

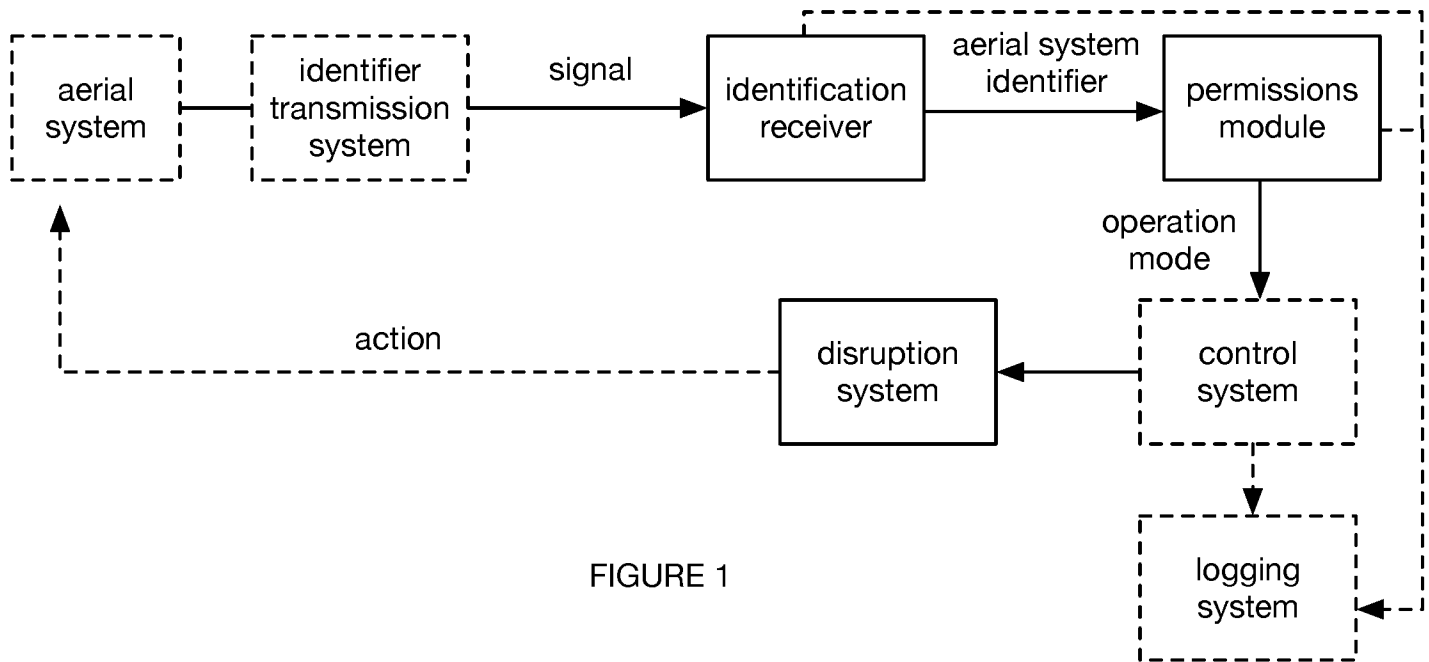


FIGURE 1

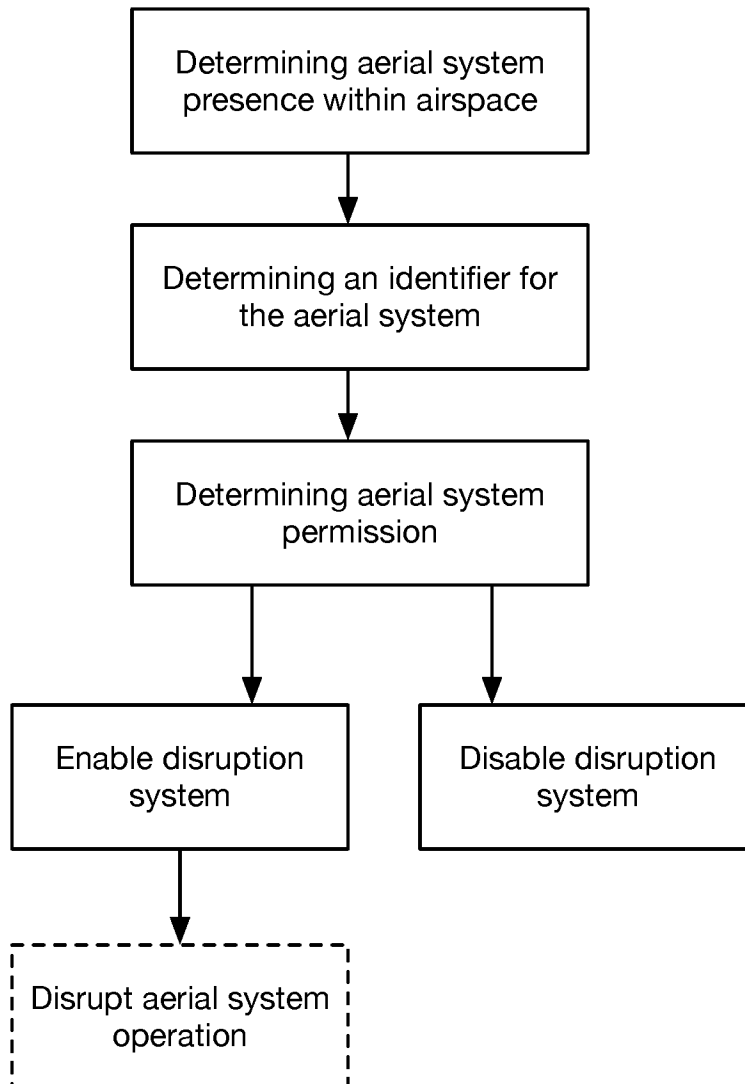


FIGURE 2

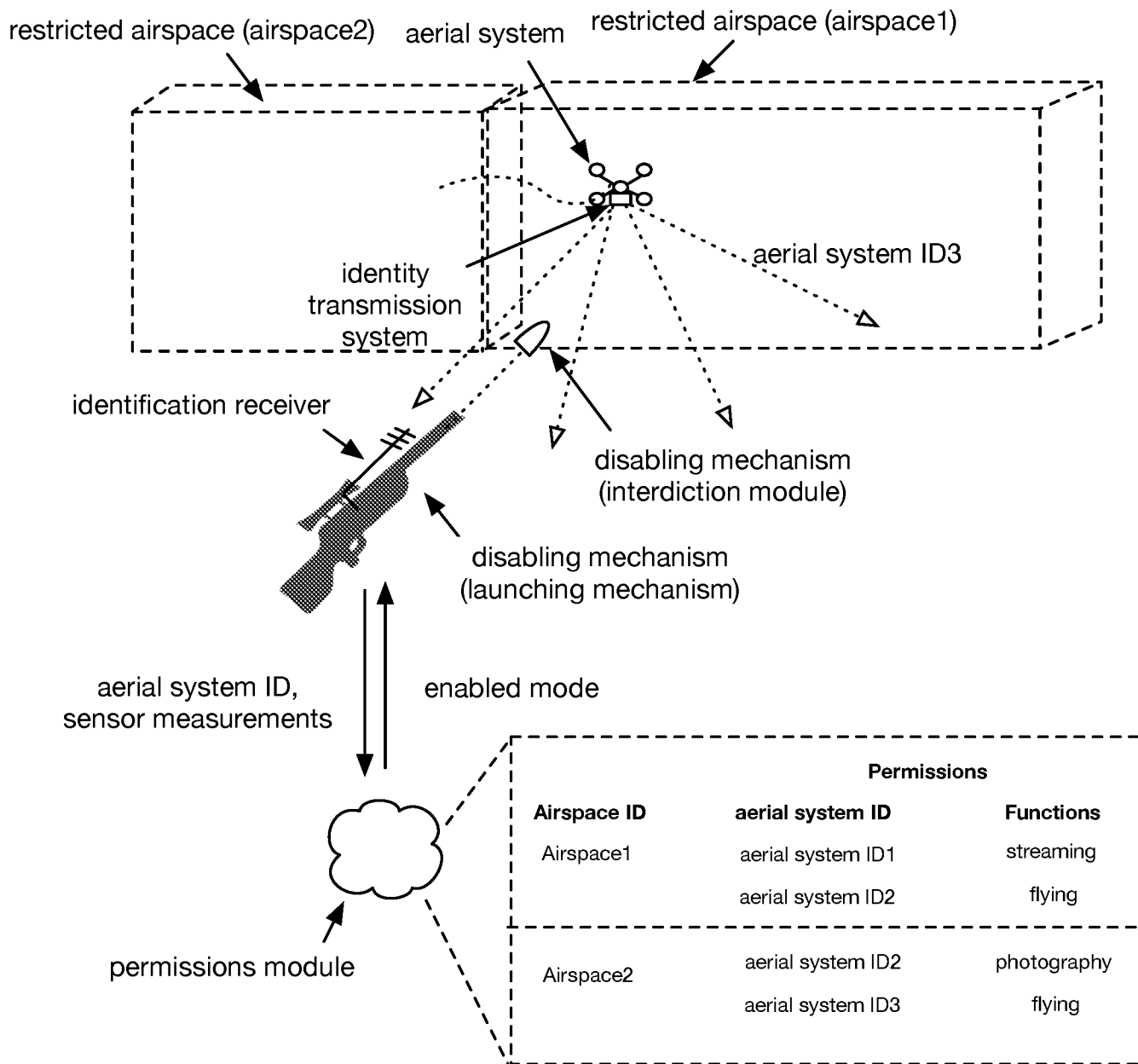


FIGURE 3

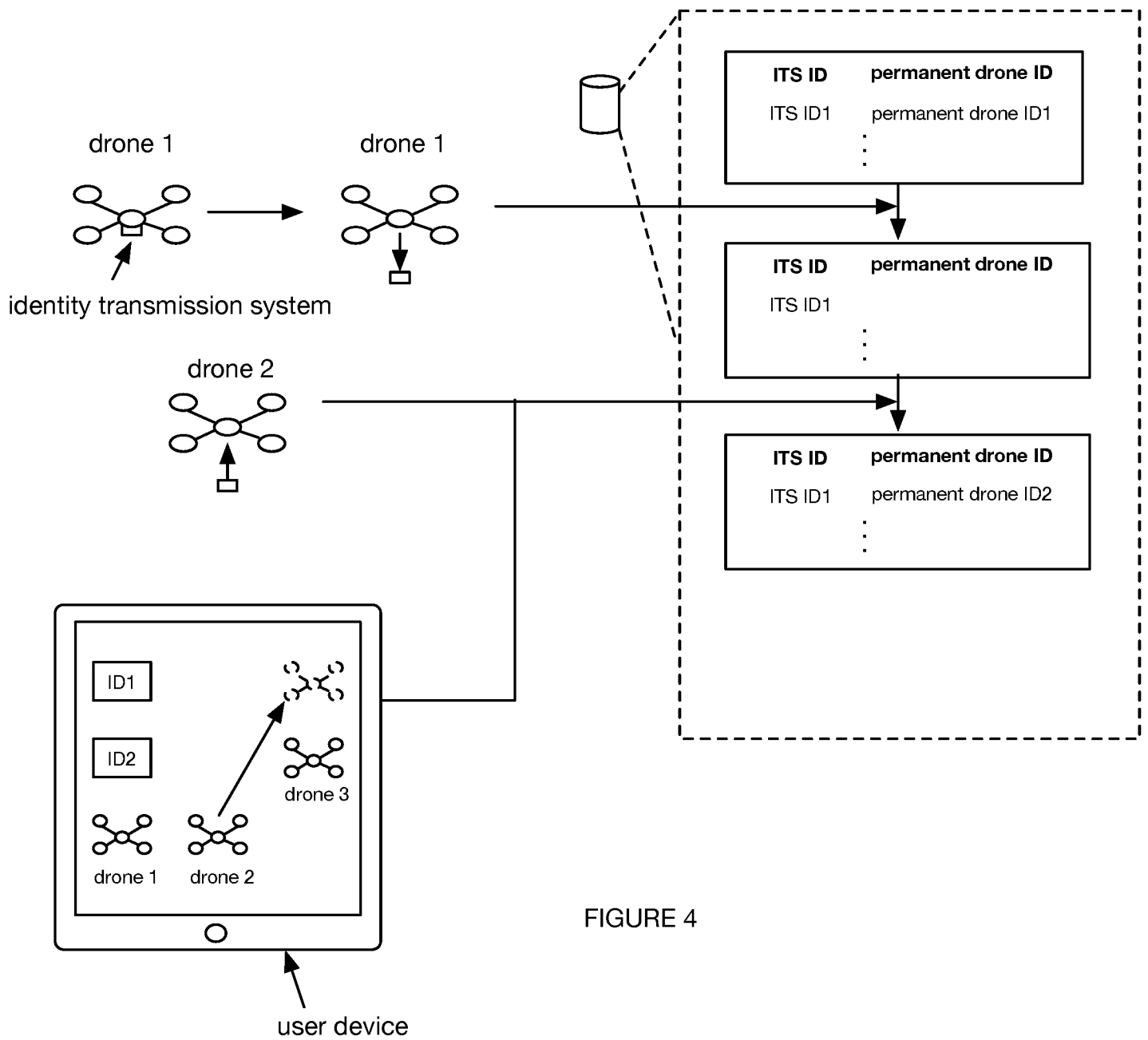


FIGURE 4

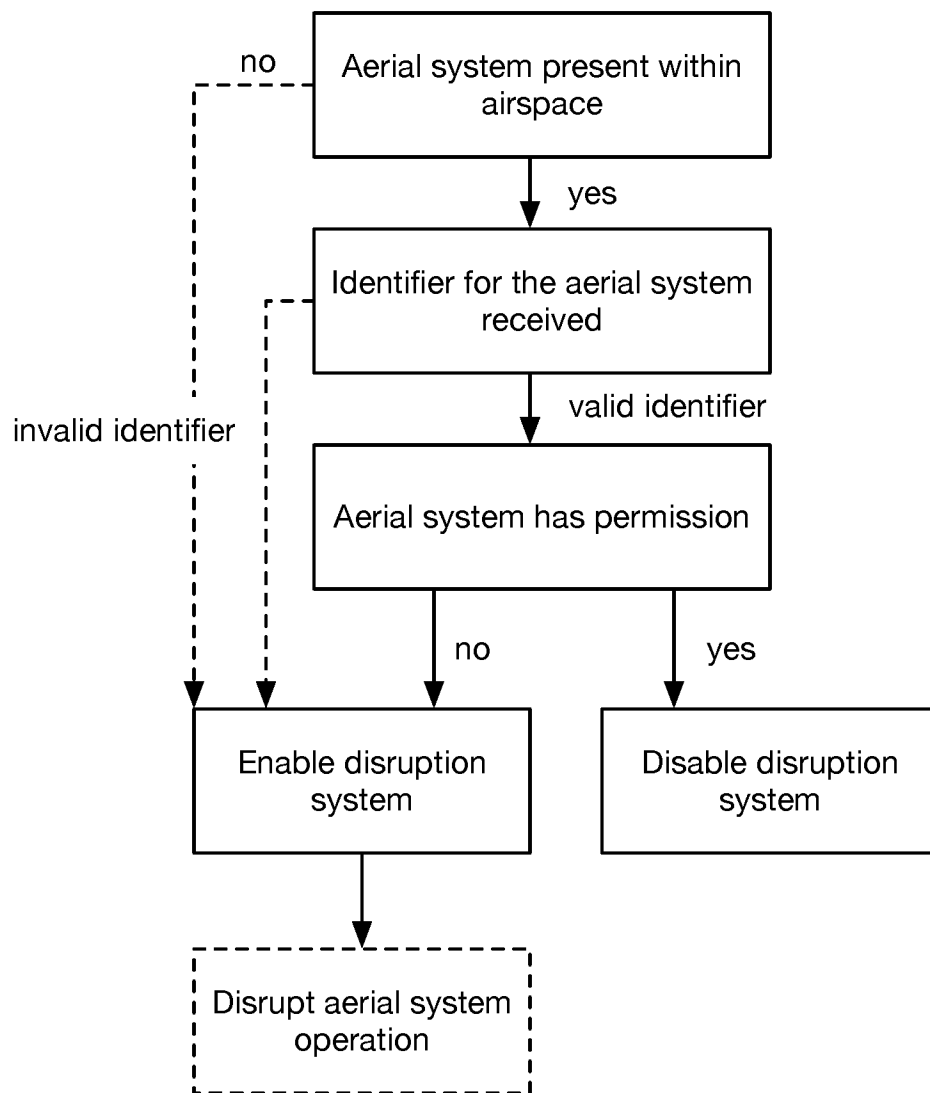


FIGURE 5

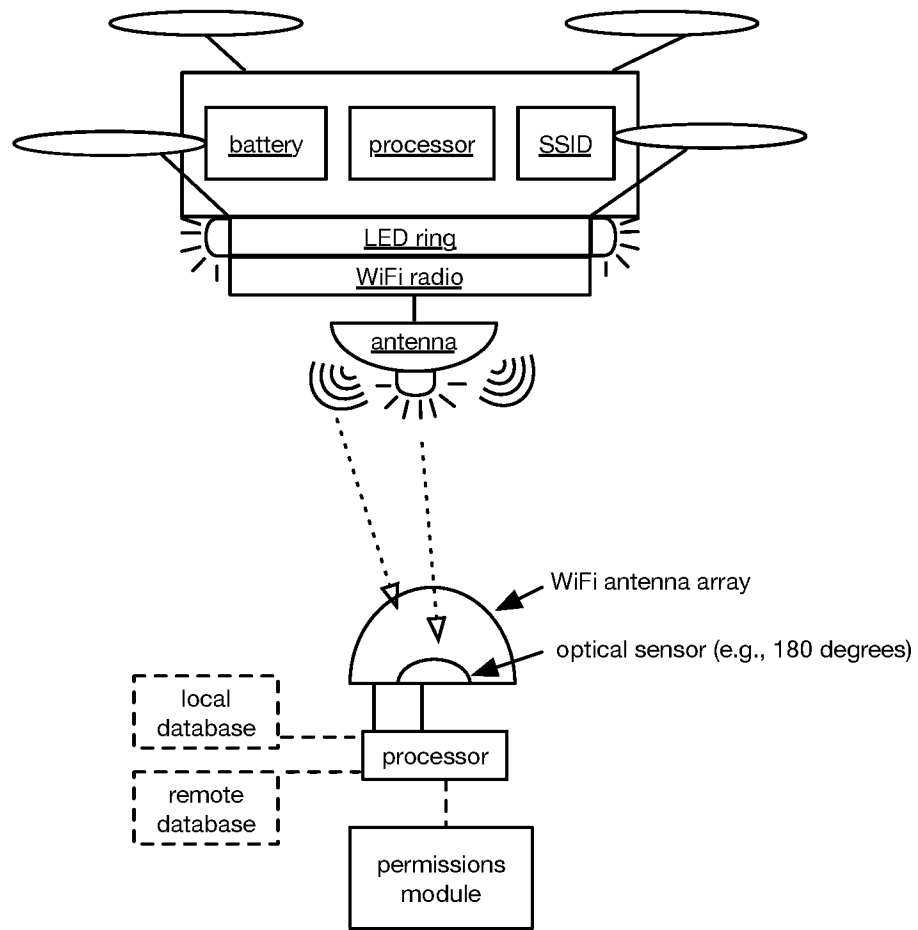


FIGURE 6

SYSTEM AND METHOD FOR AERIAL SYSTEM DISCRIMINATION AND ACTION

TECHNICAL FIELD

[0001] This invention relates generally to the aeronautics field, and more specifically to a new and useful aviation discrimination and action system and method in the avionics field.

BACKGROUND

[0002] With the increased popularity of commercial unmanned aerial vehicles (UAVs), airspace traffic has been increasing at an unprecedented rate. This increased traffic raises the need to: monitor airspace for the presence of UAVs, distinguish authorized from unauthorized UAVs, prevent unauthorized UAVs from entering restricted airspace, and/or selectively remove unauthorized UAVs from the airspace.

[0003] However, monitoring, preventing, and/or removing unauthorized UAVs from restricted airspace can be difficult when authorized UAVs are concurrently within the airspace. Conventional UAV prevention and/or removal systems are global and incapable of distinguishing between authorized and unauthorized UAVs. Manual UAV prevention and/or removal systems are also inadequate because unauthorized UAVs are difficult to visually distinguish from authorized UAVs.

[0004] Thus, there is a need in the aerospace field to create a new and useful aerial system discrimination system for selective removal from and/or permission into the airspace.

BRIEF DESCRIPTION OF THE FIGURES

[0005] FIGURE 1 is a schematic representation of the aerial system discrimination system.

[0006] FIGURE 2 is a schematic representation of the method of aerial system discrimination.

[0007] FIGURE 3 is an example of discrimination system operation.

[0008] FIGURE 4 is an example of identity transmission system reassignment.

[0009] FIGURE 5 is a schematic representation of a variation of the method.

[0010] FIGURE 6 is a specific example of an aerial system and detection system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0011] The following description of the preferred embodiments of the invention is not intended to limit the invention to these preferred embodiments, but rather to enable any person skilled in the art to make and use this invention.

1. Overview

[0012] As shown in FIGURE 1, the aerial system discrimination system includes an aerial system disruption system, an aerial system identification system, and a

permissions module. The discrimination system can additionally include or use an identifier transmission system configured to mount to the aerial system. The discrimination system functions to determine whether an aerial system is authorized or unauthorized to be in the airspace. The discrimination system can additionally function to prevent, disrupt, remove, or otherwise interact with an unauthorized aerial system within the airspace.

[0013] In a specific example, the discrimination system includes: a disruption system including a launcher and an interdiction module; an identification system including a radio; and a permissions module connected to the radio. In operation, the radio receives a UAV identifier, broadcast from a UAV. The UAV identifier is checked against the permissions module, which determines whether the UAV identifier is associated with an authorized or unauthorized UAV. The disruption system can be automatically disabled (e.g., locked) in response to determination that the UAV is authorized, and/or automatically activated (e.g., unlocked) in response to determination that the UAV is unauthorized (e.g., reporting an unauthorized identifier, not reporting an identifier, etc.). When the disruption system is in an unlocked state, the launcher can launch the interdiction module toward the UAV, wherein the interdiction module can immobilize the motive mechanism of the aerial system (e.g., by disabling the power system, entangling the motive mechanism, etc.). The identification system optionally includes a set of sensors (e.g., radar, microphone, etc.), wherein the identification system detects the presence of a UAV within a predetermined airspace based on one or more measurements from the sensors. In response to UAV detection, the discrimination

system can: activate the radio for UAV identifier receipt; aim the launcher and/or interdiction module toward the UAV based on the sensor measurements; and/or perform any other suitable functionality. The discrimination system can additionally selectively activate (e.g., unlock) the disruption system when a UAV without a UAV identifier is detected (e.g., wherein the disruption system is activated response to the absence of a UAV identifier).

2. Benefits

[0014] The discrimination system can confer several benefits. First, the discrimination system can discriminate between authorized and unauthorized aerial systems. This enables the discrimination system to treat authorized aerial systems differently from unauthorized aerial systems (e.g., leave alone vs. interdict, respectively). Second, in some variations, the identifier transmission system includes a radio chipset (e.g., WiFi chipset), which broadcasts the aerial system identifier over a long geographic distance. Third, in some variations, the aerial system identifier can be refreshed at a predetermined frequency, wherein the identification system can record and identify the aerial system based on the time-ordered series of broadcast identifiers. This can function to prevent identifier tampering and/or reproduction. Fourth, in some variations, the aerial system can include a first and second identifier, transmitted by a first and second identifier transmission system, respectively, wherein the second identifier can function as a backup identifier (e.g., in case the primary identifier transmission system is inoperable), a second factor identifier for the aerial system (e.g.,

as a secondary authenticator for the aerial system to prevent tampering and/or identifier reproduction), an identifier for a secondary identification system (e.g., a user device-compatible identifier), or be used in any other suitable manner. In one example, the first identifier transmission system can be a WiFi chipset, while the second identifier transmission system can be an optical signal generator (e.g., a blinking LED). However, the discrimination system can confer any other suitable benefit. Fifth, in some variations, the discrimination system can selectively route and/or treat aerial systems proximal or within the airspace based on the respective identifier.

[0015] This discrimination system can additionally assuage user concerns. From an aerial system owner's perspective, the discrimination system can allow the owner to gain access to restricted airspace to record rare content; prevent the owner from losing the drone; and enable the owner to easily comply with aerial system regulations (e.g., registration). From the restricted airspace entity's perspective, the discrimination system can enable the entity to selectively permit aerial systems into their airspace (e.g., monetize access to airspace), monitor which aerial systems are within their airspace (e.g., prevent liability), and control release of content generated from physical regions associated with the airspace (e.g., control which drones can record footage of sporting events within an arena). However, the discrimination system can confer any other suitable set of benefits.

3. *Auxiliary systems*

[0016] All or part of the discrimination system is preferably used with an aerial system. An aerial system is preferably an aircraft (e.g., a manned or unmanned aircraft), but can alternatively or additionally be a terrestrial system, aquatic system, or be any other suitable system. Examples of aerial systems include gliders, rotorcraft, human-powered aircraft (HPA), unmanned aerial vehicles (UAVs), planes, drones, or any other suitable aerial system. The aerial system can be automatically controlled, manually controlled (e.g. by a remote control), or otherwise controlled.

[0017] The aerial system is preferably associated with an aerial system identifier, but can alternatively be unidentified. The aerial system identifier can be that transmitted by the identifier transmission system, be a permanent identifier for the aerial system (e.g., a manufacturer-assigned identifier), or can be a different identifier. The aerial system identifier can be static (e.g., predetermined) or dynamic (e.g., periodically generated). The aerial system identifier can be automatically generated (e.g., by the aerial system, by a manufacturer, etc.), manually generated, or otherwise generated. The aerial system identifier can be automatically: selected, calculated (e.g., based on an on-board equation, remotely stored equation, etc.), or otherwise determined. The aerial system identifier can be globally unique, locally unique (e.g., to a geographic location, to an aerial system manufacturer or type, etc.), or generic. The aerial system identifier can additionally be associated with an entity, location, or any other suitable parameter.

[0018] The disruption system is preferably used to monitor restricted airspace. The restricted airspace is preferably a physical volume defined by a geographic region and altitude, but can alternatively be otherwise defined. The geographic region can be defined by a set of geographic coordinates (e.g., latitude and longitude), a place name (e.g., county, city, landmark, intersection, etc.), a physical street address, distance from a given location, a specified radius from a given location, a graphical depiction on a map, a geofence, a dynamic geographic region (e.g., that changes based on time of day, weather, etc.) or any other suitable location expression. The altitude can be a distance from the ground, be a range of distances from the ground, be an absolute altitude (e.g., from sea level), or be otherwise defined. The restricted airspace can be automatically defined or manually defined. For example, the geographic region and/or altitude can be predetermined, received from a user (e.g., from a user device), or otherwise determined. The restricted airspace is preferably associated with an entity, airspace identifier, or any other suitable parameter.

[0019] The restricted airspace is preferably associated with a set authorized aerial system identifiers (e.g., a whitelist), but can alternatively or additionally be associated with a set of unauthorized aerial system identifiers (e.g., a blacklist). One or more of the aerial system identifiers can be associated with one or more aerial system permissions. The permissions can include: temporal limitations (e.g., permitted only from 10:30a to 11a), geographic limitations (e.g., permitted above a first geographic region, not permitted above a second geographic region), altitude limitations (e.g., permitted only between 100ft – 200ft above the stadium), aerial system entity limitations (e.g., only

aerial systems associated with listed entities are permitted), aerial system type, function (e.g., data streaming prohibited, data streaming permitted, permitted emission types, etc.), predicted behavior (e.g., predicted travel path, predicted endpoint, etc.), or any other suitable set of permissions. The set of authorized aerial system identifiers and/or associated permissions is preferably determined by the restricted airspace entity, but can alternatively be otherwise defined.

4. *System.*

[0020] The disruption system of the discrimination system functions to disrupt aerial system movement. The disruption system is preferably an active system, but can alternatively be a passive system. The disruption system can be a manual system, automatic system, or be otherwise controlled. The disruption system can be a handheld system, ground-based system, an aerial system, or have any other suitable form factor. The disruption system is preferably associated with and/or controlled by the entity associated with the restricted airspace, but can alternatively be associated with any other suitable entity. A restricted airspace can be associated with one or more disruption systems of the same or different kind.

[0021] In one variation, the disruption system can include a launching system and an interdiction module, which cooperatively function to intercept, then interdict, the aerial system (example shown in FIGURE 3). However, the disruption system can include a jamming system, an electromagnetic disruption system, a buckshot system

(e.g., a system that fires buckshot), an ablation system, or any other suitable mechanism capable of interfering with aerial system operation.

[0022] The launching system of the disruption system functions to propel the interdiction module. The launching mechanism preferably propels the interdiction module into or proximal the restricted airspace, but can alternatively or additionally propel the interdiction module into a physical region proximal the target aerial system (e.g., within a predetermined radius of the target, such as within 100ft), propel the interdiction module into the target, or propel the interdiction module to any other suitable physical endpoint. Examples of the launching system include: a gun, a cannon, a catapult, a shoulder-based launcher (e.g., a t-shirt launcher, missile launcher, etc.), a second aerial system, or any other suitable launching system. The launching system can include an aiming mechanism that functions to guide or determine the interdiction module travel path after egress. Examples of the aiming mechanism include an elongated barrel (e.g., wherein the interdiction module travels along the barrel length to egress), a gun sight, an active guidance system (e.g., a laser that paints the target, wherein the interdiction module is propelled toward the painted target, a radar-guided system, camera-guided system, remote controlled system), or any other suitable aiming system. The launching system can additionally include a firing mechanism that functions to propel the interdiction module out the launching system. Examples of the firing mechanism include: combustible material (e.g., gunpowder), compressed gas (e.g., a gas canister), a rail gun, an electromagnet, or any other suitable firing mechanism capable of imparting a propulsion force on the interdiction module.

[0023] The interdiction mechanism of the disruption system functions to interfere with aerial system traversal through airspace. The interdiction mechanism preferably interferes with aerial system motive mechanism operation, but can additionally or alternatively interfere with the aerial system electronics and controls, disrupt the electrical connections between the control system and the motive mechanism (e.g., shorting the electrical connections, physically disconnecting the connections by explosion, etc.), or otherwise interfere with any other suitable aerial system component to disrupt aerial system traversal through airspace.

[0024] In a first variation, the interdiction module includes a net that entangles the aerial system motive mechanism. The net, when unfurled, can be substantially planar, parabolic, or have any other suitable configuration. The net can include secondary filaments extending from the net broad face (e.g., wherein the secondary filaments are sucked into the motive mechanism), include a cinching mechanism (e.g., a line slidably extending through the net perimeter, magnets, adhesive, etc.), or include any other suitable component. However, the net can have any other suitable construction (e.g., be a set of filaments). In this variation, the net can be part of a single-stage system that is directly fired from the launching mechanism. Alternatively, the net can be part of a two-stage system, wherein the net is encapsulated within an airframe. The airframe is launched from the launching mechanism, and the net is subsequently launched from the airframe while the airframe is in flight. However, the net can be otherwise propelled toward the target.

[0025] In a second variation, the interdiction module includes a set of masses (e.g., bullets) that physically intercept the aerial system motive mechanism and/or electronics. The set of masses can include a single mass (e.g., one bullet), a plurality of masses (e.g., birdshot), or any other suitable number of masses. The masses can be part of a single-stage system that is directly fired from the launching mechanism. Alternatively, the masses can be part of a two-stage system, wherein the masses are encapsulated within a casing, the casing is launched from the launching mechanism, and the masses are propelled out of the casing while the casing is in flight. However, the masses can be otherwise propelled toward the target.

[0026] In a third variation, the interdiction module includes collated light (e.g., a laser) that physically intercepts and burns the aerial system motive mechanism and/or electronics. The interdiction module can include a single light source, multiple light sources (concurrently or asynchronously operated), or any suitable number of light sources arranged in any suitable configuration. The light sources can be part of a single-stage system, wherein the light sources are mounted to and/or function as the firing mechanism. Alternatively, the light sources can be part of a two-stage system, wherein the light sources are encapsulated within a casing, the casing is launched from the launching mechanism, and the light sources emit light out of the casing while the casing is in flight. However, the light can be otherwise directed toward the target.

[0027] In a fourth variation, the interdiction module includes an electromagnetic signal that disrupts avionics system data transmission, data receipt, and/or electronics operation. The interdiction module can include a single electromagnetic wave generator,

multiple electromagnetic wave generator (concurrently or asynchronously operated), or any suitable number of electromagnetic wave generator arranged in any suitable configuration. The electromagnetic wave generators can be part of a single-stage system, wherein the electromagnetic wave generators are mounted to and/or function as the firing mechanism. Alternatively, the light sources can be part of a two-stage system, wherein the electromagnetic wave generators are encapsulated within a casing, the casing is launched from the launching mechanism, and the electromagnetic wave generators emit electromagnetic waves out of the casing while the casing is in flight. However, the electromagnetic waves can be otherwise directed toward the target.

[0028] However, the interdiction module can include any other suitable component capable of disrupting aerial system operation.

[0029] The identification system of the discrimination system functions to receive the aerial system identifier from the aerial system. Additionally or alternatively, the identification system can function to detect the presence of a UAV within a physical volume. The identification system is preferably mounted to the disruption system, more preferably the launching mechanism, but can alternatively be mounted to the interdiction system, a secondary mounting point (e.g., building, second aerial system, ground, etc.), or any other suitable mounting point. Alternatively, the identification system can be part of a secondary system, such as a user device (e.g., a smartphone, tablet, etc.).

[0030] The identification system can include an identification receiver, which functions to receive the aerial system identifier. The identification receiver can be

passive (e.g., receive information broadcast by the aerial system), active (e.g., be powered, request information from and/or provide power for information broadcast by the aerial system), or be otherwise configured.

[0031] In a first variation, the identification receiver is a radio including an antenna array and chipset (example shown in FIGURE 3), but can alternatively include any other suitable component. The antenna array of the identification receiver functions to receive the broadcast signal. The antenna array can include one or more antennas. The antenna is preferably mounted to the disruption mechanism, but can alternatively be mounted to any other suitable mounting point. In one variation, the antenna can be external and extend perpendicular the launching mechanism longitudinal axis. In a second variation, the antenna can extend parallel the launching mechanism longitudinal axis. In a specific example, the antenna can be embedded along the length of the launching mechanism. However, the identification receiver can be otherwise arranged relative to the disruption mechanism. In a third variation, the antenna is separate from the disruption mechanism. The antenna can be a directional antenna, omnidirectional antenna, or be any other suitable antenna. Examples of the antenna include: a Yagi-Uda antenna, a log-periodic antenna, a corner reflector antenna, or any other suitable antenna.

[0032] The chipset of the identification receiver functions to interpret the received signal. The chipset preferably interprets the signal into the aerial system identifier (e.g., decrypts the signal, etc.), but can alternatively interpret the signal into a set of data indicative of the identifier, or otherwise interpret the signal. The chipset can

function as a receiver only, transceiver, or perform any other suitable functionality. The chipset is preferably electrically connected to the antenna, but can alternatively be otherwise connected to the antenna. The chipset can be connected to the permissions module, wherein the chipset sends the raw or processed signal to the permissions module for permissions determination. However, the chipset can include the permissions module or communicate the signal to any other suitable endpoint.

[0033] In a second variation, the identification receiver includes a signal receiver that functions to read the aerial system identifier off the aerial system from signals reflected off or emitted by the aerial system. The identification receiver can include one or more signal receivers of the same or different type, operated concurrently or asynchronously). The signal receiver can record one or more measurements (e.g., frames), wherein the aerial system identifier can be read from a single measurement, from a plurality of measurements (e.g., a time-ordered set of frames, mosaiced frames, etc.), or from any other suitable number of measurements. When the identification receiver is mounted to the disruption mechanism, the signal receiver is preferably arranged such that the field of measurement (e.g., field of view) is substantially coincident with the aiming mechanism of the disruption mechanism. However, the signal receiver can be otherwise arranged.

[0034] The signal receiver can be: an optical sensor, acoustic sensor, an electromagnetic wave receiver, or be any other suitable sensor. The optical sensor can be a CCD camera, CMOS camera, multispectral camera, hyperspectral camera, stereoscopic camera, thermal camera, IR camera, or be any other suitable camera. The acoustic

sensor can be a sonar receiver, an ultrasound receiver, microphone, array of microphones, or be any other suitable acoustic sensor. The electromagnetic wave receiver can be: a radar system, a microwave receiver, or be any other suitable electromagnetic wave receiver.

[0035] In this variation, the identification receiver can additionally include a signal-emitting element that functions to emit a signal read by the camera. In operation, the emitted signal is directed toward the aerial system, the aerial system identifier reflects the signal, and the identification receiver reads the reflected signal. In one example, the emitted signal can read a visual indicator (e.g., a barcode, flashing light, etc.) from the aerial system. The signal-emitting element can be: a light source (e.g., white light, spotlight, laser, etc.), an acoustic source (e.g., ultrasound source, 3m acoustic wave source, etc.), an electromagnetic wave source (e.g., radio wave source), or be any other suitable element capable of emitting a signal. The signal-emitting element can emit a directional signal, omnidirectional signal, or any other suitable signal. In one variation, the signal is directed along a portion of the firing path, such that the signal emitted by signal emitting element hits the target when the disruption system is aimed at the target. However, the identification reader can include any other suitable component capable of reading or otherwise receiving the aerial system identifier.

[0036] When the identification reader is active, the identification reader can additionally include or be connected to a power source that powers the identification reader or components thereof. The power source can be a generator, a battery (e.g., a secondary battery, primary battery), power grid, or any other suitable power source.

When the identification reader is mounted to a mobile mounting point (e.g., the disruption system, second aerial system, etc.), the identification reader can be tethered to the power source by a wire, carry the power source onboard, or otherwise access the power source.

[0037] The identification receiver can additionally include a set of sensors, wherein the sensor measurements can be used to: detect the presence of an aerial system within a physical volume (e.g., detect aerial system proximity), refine disruption system aim (e.g., triangulate aerial system location within the volume), guide the disruption system toward the aerial system, generate secondary information about the physical volume, locate the disruption system, or perform any other suitable functionality. In one example of disruption system operation, aerial system presence within the physical volume is detected based on the sensor measurements, the identification reader is turned on in response to aerial system detection, and the identification reader reads the aerial system identifier (or determines the lack thereof) from the aerial system. However, the sensors can be otherwise used.

[0038] The sensors are preferably arranged on the disruption system, more preferably the launching mechanism but alternatively the interdiction mechanism, but can alternatively be arranged on any other suitable component. The sensors can include: audio sensors, optical sensors, electromagnetic wave receivers, location sensors (e.g., GPS system, trilateration system, accelerometer, gyroscope, altimeter, etc.), or any other suitable sensor. The sensors can be the same sensors as that of the identification reader, the same type of sensors as that of the identification reader, different sensors from that

of the identification reader, or be any other suitable sensor. In a first example, the sensors can include radar or sonar that function to identify aerial system presence in the volume. In a second example, the sensors can include audio sensors that are sensitive at the frequencies of the aerial system motors and rotors, which can function to differentiate aerial systems from birds, balloons, or other aerial elements (e.g., due to the different acoustic signature). In a third example, the sensors can include thermal sensors, which can function to differentiate aerial systems from birds, balloons, or other aerial elements (e.g., due to the different thermal pattern). However, the identification receiver can include any other suitable set of sensors.

[0039] Sensor measurements can be provided to an aerial system identification module, which functions to determine whether an aerial system is within the physical volume. The aerial system identification module can additionally function to determine one or more parameters of the aerial system (e.g., aerial system type, class, etc.). The sensor measurements provided to the aerial system identification module can include: a single sensor measurement from a single sensor; a stream of sensor measurements from a single sensor (e.g., wherein the aerial system is identified from the stream); a single sensor measurement from each of a plurality of sensors, taken at substantially the same time or within a predetermined time duration of each other; a stream of sensor measurements from each of a plurality of sensors (e.g., wherein aerial system is identified from a combination of all the streams); or any other suitable set of sensor measurements. The aerial system identification module is preferably a dynamic model that is updated with each new aerial system identification, but can alternatively be a

substantially static model. The model is preferably developed using machine learning techniques, but can be otherwise developed. The aerial system identification module can use supervised learning (e.g., using logistic regression, using back propagation neural networks, using random forests, decision trees, etc.), unsupervised learning (e.g., using an Apriori algorithm, using K-means clustering), semi-supervised learning, reinforcement learning (e.g., using a Q-learning algorithm, using temporal difference learning), or any other suitable learning style. The aerial system identification module is preferably a classification module (e.g., classifies the target as an aerial system or non-aerial system), but can alternatively be a regression module (e.g., calculate a probability of the target being an aerial system), or be any other suitable module. The aerial system identification module can be a probabilistic module, heuristic module, deterministic module, or be any other suitable module leveraging any other suitable computation method, machine learning method, or combination thereof.

[0040] The permissions module of the discrimination system functions to store permissions for the physical volume and/or individual aerial systems (example shown in FIGURE 3). The permissions module can additionally function to determine whether the aerial system has permission for a physical volume (e.g., restricted airspace), and/or generate operation permissions for the disruption mechanism based on whether the aerial system identifier is permitted. The permissions module is preferably connected to, and receives information from, the identification receiver, but can alternatively be connected to the disruption module or any other suitable component. The permissions module can be: storage on-board the disruption module, storage on-board the

identification receiver, a remote computing system connected to the disruption module (e.g., wherein the aerial system identifiers are sent to, and firing permissions are received from, the remote computing system), or be any other suitable computing system. In a first example, all disruption systems are connected to a common permissions module. In a second example, each disruption system is associated with a different permissions module, wherein the permissions for the airspace associated with the respective disruption system are updated for the permissions module associated with that disruption system. However, the permissions module can be otherwise maintained. The permissions module can be shared across one or more airspace entities, discrimination systems, identification receivers, aerial system identifiers, or otherwise shared. Alternatively, the permissions module can be specific to an airspace entity, discrimination system, identification receiver, aerial system identifier, or any other suitable population.

[0041] The permissions module preferably stores the access permissions for an airspace identifier identifying a physical volume (e.g., predetermined airspace). The stored access permissions can include permitted and/or excluded: aerial system entities (and associated aerial system identifiers), aerial system identifiers, physical volumes associated with each aerial system identifier or set thereof (e.g., parameters defining the physical volume, such as a geofence, altitude range, etc.), functions associated with each aerial system identifier or set thereof (e.g., streaming media, recording images, delivery, etc.), physical endpoints associated with each aerial system identifier or set thereof, or any other suitable parameter. The access permissions can be: received from and/or

updated by a third party (e.g., that provides the disruption mechanism), a user account associated with the geographic region, an automatic system (e.g., wherein an aerial system entity or identifier is automatically removed from a permitted list or added to restricted list in response to nonpayment of a subscription, non-registration, etc.), or be otherwise determined.

[0042] The discrimination system can additionally include a control system that functions to selectively activate or deactivate disruption system operation. The control system can additionally or alternatively control an auxiliary system based on whether the aerial system is permitted within the airspace. The control system is preferably connected to the disruption system, more preferably to the launching mechanism but alternatively the interdiction module, but can additionally or alternatively be connected to any other suitable component. The control system is preferably operable between a locked and unlocked mode, but can alternatively be operable between any other suitable modes. The control system preferably locks or otherwise disables disruption system operation in the locked mode, and unlocks or otherwise enables disruption system operation in the unlocked mode. The control system can disable the disruption system by acting on the launching mechanism (e.g., disable the trigger, disconnect the power source, disconnect the trigger from the propulsion mechanism, etc.), acting on the tracking system (e.g., disable the tracking system), acting on the interdiction module (e.g., prevent second-stage deployment), or otherwise interfere with disruption system operation. However, the control system can otherwise control disruption operation. The selected control system mode is preferably dependent upon whether the aerial system

has permissions for the physical volume (e.g., wherein the locked mode is selected when the aerial system does not have permission and the unlocked mode is selected when the aerial system has permission), but can alternatively be dependent upon any other suitable factor. The control system can default to the locked mode, default to the unlocked mode, or default to any other suitable mode. In a first variation, the control system can be a processing system that electronically controls disruption system operation (e.g., the processor that controls launching mechanism operation, the avionics of the interdiction module, etc.). In a second variation, the control system can be a mechanical linkage between a launching mechanism trigger and propulsion initiation system that is selectively engaged or disengaged in the unlocked and locked mode, respectively. In a third variation, the control system can be a cap that selectively occludes or opens a launching mechanism barrel. However, the control system can include any other suitable mechanism or process that selectively permits disruption mechanism operation.

[0043] The discrimination system can additionally include a logging system that functions to store and/or provide histories for aerial system identifiers (e.g., generated by the identifier transmission system, static identifier for the aerial system, etc.), airspace, an entity associated with a set of airspaces, an entity associated with a set of aerial systems, or any other suitable history. The history can include: operation history (e.g., SOC, flight velocity, etc.), parameters for aerial system collocation within a given volume of airspace (e.g., airspace identifier, timestamps, concurrent weather proximal the airspace, etc.), or any other suitable historic parameter. The history is preferably

generated (automatically, etc.) in response to aerial system identification within the airspace (e.g., wherein the logging system can be coupled to the identification receiver), in response to determination of unauthorized aerial system presence within the airspace (e.g., wherein the logging system can be coupled to the permissions module), or at any other suitable time. The history can be used to predict aerial system action given a set of current operation parameters (e.g., using machine learning algorithms), to verify that the aerial system was within restricted airspace, to identify or verify the aerial system (e.g., wherein the discrimination system can query the aerial system for historic information, and verifies the aerial system upon receipt of the correct historic information), or be used in any other suitable manner.

[0044] The discrimination system can additionally include an identifier transmission system that functions to mount to an aerial system and transmit an aerial system identifier to the identification receiver. The identifier transmission system preferably periodically or constantly broadcasts the aerial system identifier, but can alternatively display the aerial system identifier, send the aerial system identifier in response to receipt of a request for the aerial system identifier, or otherwise transmit the aerial system identifier.

[0045] The aerial system identifier preferably identifies an aerial system, and is preferably globally unique, but can alternatively be unique for a geographic region, unique for a period of time, generic, or otherwise related to other aerial system identifiers. The aerial system identifier is preferably static, but can alternatively be dynamic. Dynamic aerial system identifiers can be generated, re-assigned, calculated

(e.g., based on a static identifier and a changing equation; based on changing identifier and a static equation; based on static identifier, a static equation, and a changing factor, such as a timestamp, etc.), or otherwise determined at a predetermined frequency, in response to the occurrence of a trigger event (e.g., upon user reassignment of the identifier transmission system to a different aerial system), or at any other suitable time. The dynamic aerial system identifier can be generated on-board the aerial system, generated remotely (e.g., at a remote computing system, etc.; updated in-flight or when connected to a predetermined communication connection type, etc.), or generated by any other suitable system. The aerial system identifier is preferably encrypted, but can alternatively be unencrypted. The aerial system identifier is preferably an alphanumeric string, but can alternatively be an image, pattern, combination of features (e.g., combination of colors, combination of colors and light emission patterns, etc.), a flight pattern, or be any other suitable identifier.

[0046] The identifier transmission system preferably mounts to an aerial system, but can alternatively be embedded within the aerial system, be a component of the aerial system (e.g., perform dual functionality), or be otherwise associated with the aerial system. The identifier transmission system preferably includes an identification transmitter and a coupling mechanism, but can alternatively include any other suitable component.

[0047] The identification transmitter of the identifier transmission system functions to transmit the identifier. In a first variation, the identification transmitter is an optical image, such as a barcode, QR code, picture, surface feature, or other optical

image, wherein the optical image functions as, embeds, links to, or is otherwise associated with the aerial system identifier. The optical image can be static (e.g., be a sticker), dynamic (e.g., be displayed by a display on the aerial system), or have any other suitable property. However, the optical image can otherwise function as the identification transmitter.

[0048] In a second variation, the identification transmitter is a set of light emitting elements (e.g., optical signal emitting elements). The light emitting elements can be LEDs, OLEDs, incandescent light, or any other suitable light emitting element. The wavelength of the emitted light can be in the visual range and/or outside of the visual range. The emitted light can be encrypted, unencrypted, or otherwise secured. In a first embodiment, the set of light emitting elements emit modulated light, wherein the modulated light can be interpreted into the aerial system identifier. In a second embodiment, the set of light emitting elements emit light pulses according to a predetermined pattern, wherein the predetermined pattern functions as the aerial system identifier. The aerial system can include a single light emitting element on the aerial system exterior, a ring of light emitting elements, or any suitable number of light emitting elements arranged in any other suitable configuration. However, the light emitting elements can otherwise function as the identification transmitter.

[0049] In a third variation, the identification transmitter is an electromagnetic wave transmitter. The electromagnetic wave transmitter can include a chipset, an antenna, and/or any other suitable component. The chipset can function to determine the aerial system identifier (e.g., store the aerial system identifier, generate the aerial

system identifier, etc.) and control the antenna to broadcast a signal representative of the aerial system identifier. Examples of the electromagnetic wave transmitter include: a WiFi transmitter, an RFID tag, a Bluetooth beacon (e.g., BLE beacon), a modem (e.g., 3G, 4G, LTE, etc.), an ADS-B radio, or any other suitable electromagnetic wave transmitter. However, the identification transmitter can include any other suitable mechanism capable of transmitting an identifier.

[0050] The coupling mechanism of the identifier transmission system functions to couple the identification transmitter to the aerial system. The coupling mechanism is preferably substantially permanent, but can alternatively be removable (e.g., transient), such that the identifier transmission system can be moved between different aerial systems. Examples of the coupling mechanism include: clips, adhesive, weldments, complimentary magnets, straps, or any other suitable coupling mechanism.

[0051] The identifier transmission system can optionally include a tamper detection mechanism that functions to indicate whether the identifier transmission system has been tampered with. In a first variation, the tamper detection mechanism includes a microswitch coupled to the coupling mechanism. Coupling mechanism decoupling from the aerial system changes the microswitch state, which prevents the identifier transmission system from transmitting an aerial system identifier (e.g., shuts off the identifier transmission system, blocks identifier transmission system transmission, etc.). The identifier transmission system can be reactivated upon verified user action (e.g., user login to a system associated with the identifier transmission system, user entry of a passcode, etc.) or upon the occurrence of any other suitable

activation event. In a second variation, the tamper detection mechanism can include security potting that physically bonds to and encompasses the identifier transmission system electronics, such that identifier transmission system removal from the aerial system and/or attempts to physically access the identifier transmission system electronics physically destroys the identifier transmission system. In a third variation, the tamper detection mechanism can include a security mesh enclosing the identifier transmission system electronics that shorts the identifier transmission system electronics upon tampering. However, the tamper detection mechanism can include any other suitable component configured to prevent identifier transmission system tampering, render the identifier transmission system inoperable upon tampering, and/or indicate past tampering.

[0052] The identifier transmission system can additionally include a power source that functions to power the identifier transmission system. Examples of the power source include: secondary batteries (e.g., rechargeable batteries), primary batteries, energy harvesting systems, the aerial system power source, or any other suitable power source.

[0053] In some variations, the discrimination system can additionally include auxiliary sensors and a telemetry system, wherein the telemetry system can constantly or periodically transmit sensor measurements or data derived therefrom to the identification receiver or another endpoint. Measurements recorded by the sensors can include: GPS coordinates, speed, acceleration, target destination, aerial system operation parameters (e.g., SOC), ambient environment parameters (e.g., windspeed,

heading, temperature etc.), or any other suitable parameter. The telemetry system can be the identifier transmission system or be a separate and distinct component. The telemetry system can be a radio, light emitter, or be any other suitable system.

5. *Method*

[0054] As shown in FIGURE 2, the method for aerial system discrimination and action includes: determining that an aerial system has entered restricted airspace, determining an aerial system identifier for the aerial system, determining a set of permissions associated with the restricted airspace, and determining whether the aerial system parameters are permitted based on the set of permissions. The method can be entirely or partially performed by: the permissions module, the identification receiver, the disruption system, or by any other suitable system. The method is preferably performed in response to, but can alternatively be performed at any other suitable time.

[0055] Determining that an aerial system has entered restricted airspace functions to trigger permissions analysis. The restricted airspace can be: a geofenced volume (e.g., geofenced geographic area and altitude range), a predetermined radius from a reference point (e.g., the disruption system can be the reference point), or be defined in any other suitable manner.

[0056] In a first variation, an aerial system is determined to have entered restricted airspace based on sensor measurements recorded by sensors associated with the airspace (e.g., sensors monitoring the airspace, mounted to buildings or other static mounting points). In a first specific example, an aerial system is determined to have

entered restricted airspace when microphones on the periphery of the airspace record acoustic frequencies within a predetermined range. In a second specific example, an aerial system is determined to have entered restricted airspace when a light beam is intercepted.

[0057] In a second variation, an aerial system is determined to have entered restricted airspace based on sensor measurements received from the identification receiver. In a first specific example, an aerial system is determined to have entered restricted airspace when microphones on the identification receiver and/or disruption system record acoustic frequencies within a predetermined range. In a second specific example, an aerial system is determined to have entered restricted airspace when an aerial system is recognized within an image recorded by the identification receiver (e.g., wherein the camera focal length can bound the monitored airspace).

[0058] In a third variation, an aerial system is determined to have entered restricted airspace based on sensor measurements received from the disruption system, wherein airspace presence within the airspace is inferred from sensor measurements indicative of user response to the aerial system. In a specific example, an aerial system is determined to have entered restricted airspace when the on-board accelerometer indicates that the disruption system has been picked up, or the on-board gyroscope indicates that the disruption system is being aimed. However, aerial system presence within the airspace can be otherwise determined or inferred.

[0059] Determining an aerial system identifier functions to identify the aerial system. The aerial system identifier is preferably determined in response to

determination that an aerial system has entered the airspace, but can be determined at any other suitable time. The aerial system identifier is preferably determined by the identification receiver, but can alternatively be determined by the permissions module, a remote computing system (e.g., a REST server), or by any other suitable system. The identifier for the intruding aerial system can be determinable (e.g., result in a readable identifier) or indeterminable (e.g., be unreadable, not present, incompatible, etc.). The former can be used to determine whether the corresponding aerial system has permissions for the airspace, or be otherwise used. The latter can be automatically classified as unauthorized, or be otherwise treated.

[0060] In a first variation, the aerial system identifier is read from an image of the aerial system. In a specific example, the identification transmission system can be an optical image, wherein the aerial system identifier is read from or retrieved based on the optical image recorded in an image of the aerial system.

[0061] In a second variation, the aerial system identifier is received by the discrimination system, wherein the identification transmission system broadcasts the aerial system identifier at a predetermined frequency.

[0062] In a first embodiment of the second variation, the identification transmission system broadcasts the same aerial system identifier over time. In this embodiment, the aerial system identifier can be determined based on a single transmission.

[0063] In a second embodiment of the second variation, the identification transmission system broadcasts different aerial system identifiers for the aerial system

over time (e.g., every other broadcast identifier is different, etc.). In this embodiment, the aerial system identifier can be determined based on: the transmission content and timestamp that the transmission was received; a time-ordered series of transmission content, or any other suitable set of transmissions. In one example, a permanent aerial system identifier can be calculated from one or more transient aerial system identifiers based on an equation, wherein the permanent aerial system identifier is used for permissions analysis. In this example, the transient aerial system identifiers can be automatically generated by the identification transmission system based on the equation and the permanent aerial system identifier. The equation can change over time, wherein the changing equations used by the identification transmission system and system determining the permanent aerial system identifier are preferably synchronized, but can alternatively be unsynchronized, periodically retrieved by the aerial system (e.g., downloaded from a server), or determined at any other suitable time. Alternatively or additionally, the calculation can be based on a timestamp (e.g., actual or anticipated transmission time, actual or anticipated receipt time, etc.). However, the calculation can be based on any other suitable parameter.

[0064] In a specific example, the aerial system identifier is automatically generated based on the hidden, permanent aerial system identifier and the Service Set Identifier (SSID) for the WiFi chipset of the identifier transmission system. The transmitted temporary aerial system identifier is preferably refreshed (e.g., recalculated, regenerated, etc.) at a predetermined frequency (e.g., every 10s). The identification receiver can receive one or more temporary aerial system identifiers from

the aerial system, determine the SSID of the identifier transmission system, can determine the permanent aerial system identifier based on the SSID and/or based on the equation(s) used to generate the temporary identifiers, as determined from associated timestamps. However, the aerial system identifiers can be otherwise determined.

[0065] In a third variation, determining the aerial system identifier includes: requesting the aerial system identifier from the aerial system with the disruption system (e.g., challenging the aerial system); and receiving the aerial system identifier from the aerial system in response to aerial system receipt of the request (e.g., answering the disruption system). The returned aerial system identifier can additionally or alternatively include a security key (e.g., private key, etc.) or include any other suitable verification information.

[0066] Determining an aerial system identifier can optionally include verifying the authenticity of the aerial system identifier. This functions to identify aerial systems with fake identifier transmission systems, wherein such systems can be treated as unauthorized or otherwise treated. In a first variation, authentication is accomplished by recording a series of broadcast aerial system identifiers and verifying the authenticity based on the identifier series. For example, the identifier series can be compared to an expected identifier series, wherein the aerial system is deemed fake when the actual series differs from the expected series. In a second variation, authentication is accomplished by using a secondary identifier. For example, the authenticity of the identifier transmission system can be verified when a first aerial system identifier

received from a WiFi transmitter (e.g., removably couplable to the aerial system) is associated with a second aerial system identifier extracted from a pattern of pulsed light (e.g., wherein the light source is integrated into the aerial system). In a third variation, authentication is accomplished by using a communications network interface identifier (e.g., MAC address). However, the aerial system identifier can be otherwise verified.

[0067] The method can optionally include determining instantaneous or anticipated aerial system function. The aerial system function is preferably determined in response to determination that an aerial system has entered the airspace, and can additionally be determined before or after aerial system identifier determination, or be determined at any other suitable time. The instantaneous or anticipated aerial system function can be determined by a function determination module on the permissions module, a remote computing system (e.g., a REST server), by the identification receiver, or by any other suitable system. The function determination module can be a machine learning module (e.g., be updated based on whether the anticipated function was actually performed), be a deterministic module, or be any other suitable module. The instantaneous or anticipated aerial system function can be determined based on information indicative of aerial system function. Examples of information indicative of aerial system function can include: one or more sensor measurements from the identification reader and/or disruption system, time-ordered sensor measurements from the identification reader and/or disruption system, or any other suitable set of information.

[0068] In a specific example, the information indicative of aerial system function can include a signal power measurement recorded by a radio of the disruption system, wherein the aerial system is categorized as broadcasting media in response to the signal power measurement exceeding a first power threshold, and not broadcasting media in response to the signal power measurement falling below a second power threshold (different or the same as the first power threshold). The broadcasting type (e.g., streaming, sending intermittent packets, etc.) can be further determined based on the signal power pattern (e.g., based on pattern matching, categorization, etc.). In a second specific example, the information indicative of aerial system function can include an image frame, which can be processed (e.g., using image processing techniques, such as image segmentation, shape recognition, feature classification, etc.) to determine whether the aerial system includes one of a set of restricted functional components (e.g., camera, payload, etc.). In a third specific example, the information indicative of aerial system function can include a series of video frames including the aerial system, which can be used to predict the aerial system flight path and/or target endpoint (e.g., determine the probability that the aerial system flight path will intercept an endpoint for each of a set of endpoints). However, the permissions module can receive any other suitable information, which can be used in any other suitable manner.

[0069] Determining a set of permissions associated with the restricted airspace functions to identify metrics by which to determine whether the aerial system is permitted within the airspace. Determining the set of permissions associated with the restricted airspace preferably includes determining an airspace identifier for the

airspace and determining the permissions associated with the airspace identifier, but the set of permissions can be otherwise determined.

[0070] Determining an airspace identifier associated with the aerial system functions to determine the identifier for the airspace for which permissions need to be determined. The airspace can be the airspace that the aerial system is instantaneously within, be airspace that the aerial system was within (e.g., a predetermined time duration prior), or be airspace that the aerial system will be in (e.g., within a predetermined time duration). In a first variation, the airspace identifier can be received from the identification receiver, along with the aerial system identifier. In this variation, the airspace identifier can be read off a beacon mounted proximal or within the physical volume or otherwise determined.

[0071] In a second variation, the airspace identifier can be automatically determined based on information indicative of aerial system location. Examples of information indicative of aerial system location can include: the disruption system identifier (e.g., wherein the airspace identifier is associated with one or more disruption system identifiers); the disruption system geographic location (e.g., wherein the airspace identifier is associated with the geographic location); sensor measurements (e.g., acoustic, visual, or electromagnetic measurements) from a set of sensors with known locations, wherein the aerial system location can be triangulated from the sensor measurements (e.g., wherein the airspace identifier identifies the triangulated region); disruption mechanism tilt and/or heading (e.g., orientation sensor measurements), wherein the airspace identifier identifies the airspace that the disruption mechanism is

aimed at; whether distance-restricted communication systems are connected to the aerial system (e.g., WiFi, BLE, NFC, etc.), wherein the airspace identifier identifies a geographic region encompassing the connectivity radius from the communications system; or be determined based on any other suitable information. However, the airspace identifier can be otherwise determined.

[0072] Determining the permissions based on the airspace identifier functions to retrieve the permissions for the airspace. The permissions are preferably retrieved for the airspace identifier from the permissions module (e.g., remote computing system, on-board permissions, etc.), but can alternatively be dynamically determined, be default permissions, or otherwise determined. The permissions are preferably determined based on the airspace identifier, but can alternatively be determined based on secondary information, such as weather information, calendar information, time information, social media, instantaneous location of an entity of interest (e.g., person of interest), predicted location of an entity of interest, or any other suitable secondary information. The secondary information can be used to filter, adjust or otherwise influence the determined airspace permissions.

[0073] In one example, dynamically determining the permissions can include: automatically determining a concurrent event occurring within or proximal the airspace and determining permissions based on the event features (e.g., event type, pre-set permissions, etc.). In a second example, dynamically determining the permissions can include: automatically determining the location of a person of interest, and automatically adjusting the permissions associated with airspace proximal the location.

In a third example, dynamically determining the permissions can include: determining current and/or forecasted weather for the airspace and adjusting the permissions to accommodate for the weather (e.g., shifting the altitude range permitted to the aerial system from “permitted above 100ft” to “permitted above 200ft” in response to forecasted high winds). However, the permissions can be otherwise determined.

[0074] Determining whether the aerial system parameters are permitted based on the set of permissions functions to determine: whether the aerial system is permitted within the airspace, whether the instantaneous or anticipated aerial system functions are permitted within the airspace, whether the instantaneous or anticipated aerial system functions are permitted for the specific aerial system within the airspace; or determine any other suitable set of permissions. The aerial system parameters can be: permitted, prohibited, partially permitted (e.g., wherein the aerial system is permitted but the function is not), or have any other suitable outcome. The permission can be determined after aerial system identifier determination, aerial system function determination, airspace permissions determination, or at any other suitable time. The permission can be determined by the permissions module, a remote computing system (e.g., a REST server), by the identification receiver, or by any other suitable system.

[0075] The aerial system parameter permission is preferably determined by comparing the aerial system parameters (e.g., identifier, function, etc.) with the permissions for the airspace, but can alternatively be otherwise determined. In one example, the aerial system is deemed not permitted when the aerial system lacks an identifier, the identifier is not on the list of permitted aerial system identifiers for the

airspace, or the identifier is on a list of prohibited aerial system identifiers for the airspace. In a second example, the aerial system is deemed not permitted when the aerial system function (e.g., anticipated or instantaneous) is not on the list of permitted aerial system functions for the airspace. In a third example, the aerial system is deemed partially permitted when the aerial system identifier is permitted for the airspace but the function is not permitted for the aerial system identifier within the airspace. However, the aerial system permissions can be otherwise determined.

[0076] The method can optionally include controlling disruption system operation based on the aerial system permission determination, which functions to selectively enable or disable the disruption system. Alternatively or additionally, the method can include controlling one or more auxiliary systems (e.g., notifications, alarms, etc.) based on the aerial system permission determination. Controlling disruption system operation can include: selecting a disruption system operation mode based on the determined aerial system permission and controlling the disruption system operation to meet the selected mode. Selecting a disruption system operation mode based on the determined aerial system permission preferably includes: selecting an enabled operation mode in response to aerial system classification as not permitted (e.g., prohibited) and selecting a disabled operation mode in response to aerial system classification as permitted. Selecting the disabled operation mode can additionally include selecting different operation modes for different disruption system functions based on the aerial system permission. For example, a jamming mechanism can be selectively enabled but an interdiction module selectively disabled in response to

detection of unpermitted streaming for a permitted aerial system. However, the disruption system operation mode can be otherwise selected. Controlling the disruption system operation to meet the selected mode preferably includes: sending instructions indicative of the selected operation mode to the control system, wherein the control system is placed in the selected operation mode or places the disruption system in the selected operation mode. However, disruption system operation can be otherwise controlled.

[0077] The method can optionally include contacting the aerial system pilot prior to disruption system activation. In one variation, this can include: determining a user identifier associated with the aerial system based on the aerial system identifier; determining contact information for the user identifier (e.g., email, social networking system account, phone number, etc.), and contacting the user using the contact information. Contacting the user can include: presenting the user with a notification (e.g., sending, displaying, etc.), wherein the notification can notify the user that the aerial system is within restricted airspace, give the user a warning (e.g., a time limit to leave the restricted airspace), query whether the user is the pilot, or present any other suitable information to the user. However, the user can be otherwise contacted. The user information can be stored by the permissions system, retrieved, or otherwise obtained.

[0078] The method can optionally include reassigning identifier transmission systems to different aerial systems, which functions to enable a user to use one identifier transmission system for multiple aerial systems (example shown in FIGURE 4). Reassigning the identifier transmission system can include: detecting a reassignment

event, disassociating the identifier transmission system from a first aerial system identifier, detecting an assignment event for a second aerial system, and associating the identifier transmission system with a second aerial system identifier representative of the second aerial system. The detected reassignment event can include: physical identifier transmission system removal from the first aerial system (e.g., detected by the microswitch), receipt of a reassignment selection from a user device (e.g., at a native application executed on the user device), or be any other suitable reassignment event. Disassociating the identifier transmission system from a first aerial system identifier can include: disassociating an identifier for the identifier transmission system from the permanent aerial system identifier (e.g., in a database), deactivating the identifier transmission system, disassociating the system from any aerial system (e.g., wherein the transmitted aerial system identifier does not represent any aerial system), or otherwise disassociating the identifier transmission system from the first aerial system. The assignment event can be: physical identifier transmission system coupling to a second aerial system, receipt of an assignment selection from a user device (e.g., entry of the permanent identifier for the second aerial system in association with the identifier for the identifier transmission system, selection of an “assignment” icon, receipt of a virtual association between the systems from the user, etc.), or be any other suitable assignment event. Associating the second aerial system identifier with the identifier transmission system can include: assigning the permanent identifier for the second aerial system to the identifier for the identifier transmission system in the database, reactivating the identifier transmission system, or otherwise associating the identifier

transmission system with the second aerial system. The permanent second aerial system identifier can be received from the user, automatically read from the second aerial system, retrieved from a third party database (e.g., manufacturer database), or otherwise determined.

[0079] Although omitted for conciseness, the preferred embodiments include every combination and permutation of the various system components and the various method processes, wherein the method processes can be performed in any suitable order, sequentially or concurrently.

[0080] As a person skilled in the art will recognize from the previous detailed description and from the figures and claims, modifications and changes can be made to the preferred embodiments of the invention without departing from the scope of this invention defined in the following claims.

CLAIMS

We Claim:

1. The inventions as shown and/or described.