Article

Not peer-reviewed version

SecGPSR: A secure GPSR protocol for FANET against Sybil and Gray Hole Attacks

Mauro Tropea *, Mattia Giovanni Spina, Abderrahmane Lakas, Panagiotis Sarigiannidis, Floriano De Rango

Posted Date: 11 December 2023

doi: 10.20944/preprints202312.0718.v1

Keywords: GPSR; FANET; Sybil attack; Gray Hole attack

Article

SecGPSR: A secure GPSR protocol for FANET against Sybil and Gray Hole Attacks

Mauro Tropea [1,*], Mattia Giovanni Spina [1], Abderrahmane Lakas [2], Panagiotis Sarigiannidis [3] and Floriano De Rango [1]

[1] Department of Computer Engineering, Modeling, Electronics and Systems (DIMES), University of Calabria, Via P. Bucci 39/c, 87036 Rende, Italy; {m.tropea, mattiagiovanni.spina, derango}@dimes.unical.it

[2] College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 17551, United Arab Emirates; alakas@uaeu.ac.ae

[3] Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece; psarigiannidis@uowm.gr

* Correspondence: m.tropea@dimes.unical.it; Tel.: +39-0984-494786

Abstract: In recent years, drones have become increasingly prevalent in a wide range of applications, performing complex and critical tasks. To accomplish these tasks, drones cooperate by forming a Fly Ad-hoc Network (FANET) using specific routing protocols for communication. However, most of the routing protocols used in this type of network lack appropriate built-in security mechanisms, which creates numerous security challenges and concerns. To reduce the resulting security vulnerabilities and mitigate the impact of potential attacks, it is crucial to address these challenges before any deployment of FANETs. In this paper, we address two of the most harmful routing attacks - Sybil and Gray Hole and propose mitigating techniques to alleviate these attacks on FANET routing protocols. The proposed solution is secGPSR a secure version of the Greedy Perimeter Stateless Routing Protocol (GPSR). We validate the robustness of secGPSR through simulation using Omnet++ and present the results which show its effectiveness against Sybil and Gray Hole attacks.

Keywords: GPSR; FANET; sybil attack; gray hole attack

1. Introduction

The use of Unmanned Aerial Vehicles (UAVs) in many areas of applications, such as monitoring, surveillance, smart agriculture, mission-critical, etc. [1], is becoming always stronger, thanks to their ability to cooperate and accomplish a wide range of different tasks, even complex one like executing a Machine Learning (ML) model to detect malicious activities taking place in an overlay network [2,3]. Their capability to work in the group needs opportune communication mechanisms in order to make them able to perform their tasks without human intervention and create a particular network called Fly Ad-hoc Network (FANET) [4]. An important aspect to be taken into account in these new types of networks concerns the capability of providing dynamic connectivity [5,6] and the choice of the routing protocols that could consider the rapid network node changes [7], which lead to instability of the data transmission link. Many proposals of novel routing protocols have been provided in the literature, some of them based on bio-inspired approaches such as in [8]. One of these proposed protocols in these particular ad-hoc networks is the Greedy Perimeter Stateless Routing (GPSR) [9] which uses mobile position information to improve the decision of the choice of the next forwarding node considering only information about a node's immediate neighbors in the network topology in a greedy approach [10]. The high mobility of FANET could also affect security in different ways so effective and efficient countermeasures are fundamental for avoiding any possible attacks. In this context, routing protocols used to make these devices capable of communicating with each other can be targeted by potential attackers who want to compromise any form of communication, network topology, and data transmission. Indeed, these routing protocols are designed with the main objective of supporting communications characterized by high mobility patterns that result in dynamic topology changes that must be effectively handled. Therefore, the security of such a kind of protocol is most of the time neglected. This poses a great challenge when it comes to guaranteeing that the communication between drones in a FANET relies on a secure channel. Among the different routing attacks that aim at disrupting and hijacking the legacy network topology, some of them need to be carefully analyzed due to their harmful impact: *Gray Hole* and *Sybil* attacks. These two attacks are capable of completely subverting the FANET network topology. In the case of the Gray Hole attack hijacked legacy nodes or injected malicious ones will act with the main objective to drop packets that are flowing through the network following a specific dropping policy. The policy could be protocol, node, likelihood, and time-dependent. The Sybil attack, instead, is meant to wrongly modify the actual network topology by injecting a malicious node that is capable of assuming multiple identities with respect to the other nodes of the network letting them perceive the attacker's network topology.

Sybil and Gray Hole attacks belong to the class of routing attacks and any routing protocol that does not provide specific countermeasure is susceptible to them. In this paper, a FANET network that relies on the insecure GPSR routing protocol has been considered proposing an effective way to counteract Gray Hole and Sybil attacks against this routing protocol. As a result, a secure version of GPSR has been proposed which is called *secGPSR* and that is based on the use of Elliptic Curve Cryptography (ECC) to provide message authentication between drones in a FANET counteracting the Sybil attacks. In addition, a detection algorithm for Gray Hole attacks is introduced to accurately determine a drone that is misbehaving and acting as a Gray Hole node.

The remainder of this paper is organized as follows: Section 3 provides useful background on the involved technologies and attacks; in Section 2 a brief literature overview is given. Section 4 describes the proposed mitigations to secure the GPSR protocol against Gray Hole and Sybil attacks. In Section 5 the performance evaluation will be given and Section 6 will conclude the paper.

2. Related Works

In this section, a brief overview of the recent literature works on security issues in drone networks is provided. Even though there are several studies on mobile ad hoc network (MANET) and vehicular ad hoc network (VANET) security in the literature, research on FANET security is still in its early stages despite its widespread use.

2.1. Security Issues on FANET

Security aspects and possible attacks toward drones have been analyzed in various survey articles such as [11–15]. Among these, i.e. in [16] the authors provide a comprehensive taxonomy of security threats and solutions. Moreover, they try to identify and compare suitable security measures that the scientific community has proposed to mitigate FANET security threats. Drones (or UAVs) are generally not designed with security features therefore security and privacy issues, focusing on possible vulnerabilities and threats, are fundamental aspects to be studied. These papers show how it is fundamental for these new types of devices to have secure and reliable communication in order to avoid the management of false information that can cause disasters in the specific context where drones are deployed. There is no approved protocol for protected communication in a UAV ad hoc network, hence communication between nodes inside a FANET is not secure. Thus, the authors in [17] propose an approach to identify the network's malicious node, that tries to determine a node's reputation or trust value in the network using linear regression. Using the Logistic Regression Classification, the node is classified as either a malicious or normal node depending on the trust value determined by the classifier enabling a safe data transmission.

The use of emerging technologies such as Blockchain, Software Defined Networks (SDN), Machine Learning, and Fog/Edge computing as possible approaches to provide solutions to security issues in UAV architecture are presented and discussed in [18].

2.2. Gray Hole and Sybil attacks and mitigations

Researchers have proposed some works in detecting and mitigating Gray Hole and Sybile attacks in VANET that, as FANET, represent a particular type of MANET where the mobile nodes are vehicles or drones, respectively. For example, in [19] the authors have proposed a study focused on the detection of Gray Hole attacks in a vehicular network providing a solution mechanism called Smart Black Hole and Gray Hole Mitigation (SBGM) using a time series analysis of the dropped packets of each node based on Dynamic Time Warping able to improve the detection accuracy in SBGM. Also in [20], a Gray Hole attack aimed at disrupting traffic between cars and on the roadside in the field of autonomous and connected vehicles (ACVs), which represents a critical environment, is presented. The authors present a neural network-based technique for detecting and preventing these types of attacks in vehicular networks analyzing also novel systematic reactions in order to protect vehicles against dangerous behavior. Another work, [21], is focused on security threats on VANET taking into account the Sybil attack. This is a serious issue that occurs when a malicious user intentionally assumes or steals many identities used to disrupt the normal VANET operation. In the article, the authors propose a hybrid technique that combines footprint and P2DAP (privacy-preserving detection of pseudonym abuses) approaches. The results shown by the authors prove that the detection rate is increased when applying this hybrid algorithm.

Among the few works that deal with Sybil and Gray Hole attacks in FANET, there is [22]. In order to ensure trusted communication in FANET, the authors propose a detection of Sybil attack based on a novel solution that exploits the “visual” and “auditory” domains (VD and AD, respectively) in order to enable drones to accurately correlate what they “see” from VD and “hear” from AD to permit the attack detection. The simulation results show how the proposed solution is able to outperform other approaches in detecting Sybil attacks. In [23] the authors, in the context of reviewing different cryptographic techniques to secure drone communications, introduce a very general description of the possible Gray Hole and Black Hole attacks providing also some possible mitigations and countermeasures techniques. A naive version of the Gray Hole attack, in which all packets are dropped without applying any specific dropping policy is represented by the Black Hole attack. Concerning this last type of attack in [24], the authors propose an enhanced version of the OLSR protocol, called secure OLSR (S-OLSR), in order to be able to detect this type of attack in the communication between drones. The proposed S-OLSR proposes to use a fuzzy logic approach to evaluate the trustiness of a node and optimize the multipoint relay node selection algorithm in OLSR improving the security of the OLSR protocol.

2.3. Main Contributions

According to our information, only two papers are provided in the literature that deal with Sybil and Gray Hole attacks, as shown in the previous section. And, none of these propose the use of lightweight cryptographic primitives based on the ECC technique along with mathematical detection to mitigate and counteract them. In the following, the main contributions of this paper are provided highlighting the main differences with the literature proposed works.

- In order to counteract Sybil attacks the adoption of elliptic curve cryptography (ECC) to ensure drones’ message authentication by means of Elliptic Curve Digital Signature Algorithm (ECDSA) has been proposed allowing for recognizing messages that are generated by fake identities drones, without using dedicated devices but only relying on the already available resources and computation capabilities provided in each drone.
- Following the work proposed in [24], we proposed a mitigation technique based on a trustiness metric to counteract the smarter version of the Black Hole attack, namely the Grey Hole. To the best of our knowledge, this is the first attempt to provide a security countermeasure to a Gray Hole attack for the GPSR protocol. The proposed mitigation technique is able to determine

whether a drone of the network is acting as a Gray Hole node by keeping track of its behavior over time and, if needed, isolating it from the topology.
- As far as we know, there have been no proposals that combine the use of lightweight cryptographic primitives along with a mathematical detection algorithm to counteract the Sybil and Gray Hole attack.

3. Background

3.1. Flying Ad-Hoc NETworks (FANETs)

FANETs are an emerging technology that allows to obtain sensor networks in regions where there is no fixed infrastructure or where they are difficult to reach. They are made up of swarms of UAVs communicating with each other. Thanks to recent technological advances in electronics, sensors, and communication systems, the production of small UAVs has paved the way for the development of low-cost FANETs. Given their versatility, they can be used in many fields, such as Traffic monitoring, Agricultural remote sensing, Forest fire management, etc... Such networks have significant advantages, as they can be deployed anywhere without a fixed infrastructure, developing a multi-hop network where all the UAVs communicate with each other and the base station. In this way, information can be shared between connected network nodes, and in the event that one node goes offline, it is possible to communicate with the others still connected to the network. In these types of networks, it is possible to solve the problems related to short-range connectivity by exploiting multi-hop communications [4].

Although FANETs appear to be the ideal solution for many scenarios, problems related to communication and networking can arise, as UAVs can move in 3D space by rapidly changing the network topology. For this reason, it is necessary to choose an appropriate communication architecture and reliable routing protocols to provide robust communication between UAVs. Our project activity fell on the analysis of the geographic routing protocol GPSR and of two possible attacks associated with it: Sybil and Gray Hole attacks.

3.1.1. Greedy Perimeter Stateless Routing (GPSR)

GPSR is a geographic routing protocol for wireless networks. The routing algorithm uses routing information for each node: the positions of nearby nodes, the position of the destination node, and its own location. In this work, it is assumed that each node knows the position of the destination of the packets to be routed. Concerning the locations of nearby nodes beacons are used. Each node broadcasts a beacon containing its identifier (an index or an IP address) and its coordinates so that every other node within the transmission range of the sender receives adequate information on the position of the latter and stores it. Beacons are sent by nodes, and if a node does not receive a beacon from another node after a certain amount of time, it removes this last from its neighbors' list [9,25]. The GPSR uses two methods for forwarding packets:

- Greedy forwarding, used where possible;
- Edge forwarding, used where the technique cannot be used greedy.

Greedy forwarding uses the receiver location and its neighbors to calculate which of them is closest to the destination, to which it will then forward the packet. Repeating this procedure step by step for each node the destination node is reached.

However, there are situations where this algorithm is not applicable. There are topologies in which the only possible route to a destination forces a packet to be moved temporarily farther in geometric distance from the destination. In these cases, perimeter forwarding is used to decide which node will be the next hop [9].

Under these circumstances, there is a gap region formed between the intersection of the transmission ranges of the current and destination nodes, and the goal of perimeter forwarding is to bypass this region. The network is interpreted as a graph whose nodes are the nodes of the network and the edges connect each node to those in its neighbor list. To route packets through the nodes around the void region, the right-hand rule is used, i.e. given one face of the graph, we traverse the nodes in sequence in an anticlockwise direction so as to traverse the entire void region outwards. In order to exploit this property, the graph representing the network must be planar, i.e. a graph in which there is no pair of crossing vertices. In GPSR it is possible to use two different planar graphs:

- Relative Neighborhood Graph, ie a graph in which if there is an arc between two nodes A and B, then there must not exist a third node C such that its distance from A or B is less than the distance of A from B.
- Gabriel Graph, i.e. a graph in which if there is an arc between two nodes A and B, then there must be no other nodes in the area of the circumference having AB as diameter.

According to the perimeter forwarding algorithm, each node will exclude from potential candidates for the next hop the nodes to which it is not connected by an edge in the planar graph chosen among the two listed above. When node A starts perimeter forwarding, it writes its position in the packet header and will send the packet crossing, with the right-hand rule, the faces of the planar graph closest to the destination (calculated considering the intersection between the faces and the segment joining node A to the destination). When the packet is received by a node whose distance from the destination is less than that of node A which initiated the perimeter forwarding, it is possible to go back to using the greedy technique.

3.2. *Public Key Cryptography*

Cryptography can be historically split into two main eras: *classical*, mostly related to symmetric key cryptography; and *modern*, related to public key cryptography algorithms [26]. The turning point between these two eras was the introduction of the breakthrough algorithm that allowed to overcome all the shortcomings related to the exchange of the symmetric key between two communication parties without the need to share any secret information but only keying material information that *must* be authentic but not secret. This algorithm was the Diffie-Hellman key exchange, introduced in 1975 and that is still the basis of almost all the authentication schemes used nowadays (e.g. TLS: Transport Layer Security). However, public key cryptography can be used also to encrypt/decrypt data and to generate digital signatures providing integrity, non-repudiation, and authentication. All the public key cryptography schemes are based on a set of common fundamentals [27]:

- Each communication party is associated with two keys: the public key and the private key.
- As their name suggests, the public key is publicly available while the private key *must* be kept private.
- When one of the keys is used to encrypt data, the other one must be used to decrypt that data. Generally, if public key cryptography is used to guarantee confidentiality the public key of the receiver party is used to encrypt data. Then the receiver will use its private key to decrypt it. If public key cryptography is used to generate digital signatures, the sender uses its private key to sign the message that the receiver will verify retrieving the public key of the sender.

One of the main issues of public key cryptography schemes is related to the size of the keys that need to be used to ensure that the algorithm cannot be broken (e.g. at least 2048-bit key size for RSA) in a reasonable finite amount of time. This poses a great challenge when we need to adopt such methods on constrained resource devices, such as drones. To overcome this issue, Elliptic Curve Cryptography was introduced in 1985. ECC is one of the main applications of public key cryptography through which, exploiting an algebraic and geometric object, namely an elliptic curve, it was possible to reduce the size of the generated keys preserving the security degree associated with them [27].

3.2.1. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography system that relies on an algebraic structure called *elliptic curve*. An elliptic curve E is described by the following equation:

$$y^2 = x^2 + ax + b, with\ a, b \in \Re \tag{1}$$

The curve *must* be non-singular which mathematically means that its discriminant must satisfy the following condition:

$$4a^3 + 27b^2 \neq 0 \tag{2}$$

It must be also ensured that the curve has a special point $\overline{O}$, called *point at infinity*, such that $\forall\ point\ P \in E$ it holds that $P + \overline{O} = P$. This is the general equation that describes an elliptic curve defined on $\Re$. However, an elliptic curve for practical cryptography applications is limited to a finite field. Let p be a prime number and F_p the finite field of integers modulo p. An elliptic curve E over F_p is defined as follows:

$$y^2 = x^2 + ax + b\ mod\ p,\ with\ a, b \in F_p \tag{3}$$

Consequently, the condition in Equation (2) changes as follows:

$$4a^3 + 27b^2 \neq 0\ mod\ p \tag{4}$$

In a nutshell, the number of points on the curve are (and for practical applications cannot be) infinite, but are all the points that can be enumerated in F_p, which is a *finite* field. ECC has been highly adopted, especially in constrained devices, thanks to the highly efficient key generation mechanism that is based on a simple addition of points or multiplication between a scalar value and a point over an elliptic curve. More specifically, let $P\ \in E(F_p)$, a point belonging to the set of all the points over the curve $(E(F_p))$. Let x be a randomly generated integer. Summing x times the point P to itself, it is possible to obtain a point $X\ \in\ E(F_p)$ defined as follows:

$$X = x * P \tag{5}$$

The point X, in this setting, will be the public key, while the number x must be kept private since it is used as a private key. The Equation (5) defines the classical trapdoor function that is needed in a public key cryptography scenario: having x it is easy to compute X. But starting from X it is not possible to retrieve and obtain x. This is granted and holds due to the commonly known *Discrete Logarithm Problem (DLP)* extended to the Elliptic Curves (ECDLP), which has been demonstrated to be more robust than the traditional DLP which lays the foundation of the Diffie-Hellman algorithm robustness against an attacker that tries to retrieve the private key starting from only the public key (either using brute force or more advanced and complex mathematical methods). Based on these premises, the ECC allows for the use of keys that are characterized by a limited size (in terms of occupied bits) but preserve their security degree. The NIST in [28] demonstrated that a 256-bit ECC key is as secure as a 3072-bit RSA key. As with any other public key cryptography scheme, ECC can be used to compute Digital Signatures in order to guarantee not only data integrity but also non-repudiation and accountability. The Digital Signature Algorithm (DSA) extended to the ECC is called the ECDSA. It allows to generate and verify signatures relying on the security granted by the ECDLP.

3.3. Considered Attacks in the FANET

There is a wide plethora of attacks that can be attempted against FANET, as has been described in the literature review presented in Section 2. In this paper, two of the most harmful routing protocol attacks—Sybil and Gray Hole attacks—have been analyzed and in this section, a brief description of the two considered attacks is provided.

3.3.1. Sybil Attack

The Sybil attack is a common attack that mostly affects peer-to-peer wireless and wired networks. In this attack, a malicious node generates one or more fake identities and uses them to fool the legacy nodes of the network pretending to be one of them. The number of fake identities a malicious node can create uniquely depends on its resource and computational capabilities such as the memory needed to store information about these fake identities and the corresponding routing data, as well as the bandwidth that is needed to handle and serve multiple concurrent requests ensuring a not suspicious delay. When dealing with geographic protocols, such as the GPSR protocol, the routing protocol strongly relies on the positional coordinates of a node, Sybil attack can be very harmful. Indeed, the legacy network topology could be completely disrupted. In Figure 1 an example of an attack is depicted. The malicious node M generates a fake identity for each legacy node of the network. Finally, it pretends to be D with respect to A injecting fake topology information making A seem that D is its neighbor. This kind of attack, on a larger scale, allows an attacker to potentially take control over the entire topology and even its management.

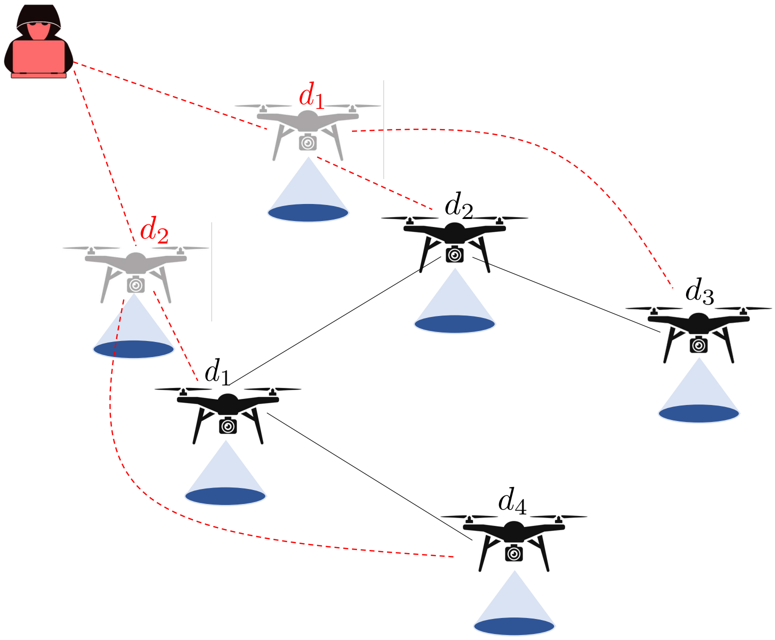

Figure 1. Sybil attack scenario.

3.3.2. Gray Hole Attack

The *Gray Hole Attack* [29], depicted in Figure 2, is a routing layer attack in which a malicious node inside the network selectively drops packets. It is an advanced and specialized version of the Black Hole attack that, as the name suggests, generates a point in the network in which all the packets that reach it get dropped. The behavior of the Gray Hole attack, instead, is driven by a *packet dropping* policy used to define the criteria based on which packets should be dropped. More specifically, several policies can be applied to specialize the attack making it way smarter than the Black Hole:

1. Node Dependant Policy: only packets coming from or directed to a specific node of the network get discarded (e.g. packets from node "X" get dropped).

2. Time Dependant Policy: Packets are dropped based on predetermined trigger time (e.g. each five seconds drop a packet).
3. Protocol Dependant Policy: a packet is dropped according to the protocol to which it belongs (e.g. drop every TCP packet).
4. Likelihood Dependant Policy: a packet is dropped based on the value that a variable, that follows a specific likelihood distribution, can take (e.g. following a random uniform likelihood distribution, each packet is dropped with a likelihood of 50%).

Such a type of attack is very difficult to detect, needing a wide detection strategy that is able to take into account the network performance of all the nodes and the relationships that exist among all of them.

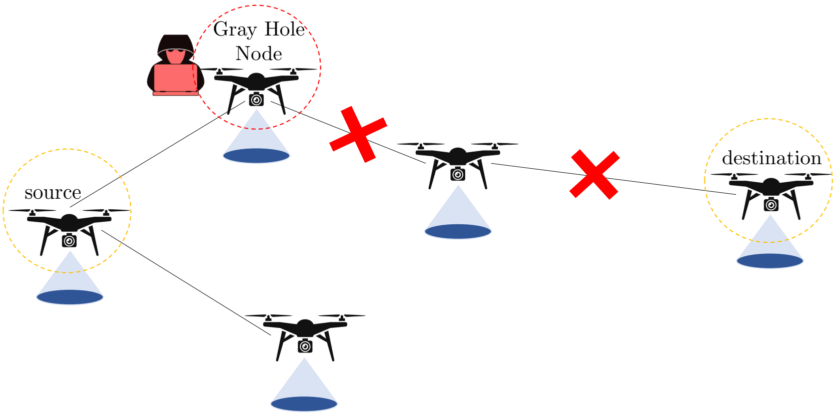

Figure 2. Gray Hole attack scenario.

4. Proposed Secure GPSR (SecGPSR)

In this section, the secure protocol schema designed to protect GPSR communications from Sybil and Gray Hole attacks is described.

System Model

The main entities and components of the system are described as follows:

- A set of drones $D = \{d_1, d_2, \ldots, d_n\}$, such that $n \in \mathbb{N}^+$ that compose the FANET.
- A set of drone identifiers $ID = \{id_1, id_2, \ldots, id_n\}$. More specifically, each drone d_i will be univocally identified in the system using $id_i \in ID$ with $i = 1, \ldots, n$.
- Each drone $d_i \in D$ is associated with a public and private key pbK_{d_i} and prK_{d_i}.
- The framework involves a set of trusted Certificate Authorities (CAs) indicated with the acronym $CA = \{CA_1, CA_2, \ldots, CA_N\}$ that issue a certificate to create the binding between a drone d_i and its public key pbK_{d_i}. Each CA also checks the authenticity of the binding and manages the certificate life cycle (Enrollment, Renewal, and Revocation). With no loss of generality and for the sake of simplicity we considered a unique CA that handles all the entities of the system.
- A set elliptic curves E $= \{e_1, e_2, \ldots\ e_l\}$ with $l \in \mathbb{N}^+$ supported by each drone $d \in D$.

Threat Model

Without losing generality, the CA has been considered "trusted" and is verified and approved by a Root Certificate Authority (RCA). Therefore, it is not possible for an attacker to fool the CA by issuing a request for a certificate with a fake entity-public key binding

- The unique CA used to issue and verify the certificate of the drones' public key ($\forall\ drone\ d_i\ pbK_{d_i}$), has been considered trusted. This means that the used CA is verified and approved by a Root Certificate Authority.

- It is supposed that the CA cannot be fooled by an attacker who wants to create a fake entity-public key binding issuing a crafted and fake certificate request to the CA.
- Each drone will act following the GPSR protocol specifications. No assumptions are made about unexpected wrong behaviors of drones (that are not related to malicious activities) that lead them to deviate from the normal behavior of the GPSR.
- It is assumed that each drone of the system can be hijacked by a malicious user who wants to turn the drone into a Sybil and/or Gray Hole node.
- No assumptions are considered on the resources available for the attacker. In other words, we built the proposal considering that the attacker has potentially infinite available resources.
- No assumptions have been made regarding the amount of possible fake identities that the attacker can create when launching a Sybil attack. We built the proposal considering that the attacker can craft an unlimited number of fake identities.
- The proposal does not rely on any assumption about how severe could be the dropping policy used for the Gray Hole attack.

4.1. Sybil Attack: Mitigation

The Sybil attack aims at forging multiple fake identities in order to subvert legacy nodes' authenticity. Nodes of the network are not able to recognize, in such a way, malicious entities from legacy ones. Based on these considerations, the proposed *secGPSR* aims at providing authentication among all legacy nodes of the network. More specifically, following GPSR specifications, each node before being part of the network topology must advertise its neighbors about its MAC source address as well as its geographic position using a *beacon* packet. Let *d* be a drone that wants to join the network:

$$\begin{gathered} beacon \leftarrow d\_MAC \;||\; d\_position \\ \forall\; droned_j \in Neighborood(d) \\ advertise\; d_j \end{gathered}$$

Data embedded in the beacon are sent over an insecure communication channel as plaintext. This means that an attacker can forge a malicious beacon, containing arbitrarily chosen information, that will be accepted and used by any other legacy node to update its network topology view in a not consistent way. To solve this crucial security issue, we developed an authentication procedure that relies on ECC, and more specifically on the DSA algorithm extended to ECC namely ECDSA. Each exchanged beacon is signed using an elliptic curve DSA. Let d_i be a drone that wants to join the network, and let $Neighborhood(d_i)$ the set of drones that are neighbors of d_i

$$\begin{gathered} sign \leftarrow ECDSAsign(beacon, prK_d, H) \\ sec\_beacon \leftarrow beacon \;||\; sign \;||\; sn \end{gathered}$$

Where *sn* is the packet sequence number defined as a 32-bit string $\{0,1\}^{32}$ that is used to prevent from *replay attack*.

The drone d_i will advertise each drone $d_j \in Neighborhood(d_i)$ using this sec_beacon. To verify the validity of the beacon, each d_j executes the following steps:

1. Extracting $sign$ from sec_beacon.
2. Computing $\{V, NV\} \leftarrow ECDSAver(beacon, sign, pbK_{d_i}, H)$
3. If $V(alid)\; \forall\, d_j\; \in Neighborhood(d_i),\; d_i$ will be correctly authenticated and allowed to enter the network.
4. If $\exists\, d_j \in Neighborhood(d_j)\; s.t.\; N(ot)\; V(alid)$ the node will not be allowed to join the network.

It is worth noting that we also used the $sequencenumber$ already included in the beacon to prevent $ReplayAttack$. Particularly, when a drone receives a beacon, before executing any other of the steps previously described, it checks the validity of the sequence number included in the beacon it has just received compared with the last recorded sequence number $last_{sn}$:

$$\{V, NV\} \leftarrow verify(sn)$$

where $verify$ is a function defined as follows:

$$verify(\text{sn}) = \begin{cases} \text{False} & \text{sn} \leq \text{last}_{\text{sn}} \\ \text{True} & otherwise \end{cases}$$

If $False$ is returned it means that this beacon has been already received and handled therefore it is discarded and ignored, preventing a beacon reply attack. Otherwise, the previously described steps will be executed to properly handle the sec_beacon.

4.2. Gray Hole Attack: Mitigation

Gray Hole attack, as previously stated, is an advancement of the Black Hole attack. With respect to it, Gray Hole is more complex to detect due to the dropping policy that makes the attack more silent and noticeable. To properly detect this kind of attack it is needed a detection method that takes into account and analyses the network performance of all the nodes of the network (e.g. packets transmitted and packets dropped by each node). More specifically, we considered that a drone $d \in D$ is hijacked by an attacker which makes it a Gray Hole drone. A Gray Hole attack is based on the following steps::

1. The malicious drone receives a packet m.
2. Based on a chosen dropping policy p it decides whether to drop or not m.
3. If the result of the policy p is "drop" then the packet will be dropped.
4. Otherwise the packet will be routed following the legacy routes and the routing protocol towards the destination.

Being the packets dropping driven by a smart policy, and not being a blind drop as happens for the Black Hole attack, is complex to detect whether a node is maliciously acting or not. Therefore, it is complex to determine if one of the legacy nodes gets hijacked and starts to act not following the normal expected behavior. We considered this complex scenario, in which the Gray Hole attack is carried out internally in the legacy network, considering a legacy node that gets hacked and hijacked by a malicious user that makes it a Gray Hole drone.

Based on these considerations, we proposed a system-wide detection mechanism based on a trustiness metric T. Given a drone $d_i \in D$, the trustiness of d_i is computed as follows:

$$T(d_i) \leftarrow \frac{\sum_k \gamma_{k,i}}{\sum_k \gamma_{k,i} + \sum_k \psi_{k,i}}$$

where γ denotes the packets correctly handled and forwarded by d_i; while ψ denotes the number of packets that the drone d_i did not forwarded. The output provided by this metric is then compared against a threshold θ used to determine whether the node is acting as a Gray Hole or not. More specifically, the Gray Hole detection method works as follows:

$$\forall\ droned_i \in D$$
$$\text{compute } T(d_i) \leftarrow \frac{\sum_k \gamma_{k,i}}{\sum_k \gamma_{k,i} + \sum_k \psi_{k,i}}$$
$$Malicious, Benign \leftarrow GHdetection(T(d_i))$$
$$\text{where } GHdetection(T(d_i)) = \begin{cases} \text{Malicious} & \text{T}(\text{d}_\text{i}) < \theta \\ \text{Benign} & otherwise \end{cases}$$

5. Performance Evaluation

In this section, we evaluated the performance of secGPSR, proving the effectiveness of the security proposal against the Sybil and Gray Hole attacks. Different officials and new proposals of network simulators can be used for performing experiments in FANET [30]. In this work the simulation campaigns are carried out using Omnet++ simulating a three-dimensional area whose size is 1500mx800mx200m, deploying across this area fifty drones. Each drone moves in the area following the "TurtleMobility" mobility pattern; each of them is characterized by a communication range of 300m. In Figure 3 is depicted the map of the University of Calabria used to perform simulations. Simulations have been conducted considering an increasing number of malicious nodes for both attack types, namely Gray Hole and Sybil. Specifically, out of the fifty legacy drones we considered a number of malicious drones starting from five and reaching half of the network with an increasing step of five. It is worth noting that for the Gray Hole attack, we considered a likelihood-dependant dropping policy based on a uniform distribution and a drop rate of 0.6.

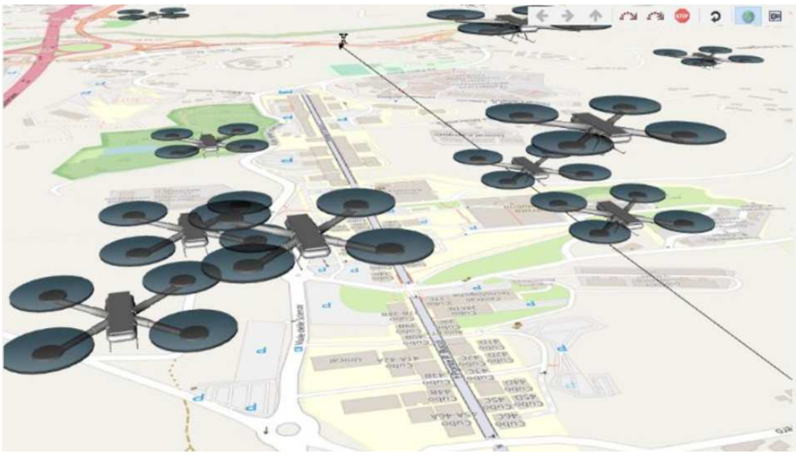

Figure 3. Reference Scenario—University of Calabria map.

Table 1. Simulation parameter.

Parameter	Value
Simulation Area (m)	1500x800x300
Simulation Time (s)	600
Number of Drones	50
Mobility model	TurtleMobility
Beacon Transmission Interval (s)	1
Protocol Type	UDP
Bit Rate (Mbps)	24
Communication Range (m)	300
Packet Size (Byte)	128
Types of attack	Sybil and Gray Hole
Maximum Number of Sybil nodes	25
Maximum Number of Gray Hole nodes	25
Gray Hole Drop Rate (DR)	0.6
θ	0.7

5.1. Sybil and Gray Hole Attacks: GPSR Performance

This simulation campaign aims to demonstrate the impact of the two aforementioned attacks on the GPSR protocol when no security measures are applied to it. The parameter taken into account to quantify how they affect GPSR communication is the Packet Transmission Rate (PTR) measured while either Sybil or Gray Hole is taking place. It evaluates the number of packets that are successfully transmitted. Table 2 and 3 show the PTR of the system when it is targeted by a Sybil and a Gray Hole attack, respectively. It can be observed that while the number of malicious users increases the network performance of the legacy nodes of the network dramatically decreases. The worst behavior is shown when the network is targeted by a Sybil attack since the network topology is completely disrupted by the fake identities created by each Sybil node. Network packets will be routed toward fake nodes that are not the expected legacy ones. Different is the case of the Gray Hole, in which the dropping policy makes the attack less disruptive since each packet is dropped with a likelihood of 60%. In such a case, accordingly with the DR, the PTR when the number of malicious nodes is 25 (half of the network) is around 53%.

Table 2. Sybil attack.

Hosts Number	Sybil Number	Sent Packets	Received Packets	PTR (%)
50	0	636	582	91.51
45	5	636	552	86.79
40	10	636	430	67.61
35	15	636	383	60.22
30	20	636	295	46.38
25	25	636	188	29.56

Table 3. Gray Hole attack with a DR of 0.6.

Hosts Number	Gray Hole Number	Sent Packets	Received Packets	PTR (%)
50	0	636	582	91.51
45	5	636	561	88.21
40	10	636	491	77.20
35	15	636	460	72.33
30	20	636	450	70.75
25	25	636	337	52.99

5.2. Sybil and Gray Hole Attacks: secGPSR Performance

In this section, the impact of the proposed secGPSR in mitigating Sybil and Gray Hole attacks is analyzed. In order to evaluate the effectiveness of our proposal in mitigating Sybil and Gray Hole attacks, we repeated the same simulations shown in Section 5.1, but with the proposed secGPSR enabled. In Table 4 we summarize the amount of packets that flow (sent/received) in the network. It can be noticed, comparing Table 4 with Table 2, that the amount of correctly received packets significantly increases. As the number of Sybil nodes increases, the amount of received packets is not affected as it happened in the case of GPSR with no security mechanism enabled. Even the worst-case scenario (25 Sybil nodes), strongly benefits from the proposed mitigation: the number of packets that are correctly delivered is more than doubled, from 188 (no mitigation) to 407 (with secGPSR mitigation). In Figure 4 the benefits in terms of PTR that the mitigation can provide with respect to the traditional GPSR (with no security measure enabled). Indeed, enabling the secGPSR, it can be noticed how the attempt of Sybil nodes to disrupt and violate the legitimate network topology is restricted. The PTR is, in most cases, not affected by the presence of Sybil nodes and, even in the worst case the impact of the Sybil nodes is limited leading to (more than) doubling the PTR with respect to GPSR. These results prove the effectiveness of the proposed secGPSR in thwarting Sybil attack.

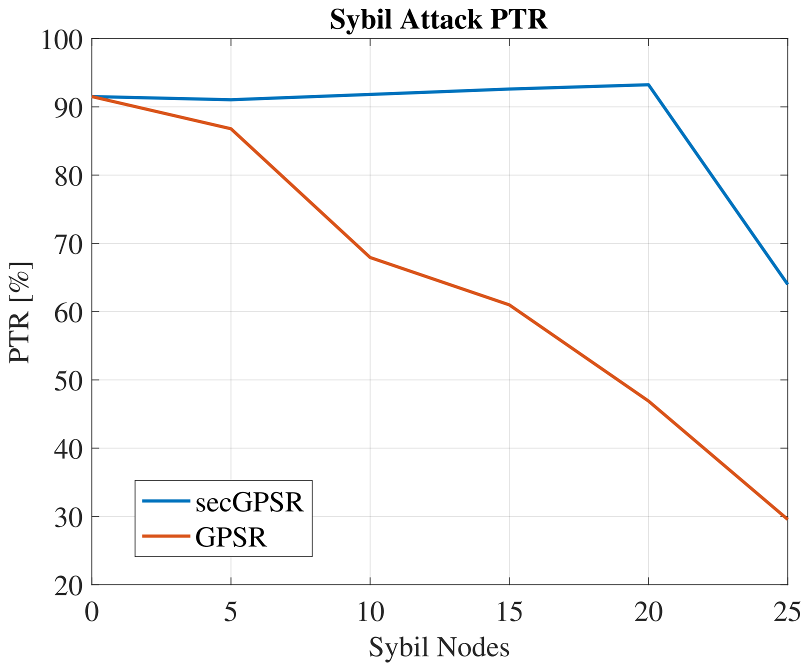

Figure 4. Sybil Attack PTR Evaluation.

Table 4. SecGPSR: Sybil attack mitigation.

Hosts Number	Sybil Number	Sent Packets	Received Packets	PTR (%)
50	0	636	582	91.51
45	5	636	579	91.04
40	10	636	584	91.82
35	15	636	589	92.61
30	20	636	593	93.24
25	25	636	407	64.00

The secGPSR, as mentioned in Section 4.2, is also designed to counteract the Gray Hole attack. In Table 5, results about the effectiveness of the proposal against Gray Hole are shown in terms of packets that are correctly routed in the network while the attack is taking place.

Table 5. secGPSR: Gray Hole attack with a DR of 0.6.

Hosts Number	Gray Hole Number	Sent Packets	Received Packets	PTR (%)
50	0	636	582	91.51
45	5	636	580	91.19
40	10	636	545	85.69
35	15	636	530	83.33
30	20	636	489	80.19
25	25	636	421	66.19

Also in this case the mitigation is successful and, concerning GPSR with no mitigation Table 3, the received packets increase. This means that the mitigation is able to isolate Gray Hole nodes that are targeting the network, recognize them, and tear them down increasing the ability of the network to correctly route packets towards the destination avoiding the Gray Hole nodes. These results can be further highlighted in Figure 5, where the PTR of secGPSR is compared to the PTR of classic GPSR. The PTR when the secGPSR is adopted increases by $\sim 10\%$ mitigating the harmful impact that a Gray Hole attack can cause on the network.

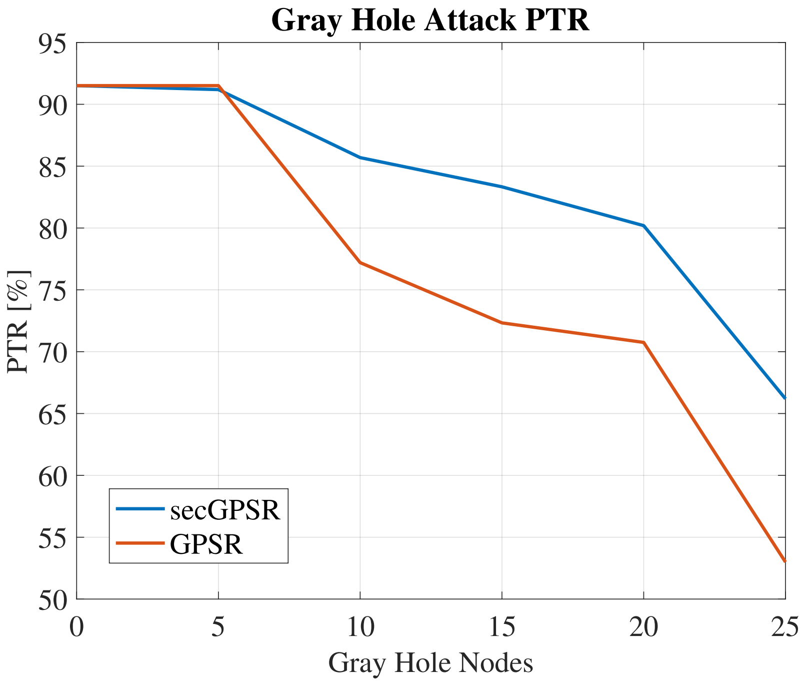

Figure 5. Gray Hole Attack PTR Evaluation.

However, to verify the effectiveness of the proposal in counteracting the Gray Hole attack, the analysis of the successfully routed/delivered packets is not enough. The proposed mitigation is based on a trust metric whose objective is to determine the degree of legitimacy of a node, by analyzing its behavior during time; in other words, determining whether it is correctly handling the network traffic or misbehaving and hijacking packets' routes. Therefore, the capability of the proposed mitigation to correctly distinguish malicious from legitimate nodes has to be analyzed. For such a reason and to provide a complete analysis, the False Negatives (FNs) and False Positives (FPs) produced by the proposed mitigation are studied, considering also the True Positives (TPs) and True Negatives (TNs) detection. We studied on each node of the network the behavior of the proposed Gray Hole mitigation (in terms of FNs, FPs, TPs, TNs), and in Table 6 we summarized all the obtained results to get insights into the malicious node detection capability on a system-wide level.

Table 6. secGPSR: Gray Hole nodes detection performance

	Gray Hole Nodes				
	5	**10**	**15**	**20**	**25**
TP	84	64	57	52	38
FN	1	1	1	0	0
FP	0	1	3	2	5
TN	2	4	10	11	22

The crucial results that must be emphasized are related to FNs and FPs, especially FNs which represent Gray Hole nodes incorrectly recognized as legitimate ones. As can be noticed in Table 6 while the number of grayhole nodes increases, the number of FNs is negligible. However, the same still holds for FPs which, instead, represent legitimate nodes incorrectly detected as grayhole. These results shed light on the capability of the secGPSR to accurately thwart the Gray Hole attack.

doi:10.20944/preprints202312.0718.v1

5.3. secGPSR: Combined Attack Sybil and Gray Hole

The combination of the two considered attacks is provided in this section. The simulation results in which both Sybil and Gray Hole attacks are considered are shown in Tables 7 and 8 taking into account the proposed mitigation mechanism.

Table 7. GPSR: Gray Hole and Sybil attacks.

Hosts Number	Gray Hole Number	Sybil Number	Sent Packets	Received Packets	PTR (%)
50	0	0	636	582	91.51
44	3	3	636	560	88.05
40	5	5	636	455	71.54
34	8	8	636	400	62.89
30	10	10	636	321	50.47
24	13	13	636	228	35.06

Table 8. secGPSR: Gray Hole and Sybil attacks with a DR of 0.6.

Hosts Number	Gray Hole Number	Sybil Number	Sent Packets	Received Packets	PTR (%)
50	0	0	636	578	91.19
44	3	3	636	577	90.72
40	5	5	636	575	90.25
34	8	8	636	542	88.05
30	10	10	636	512	82.39
24	13	13	636	359	63.05

As can be noticed, comparing Tables 7 and 8, even when both Sybil and Gray Hole attacks are launched against the GPSR protocol, the proposed mitigation is able to successfully counteract them showing a PTR rate that is almost equal to the cases when only one of the considered attacks is thwarting the system (see Tables 4 and 5). These results prove the scalability of the mitigation to adapt itself to a more complex condition due to a combined and more harmful attack.

5.4. secGPSR Overhead Analysis

In this section, we additionally evaluated the overhead caused by the use of the ECDSA to compute and verify exchanged packets' signatures considering different elliptic curves.

In Figures 6 and 7 can be observed the time needed by the drone that uses the ECDSA. We evaluated the time by varying the used elliptic curve, starting from a curve that uses a 112-bit key till reaching a 256-bit key. The time needed to compute the signature increases with the increasing of the key size, for both generation and verification processes. However, signature verification is more time-consuming due to the complex verification algorithm of the ECDSA as demonstrated in [27,31]. However, the obtained results suggest that 192-bit keys are a good balanced trade-off between security and time needed to generate and verify packets' signatures. Finally, we have to consider that beacons are packets characterized by a limited size (between 60 bytes and 450 bytes) therefore even a 256-bit EC key can be considered since the delay related to the creation of the beacon's signature introduces a negligible delay of $\sim$ 0,0012 seconds and for the beacon's signature verification $\sim$ 0,0035 seconds, which is still negligible. These results prove that this protocol can be secured using not only a more advanced and modern cryptographic primitive, that can provide a higher security degree with respect to traditional DSA but also a cryptographic primitive that offers an optimal trade-off between security degree and computing/resources overhead.

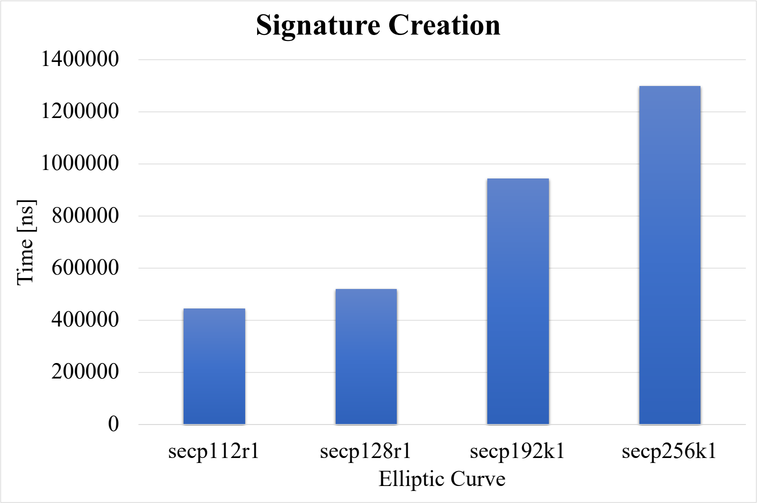

Figure 6. ECDSA: Signature Creation.

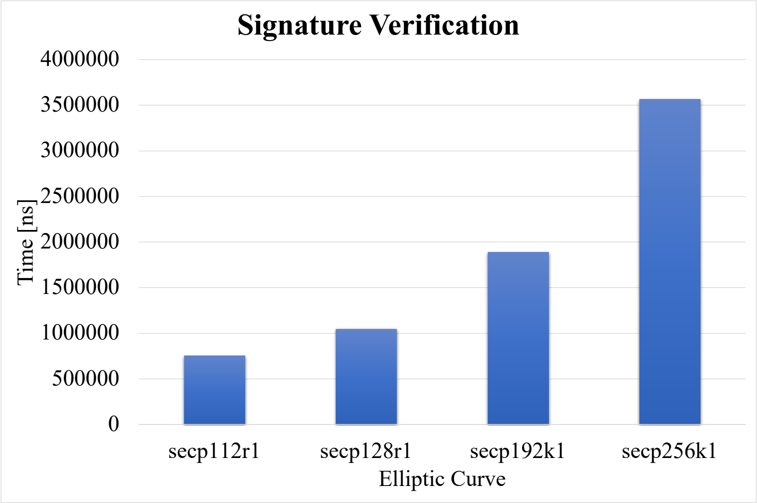

Figure 7. ECDS: Signature Verification.

6. Conclusions

FANET routing protocols are not developed considering security concerns. This lack of security may cause serious damage to FANET communications. Among all the routing attacks in this paper two of the most harmful ones have been considered: Gray Hole and Sybil attacks. For each of them, a specific mitigation has been proposed considering as a routing protocol the GPSR. To detect and counteract the Gray Hole attack a trustiness metric has been introduced in order to effectively detect drones that behave as Gray Hole nodes. In order to mitigate Sybil attacks, the beacon packet of GPSR protocol has been extended with a digital signature generated and verified using the ECDSA in order to guarantee drone authentication. The proposed mitigations have shown effective results in counteracting the aforementioned attacks proving that routing protocols can be securely designed without imposing a huge overhead on the drones.

Author Contributions: Conceptualization, F.D.R., M.T. and M.G.S.; methodology, F.D.R.; software, M.G.S.; validation, F.D.R., M.T., P.S. and A.L.; data curation, M.T. and M.G.S.; writing—original draft preparation, M.T. and M.G.S.; writing—review and editing, M.G.S, F.D.R., M.T., A.L. and P.S.; supervision, F.D.R. and M.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Lagkas, T.; Moscholios, I. A compilation of UAV applications for precision agriculture. *Comput. Netw.* **2020**, *172*, 107148.
2. Tropea, M.; Spina, M.G.; De Rango, F. Supporting Dynamic IDS Deployment with Load Balancing Strategy for SDN-Enabled Drones in Emergency Scenarios. Proceedings of the Int'l ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems; Association for Computing Machinery: New York, NY, USA, 2023; MSWiM '23, p. 297–300. https://doi.org/10.1145/3616388.3617549.
3. Tropea, M.; Spina, M.G.; De Rango, F. SDN-driven Dynamic Deployment of IDS with Load Balancing for Drones in Emergency Scenarios. 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 2023, pp. 1–6. https://doi.org/10.1109/ICT-DM58371.2023.10286918.
4. Pasandideh, F.; da Costa, J.P.J.; Kunst, R.; Islam, N.; Hardjawana, W.; Pignaton de Freitas, E. A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies. *Remote. Sens.* **2022**, *14*, 4459.
5. Oubbati, O.S.; Chaib, N.; Lakas, A.; Lorenz, P.; Rachedi, A. UAV-assisted supporting services connectivity in urban VANETs. *IEEE Transactions on Vehicular Technology* **2019**, *68*, 3944–3951.
6. Tropea, M.; Fazio, P.; De Rango, F.; Cordeschi, N. A new fanet simulator for managing drone networks and providing dynamic connectivity. *Electronics* **2020**, *9*, 543.
7. Amponis, G.; Lagkas, T.; Sarigiannidis, P.; Vitsas, V.; Fouliras, P.; Wan, S. A survey on FANET routing from a cross-layer design perspective. *J. Syst. Archit.* **2021**, *120*, 102281.
8. De Rango, F.; Tropea, M.; Fazio, P. Bio-inspired routing over fanet in emergency situations to support multimedia traffic. Proceedings of the ACM MobiHoc workshop on innovative aerial communication solutions for FIrst REsponders network in emergency scenarios, 2019, pp. 12–17.
9. Karp, B.; Kung, H.T. GPSR: Greedy perimeter stateless routing for wireless networks. Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, pp. 243–254.
10. Oubbati, O.S.; Lakas, A.; Zhou, F.; Güneş, M.; Yagoubi, M.B. A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs). *Veh. Commun.* **2017**, *10*, 29–56.
11. Lin, C.; He, D.; Kumar, N.; Choo, K.K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69.
12. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218.
13. Jasim, K.S.; Alheeti, K.M.A.; Alaloosy, A.K.A.N. A review paper on secure communications in FANET. 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI). IEEE, 2021, pp. 1–7.
14. Kumar, C.; Mohanty, S. Current trends in cyber security for drones. 2021 International Carnahan Conference on Security Technology (ICCST). IEEE, 2021, pp. 1–5.
15. Yang, W.; Wang, S.; Yin, X.; Wang, X.; Hu, J. A review on security issues and solutions of the Internet of Drones. *IEEE Open J. Comput. Soc.* **2022**.
16. Tsao, K.Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Netw.* **2022**, *133*, 102894.
17. Tangade, S.; Kumaar, R.A.; Malavika, S.; Monisha, S.; Azam, F. Detection of Malicious Nodes in Flying Ad-hoc Network with Supervised Machine Learning. 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE). IEEE, 2022, pp. 1–5.
18. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2802–2832.
19. Remya Krishnan, P.; Arun Raj Kumar, P. Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping. *Wirel. Pers. Commun.* **2022**, pp. 1–36.
20. Younas, S.; Rehman, F.; Maqsood, T.; Mustafa, S.; Akhunzada, A.; Gani, A. Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs. *Appl. Sci.* **2022**, *12*, 12448.
21. Hamdan, S.; Hudaib, A.; Awajan, A. Detecting Sybil attacks in vehicular ad hoc networks. *Int. J. Parallel, Emergent Distrib. Syst.* **2021**, *36*, 69–79.

22. Cui, Y.; Zhang, Q.; Feng, Z.; Li, X.; Wei, Z.; Zhang, P. Seeing is Believing: Detecting Sybil Attack in FANET by Matching Visual and Auditory Domains. *arXiv* **2023**, arXiv:2306.16339.
23. Aissaoui, R.; Deneuville, J.C.; Guerber, C.; Pirovano, A. A survey on cryptographic methods to secure communications for UAV traffic management. *Veh. Commun.* **2023**, p. 100661.
24. Ren, S.; Li, D.; Hu, Q.; Liu, Y.; Liu, J. An Improved Security OLSR Protocol against Black Hole Attack based on FANET. 2022 13th Asian Control Conference (ASCC). IEEE, 2022, pp. 383–388.
25. Zhou, Y.; Zhichao, M.; Wang, H.; Lu, Y.; Tian, Y. SZLS-GPSR: UAV Geographic Location Routing Protocol Based on Link Stability of Communication Safe Zone. 2023 15th International Conference on Computer Research and Development (ICCRD). IEEE, 2023, pp. 258–267.
26. Klima, K. *Cryptology:Classical and Modern*; Taylor & Francis: Andover, England, UK, 2018. https://doi.org/10.1201/9781315170664.
27. *Guide to Elliptic Curve Cryptography*; Springer-Verlag, 2004. https://doi.org/10.1007/b97644.
28. Barker, E. *Recommendation for key management*; 2020. https://doi.org/10.6028/nist.sp.800-57pt1r5.
29. Shanmuganathan, V.; Anand, T. A survey on gray hole attack in manet. *IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC)* **2012**, *2*.
30. De Rango, F.; Palmieri, N.; Tropea, M.; Potrino, G. UAVs Team and Its Application in Agriculture: A Simulation Environment. *Simultech* **2017**, *2017*, 374–379.
31. Imem, A.A. Comparison and evaluation of digital signature schemes employed in ndn network. *arXiv* **2015**, https://doi.org/10.48550/arXiv.1508.00184.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.