarios:
    - The packet is normal, in this case no notification will be sent to the system administrator,
    - The packet is intrusive: An alert will be sent to the administrator to prompt him to see the details of the intrusion.
- Step 9: Whatever the result of the detection (Intrusion or not), the new pattern will be stored in the knowledge base to be used in step 3.

V. Experimentation

In this section, we will discuss the micro level of our system's operation. This section deals with the experimentation part related to the use of machine learning techniques to make the system learn the different known attacks and to make it possible for it to detect zero-day attacks by opting for semi-supervised machine learning techniques. In this part, we will be focusing on the two used techniques to detect known and unkown attacks.

A. Dataset

To test our model, we used the CICIDS2017 dataset which is an up-to-date dataset encompassing all normal events as well as those of the various most recent known attacks. This dataset includes data annotated using the network analysis tool CICFlowMeter, which allows us to label the flow based on the timestamp, source and destination IP addresses, source and destination network ports, protocols used and the name of the attack [42].

The CICIDS2017 dataset contains all kinds of network traffic that can pass through a network. On the one hand, it includes normal network events that do not present any risk of compromising the security principles (CIA) and on the other hand, it gathers all events that may be generated by cyber attacks. CICIDS2017 recognizes the following attacks [42] [43]:

- Brute force attacks: This technique attempts to guess passwords or encryption keys by trying a large number of possible combinations. This technique requires much more effort depending on the complexity of passwords and encryption keys.
- Denial of Service (DoS) attacks: This type of attack prevents authorized users from using a service, network or computer system. During this attack, the attacker can act in several ways to make the target inaccessible and out of service: Notably, overloading a network with packets to cause network congestion and thus degrade its performance, or targeting a specific host computer to

make it out of service and thus prevent users from accessing it.

- Botnet attacks: This attack is very widespread and is based on the use of a network of Bots (zombies), these are usually computers infected with malware to become part of the Botnet network and therefore obey the commands of the C&C attacker against a specific target.
- Port scanning: This attack allows an attacker to send probe packets to a network or a system to extract information from the received responses. In particular, the attacker can detect ports that are open, closed and filtered by a firewall. Without forgetting that the hacker, via this technique, can identify the version of the used OS (Fingerprinting) and thus better understand the victim's vulnerabilities.
- SQL injections: This is the most dangerous attack since it allows inserting, reading and modifying information contained in a database. This attack takes advantage of coding vulnerabilities (No input validation, XSS vulnerability...) and web server vulnerabilities to inject SQL commands into text and search boxes.
- XSS (Cross-Site-Scripting) attacks: This attack can be undertaken if the attacker has the ability to place scripts in the HTML content of a web page. This attack occurs when the developer has not reinforced the input validation in his application during the development phase. Through this attack, the hacker can steal a user's cookies in order to impersonate him without any authentication or authorization.
- Heartbleed: This is a bug in the Open-SSL library used in asymmetric PKI (Public Key Infrastructure) cryptography. This attack was discovered in 2014 and allows an attacker to execute arbitrary code in the compromised target.

B. Tools for Simulation

In order to test the proper functioning of our system we have used the data analysis tool called Knime. It is widely used in the field of data science to test machine leaning techniques.

Knime is a software designed to create and produce scientific data using a simple and intuitive environment that allows each stakeholder in data science to focus on what they do best.

C. Supervised Machine Learning

As we have seen in the "Proposed model" section, our IDS is based on two machine learning techniques which are: Supervised and unsupervised machine learning techniques. The supervised machine learning is performed using the Decision Tree algorithm, which has given conclusive results with 100% of accuracy and a zero false positive rate.

1) Decision Tree workflow: To train and test our model, we have opted for the following workflow (Fig. 13).

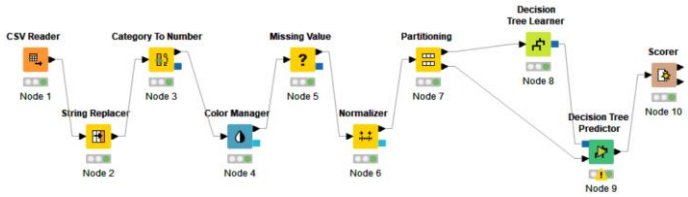

Fig. 13. Decision Tree Workflow.

As we see in the figure above, the data undergoes some pre-processing operations before being consumed by the machine learning decision tree algorithm. These operations generally consist of:

- String Replacer: The objective of this phase is to make data readable while replacing erroneous characters with readable and more meaningful ones.
- Data transformation: Data must be transformed into quantitative data to be consumed by the Decision Tree algorithm. As a result, all categorical values have been transformed into quantitative values that can be used by the mathematical equations of the Decision Tree algorithm.
- Missing data: This process allows missing data to be replaced by their average for example. This helps to have satisfactory results during the learning phase. The action of replacing null and missing values took place to make the CICIDS data more reliable and more readable by the Decision Tree algorithm.
- Data normalization: This technique allows to modify the values of the numerical columns of the dataset in order to use a common scale without markup or loss of information. The Decision Tree algorithm needs this normalization operation in order to model the data correctly.
- Data partitioning: During this phase, we segmented the data into two categories:
  - Training dataset: This is the data for training and represents 80% of the total dataset. The training dataset contains all possible categories of network events (normal traffic and malicious traffic), which allows the model to be trained on any possible type of event.
  - Test dataset: This dataset represents 20% of the dataset and allows to evaluate the implemented model.

2) Results and metrics: After preparing the training dataset, the Decision Tree algorithm uses this data to come up with a model capable of distinguishing normal traffic from other suspicious activities. The ML algorithm used has proven very good results in detecting known attacks, it was able to achieve 100% detection accuracy with zero false positives (FP) and false negatives (FN). Fig. 14 illustrates the obtained results using the Decision Tree algorithm. The results are conclusive and are represented by the following rates:

- True Positives: TP
- False Positives: FP
- True Negatives: TN
- False Negatives: FN

Fig. 15 below shows the confusion matrix of the used algorithm. This table illustrates the effectiveness of the Decision Tree against the modeling of known attacks contained in the CICIDS2017 dataset.

D. Semi-Supervised Machine Learning

In this part, we will clarify the mechanism for detecting unknown attacks that are not recognized by the first phase of filtering based on supervised machine learning. The figure 16 highlights the workflow adopted by network traffic before the nature of network events is identified. Network traffic that is not recognized by the FA (Supervised Machine Learning) moves on to the next steps to undergo semi-supervised machine learning operations.

Traffic	TP	FP	TN	FN
Benign	454861	0	111288	0
DDoS	25671	0	540478	0
Port Scan	31695	0	534454	0
Bot	384	0	565765	0
Infiltration	7	0	566142	0
Web Attack Brute Force	307	0	565842	0
Web Attack XSS	130	0	566019	0
Web Attack SQL Injection	4	0	566145	0
FTP-Patator	1622	0	564527	0
SSH-Patator	1192	0	564957	0
DoS Slowloris	1161	0	564988	0
DoS Slowhttptest	1119	0	565030	0
DoS Hulk	45933	0	520216	0
DoS GoldenEye	2061	0	564088	0
Heartbleed	2	0	566147	0

Fig. 14. Accuracy Statistics.

	Benign	DDoS	Port Scan	Bot	Infiltration	Web Attack Brute	Web Attack XSS	Web Attack SQL	FTP-Patator	SSH-Patator	DoS Slowloris	DoS Slowhttptt	DoS Hulk	DoS GoldenEye	Heartbleed
Benign	454861	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DDoS	0	25671	0	0	0	0	0	0	0	0	0	0	0	0	0
Port Scan	0	0	31695	0	0	0	0	0	0	0	0	0	0	0	0
Bot	0	0	0	384	0	0	0	0	0	0	0	0	0	0	0
Infiltration	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0
Web Attack Brute Force	0	0	0	0	0	307	0	0	0	0	0	0	0	0	0
Web Attack XSS	0	0	0	0	0	0	130	0	0	0	0	0	0	0	0
Web Attack SQL Injection	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0
FTP-Patator	0	0	0	0	0	0	0	0	1622	0	0	0	0	0	0
SSH-Patator	0	0	0	0	0	0	0	0	0	1192	0	0	0	0	0
DoS Slowloris	0	0	0	0	0	0	0	0	0	0	1161	0	0	0	0
DoS Slowhttptest	0	0	0	0	0	0	0	0	0	0	0	1119	0	0	0
DoS Hulk	0	0	0	0	0	0	0	0	0	0	0	0	45933	0	0
DoS GoldenEye	0	0	0	0	0	0	0	0	0	0	0	0	0	2061	0
Heartbleed	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2

Fig. 15. Confusion Matrix.

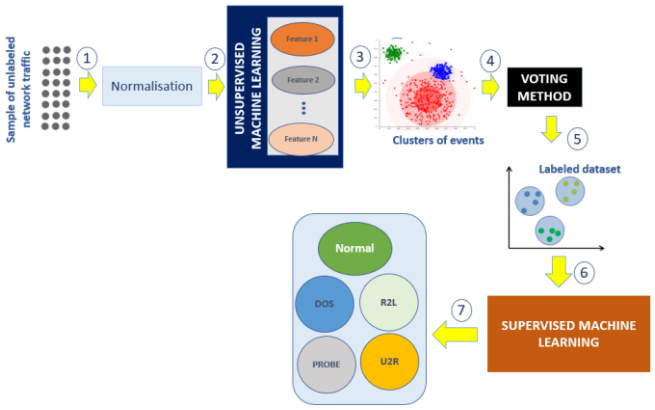

Fig. 16. Semi-Supervised Machine Learning Workflow.

Semi-supervised machine learning techniques consist in passing network traffic through the following phases:

- Phase 1 (Non-supervised machine learning): In this step, the unannotated network traffic is learned by an unsupervised machine learning technique. At the end of this phase, the algorithm groups the network events into a set of Clusters (Each Cluster includes events that have certain similarities).
- Phase 2 (Voting Method): Arriving at this stage, the unannotated data are not yet annotated with labels. To do this, the voting method is used to be able to name the different Clusters with significant attack names [44]. The output of this operation gives us annotated data that can be learned using supervised machine learning techniques.
- Phase 3 (Supervised machine learning): After having produced the annotated data, the latter undergoes learning actions by the supervised machine machine algorithms so that the different events can be recognized later during the next filtering by the FA.

For the semi-supervised machine learning techniques, we have unfortunately not yet experimented with this part and it will be dealt with in another work in the near future.

VI. Conclusion and Perspectives

In this paper, we put forward a model of an Intrusion Detection System (IDS) to detect intrusions in a UAV fleet using an adhoc communication architecture. The proposed IDS is distributed and based on the multi-agent paradigm and an HDFS storage cluster. Our system can detect any type of attacks and intrusions that can target a network of drones. It ensures the detection of known and unknown attacks in real time based on machine learning techniques that allow the modeling of the network traffic of the UAV fleet. This application demonstrates the usefulness of the methodologies proposed by the multi-agent community that can be used to ensure the security of a network of drones linked by adhoc. Our IDS model perfectly meets the security requirements of an UAV network based on adhoc networks in terms of:

- Distribution: Given the distributed nature of the network linking drones with small adhoc networks.

- Dynamism: The rapid and continuous change of the network topology due to the mobility of nodes and the possibility of losing a node at any time.
- Volumetry: The data generated by a network of a fleet of UAVs is voluminous and requires appropriate means to process it.
- Cooperation: UAVs in an adhoc communication architecture are communicative and cooperative; security systems must take this aspect into account.
- Autonomy: UAVs are autonomous, so the security system must be autonomous in order to effectively detect intrusions.
- Learning: The detection of unknown intrusions must be based on machine learning techniques, so our system is built using intelligent learning agents.
- Performance: The security system must be efficient to take into account the limited resources of the UAVs in the fleet in terms of CPU, RAM and storage.

The work is not finished yet, there are still several tasks to be done to make our system more efficient and able to detect known and unknown attacks in real time, we quote in particular:

- Testing the semi-supervised machine learning with Knime: This allows us to choose the right algorithms with increased detection accuracy and a much reduced false positive rate.
- Setting up an HDFS (Hadoop Distributed File System) environment: This allows us to evaluate the real-time character of our system. Bearing in mind that machine learning algorithms generally require CPU, RAM and storage resources.
- Retrieving a real dataset gathering the set of network events generated by the nodes of a fleet of UAVs communicating by adhoc.
- Testing the entire system within a real fleet's network.

REFERENCES

[1] Undertaking, S.J. European Drones Outlook Study. Unlocking the Value for Europe; Technical Report; SESAR Joint Undertaking: Brussels, 2016.

[2] Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A survey Gaurav Choudhary, Vishal Sharma, Ilsun You, Kangbin Yim, Ing-Ray Chen, Jin-Hee Cho

[3] Architecture de communication sécurisée d'une flotte de drones Jean-Aimé Maxa.

[4] A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks Hichem Sedjelmaci, Sidi Mohammed Senouci, Nirwan Ansari.

[5] Detecting signal spoofing and Jamming Attacks in UAV networks using a light weight IDS Menaka Pushpa Arthur Menaka Pushpa Arthur.

[6] Raja Naeem Akram, Pierre-François Bonnefoi, Serge Chaumette, Konstantinos Markantonakis, and Damien Sauveron. Improving security of autonomous uavs fleets by using new specific embedded secure elements a position paper.

[7] Sonja Buchegger and J-Y Le Boudec. Nodes bearing grudges : Towards routing security, fairness, and robustness in mobile ad hoc networks. In Parallel, Distributed and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on, pages 403–410. IEEE, 2002.

[8] https://www.drone-malin.com/pages/en-savoir-plus/les-drones/c-est-quoi-un-drone.html.

[9] Lum, C.; Mackenzie, M.; Shaw-Feather, C.; Luker, E.; Dunbabin, M. Multispectral Imaging and Elevation Mapping from an Unmanned Aerial System for Precision Agriculture Applications. In Proceedings of the 13th International Conference on Precision Agriculture, St. Louis, MO, USA, 31 July–4 August 2016.

[10] Hamza, M.; Jehangir, A.; Ahmad, T.; Sohail, A.; Naeem, M. Design of surveillance drone with X-ray camera, IR camera and metal detector. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 111–114.

[11] Zipline. Zipline, 2017. Available online: http://www.flyzipline.com (accessed on 11 April 2018).

[12] Amazon. Amazon Prime Air, 2016. Available online: https://www.amazon.com/Amazon-Prime-Air/b? node=8037720011 (accessed on 11 April 2018).

[13] Eric W Frew and Timothy X Brown. Networking issues for small unmanned aircraft systems. Journal of Intelligent and Robotic Systems, 54(1-3) :21–37, 2009.

[14] Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang, and Hal Aldridge. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. Infotech@ Aerospace, 2012.

[15] Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Homeland Security (HST), 2012 IEEE Conference on Technologies for, pages 585–590. IEEE, 2012.

[16] Ping Yi, Zhoulin Dai, Shiyong Zhang, and Yiping Zhong. A new routing attack in mobile ad hoc networks. International Journal of Information Technology, 11(2) :83–94, 2005.

[17] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security, pages 30–40. ACM, 2003.

[18] Jack Elston, Eric W Frew, Dale Lawrence, Peter Gray, and Brian Argrow. Net-centric communication and control for a heterogeneous unmanned aircraft system. Journal of Intelligent and Robotic Systems, 56(1-2) :199–232, 2009.

[19] Matthew Pirretti, Sencun Zhu, Narayanan Vijaykrishnan, Patrick McDaniel, Mahmut Kandemir, and Richard Brooks. The sleep deprivation attack in sensor networks : Analysis and methods of defense. International Journal of Distributed Sensor Networks, 2(3) :267–287, 2006.

[20] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour. A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, 14(5) :85–91, 2007.

[21] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, no. 8, pp. 805–822, 1999.

[22] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks: challenges and solutions. IEEE wireless communications, 11(1) :38–47, 2004.

[23] J. Ferber – 1995 – "Les systèmes multi-agents, vers une intelligence collective", Inter Editions (1995).

[24] Said OUIAZZANE et all Toward Network Intrusion Detection System for Geographic Data.

[25] Barramou F., Addou M. – 2012- An agent based approach for simulating complex systems with spatial dynamicsapplication in the land use planning.

[26] Said OUIAZZANE et al. A Multi-Agent Model for Network Intrusion Detection.

[27] Philippe Caillou Présentation Des Systèmes Multi-Agents - Master IAC 2014 – 2014.

[28] Behavior and Vulnerability Assessment of Drones-Enabled Industrial Internet of Things (IIoT) Vishal Sharma ; Gaurav Choudhary ; Yongho Ko ; Ilsun You.

[29] An intelligent approach for UAV and drone privacy security Tarun Rana, Achyut Shanker, Mohd Karman Sultan, Rizwan.

[30] J. Maxa, M. S. Ben Mahmoud and N. Larrieu, Secure routing protocol design for UAV Ad hoc NETworks. IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, 2015, pp. 4A5-1-4A5-15.

[31] User-Centric View of Unmanned Aerial Vehicle Transmission Against Smart Attacks Liang Xiao, Senior Member, IEEE, Caixia Xie, Minghui Min, Student Member, IEEE and Weihua Zhuang, Fellow, IEEE.

[32] R. Mitchell and I. Chen. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications. in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 5, pp. 593-604, May 2014.

[33] D. Shen, G. Chen, E. Blasch, and G. Tadda, "Adaptive markov game theoretic data fusion approach for cyber network defense," in IEEE Military Communications Conference (MILCOM 2007), 2007, pp. 1–7.

[34] Lasheng et Chantal - Agent Based Distributed Intrusion Detection System.

[35] Navarro et al. - 2010 - Approaching Real-Time Intrusion Detection through.

[36] Manjula, D College, R M D Engineering Nadu, Tamil – 2012 – Dynamic Distributed Intrusion Detection System Based on Mobile Agents with Fault Tolerance Department of Computer Science and Engineering , Department of Computer Science and Engineering.

[37] Gowadia, Vaibhav Farkas, Csilla Valtorta, Marco – 2005 – PAID: A probabilistic agent-based intrusion detection system.

[38] Miller, P. Inoue, A. – 2003 – Collaborative intrusion detection system – Annual Conference of the North American Fuzzy Information Processing Society – NAFIPS.

[39] Boudaoud, K. Labiod, H. Boutaba, R. Guessoum, Z. – 2000 – Network security management with intelligent agents – IEEE Symposium Record on Network Operations and Management Symposium.

[40] Afzali, Neda Azmi, Reza – 2014 – Engineering Applications of Artificial Intelligence MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach.

[41] Abdelilah Alshbatat, Liang Dong Performance Analysis of Mobile Ad Hoc Unmanned Aerial Vehicle Communication Networks with Directional Antennas.

[42] A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems.

[43] Vilhelm Gustavsson Machine Learning for a Networkbased Intrusion Detection System 2019.

[44] Muhammad Aamir, Syed Mustafa Ali Zaidi - Clustering based semi-supervised machine learning for DDoS attack classification.