(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 May 2025 (08.05.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/097095 A1

(51) International Patent Classification:
G08B 13/186 (2006.01) *B64C 39/02* (2006.01)
G08B 13/196 (2006.01) *G01H 9/00* (2006.01)
G08B 13/16 (2006.01) *B64U 101/31* (2023.01)

(21) International Application Number:
PCT/US2024/054324

(22) International Filing Date:
03 November 2024 (03.11.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/595,825 03 November 2023 (03.11.2023) US
18/935,489 02 November 2024 (02.11.2024) US

(71) Applicant: **NEC LABORATORIES AMERICA, INC.** [US/US]; Suite 200, 4 Independence Way, Princeton, New Jersey 08540 (US).

(72) Inventors: **DING, Yangmin**; 710 Village Drive South, Apt. B, North Brunswick, New Jersey 08902 (US). **WANG, Ting**; 10 Glacier Drive, West Windsor, New Jersey 08550 (US). **TIAN, Yue**; 22 Truman Avenue, Princeton, New Jersey 08540 (US). **OZHAHAR, Sarper**; 465 Meadow Road, Princeton, New Jersey 08540 (US). **JIANG, Zhuocheng**; 1315 Deer Creek Drive, Plainsboro, New Jersey 08536 (US). **WANG, Yanchao**; 206 Salem Court #2, Princeton, New Jersey 08540 (US).

(74) Agent: **KOLODKA, Joseph**; NEC Laboratories America, Inc., 4 Independence Way, Suite 200, Princeton, New Jersey 08540 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ,

(54) Title: INTEGRATED SECURITY SYSTEM FOR SUBSTATION MONITORING AND DETECTION USING DISTRIBUTED ACOUSTIC SENSING, DRONES, AND SECURITY CAMERAS

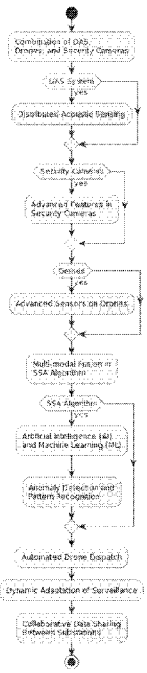


FIG. 2

(57) Abstract: Disclosed are integrated systems and operating methods that provide an integrated security system for substation monitoring and detection that effectively combines the strengths of distributed acoustic sensing, drones, and security cameras for comprehensive protection. The integrated system comprises a DAS system configured to monitor vibrations and acoustic signals along the length of fiber optic cables, one or more drones equipped with advanced sensors for aerial surveillance, and a plurality of security cameras installed throughout the substation to capture real-time video feeds and provide visual confirmation of activities. A central control system integrates and analyzes data from the DAS system, drones, and security cameras, and utilizes a novel, advanced algorithm, named Substation Security Analytics (SSA), specifically designed for the unique challenges associated with substation security monitoring and detection.

WO 2025/097095 A1

[Continued on next page]

RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

INTEGRATED SECURITY SYSTEM FOR SUBSTATION MONITORING AND DETECTION USING DISTRIBUTED ACOUSTIC SENSING, DRONES, AND SECURITY CAMERAS

FIELD OF THE INVENTION

[0001] This application relates generally to distributed fiber optic sensing (DFOS) systems, methods, structures, and related technologies. More particularly, it pertains to integrated security systems for substation monitoring and detection using distributed acoustic sensing (DAS), drones, and security cameras.

BACKGROUND OF THE INVENTION

[0002] Distributed fiber optic sensing (DFOS) systems, methods, and structures have found widespread utility in contemporary industry and society. Of particular importance, DFOS techniques have been used to usher in a new era of monitoring including perimeter security, traffic monitoring, and civil infrastructure monitoring.

[0003] Power utility substations are critical components of the electricity distribution infrastructure, responsible for the transmission, distribution, and transformation of electrical energy. Ensuring their security is of paramount importance due to the economic, social, and environmental consequences of disruptions caused by equipment failure, theft, vandalism, or sabotage. As the demand for electricity continues to grow, and power systems become more complex and interconnected, the need for advanced security solutions for substations becomes increasingly important.

[0004] Conventional security measures for substations have included physical barriers such as fences and walls, security guards, standalone security cameras, and simple intrusion detection systems. While these measures can provide a basic level of security, they have several limitations.

[0005] **Coverage:** Standalone security cameras and intrusion detection systems may not provide comprehensive coverage of the entire substation area, leaving blind spots that could be exploited by potential intruders. Additionally, security guards can only patrol a limited area and may not be able to detect or respond to incidents occurring in remote or hidden areas of the substation.

[0006] **Efficiency:** Manually monitoring security camera feeds or patrolling the substation perimeter can be labor-intensive and time-consuming for security personnel, reducing their ability to respond to incidents promptly and effectively.

[0007] **Adaptability:** Conventional security measures may not be well-suited to adapt to different situations or environmental conditions, such as inclement weather, low-light conditions, or varying levels of activity at the substation. This can result in reduced effectiveness of the security system and an increased likelihood of false alarms or missed incidents.

[0008] **Integration:** Standalone security measures may not be well-integrated, requiring security personnel to monitor and manage multiple systems simultaneously. This lack of integration can hinder the rapid identification and assessment of potential security threats, further delaying the response to incidents.

SUMMARY OF THE INVENTION

[0009] The above problems are solved and an advance in the art is made according to aspects of the present disclosure directed to systems and methods providing comprehensive protections for substations, overcoming the limitations of conventional security measures.

[0010] In sharp contrast to the prior art, systems and methods according to aspects of the present disclosure achieve such solutions and advances in the art by integrating advanced technologies such as distributed acoustic sensing (DAS), drones, and security cameras for enhanced monitoring, detection, and response capabilities.

[0011] As we shall show and describe systems and methods according to aspects of the present disclosure advantageously provide an integrated security system for substation monitoring and

detection that effectively combines the strengths of distributed acoustic sensing (DAS), drones, and security cameras for comprehensive protection. The integrated security system comprises the following interoperating components.

[0012] A DAS system configured to monitor vibrations and acoustic signals along the length of fiber optic cables. The DAS system may be installed along a substation perimeter, as well as around critical equipment within the substation. This advantageously enables the detection of attempted breaches, equipment tampering, or potential equipment failure, providing real-time alerts to any unusual activity.

[0013] One or more drones equipped with advanced sensors for aerial surveillance. These drones enable rapid response to incidents, providing expanded coverage of the substation and its surroundings. These drones can be equipped with sensors such as infrared, thermal imaging, or light detecting and ranging (LiDAR) sensors, allowing them to detect potential security threats in various environmental conditions and at different times of day.

[0014] A plurality of security cameras installed throughout the substation to capture real-time video feeds and provide visual confirmation of activities. The security cameras can have advanced features such as pan-tilt-zoom (PTZ) capabilities for wide-area coverage, infrared or thermal imaging for low-light conditions, and weather-resistant enclosures for protection against adverse weather.

[0015] A central control system for integrating and analyzing data from the DAS system, drones, and security cameras. The central control system utilizes a novel advanced algorithm, named Substation Security Analytics (SSA), specifically designed for the unique challenges associated with substation security monitoring and detection. The SSA algorithm incorporates artificial intelligence (AI) and machine learning (ML) techniques to process the collected data and identify potential security threats. The SSA algorithm is based on a multi-modal fusion approach, which combines data from the DAS system, drones, and security cameras in a complementary manner. The algorithm first extracts relevant features from the raw data, such as acoustic signatures, visual cues, and motion patterns. It then applies AI and ML techniques, such as deep learning and decision trees, to classify the extracted features and detect potential security threats. The algorithm advantageously learns from historical data, allowing it to adapt and improve its performance over time.

[0016] **Anomaly detection and pattern recognition:** The SSA algorithm according to the present disclosure includes advanced algorithms that can identify unusual activities or patterns, such as trespassing or potential equipment failure, by analyzing historical data and establishing baseline behavior.

[0017] **Automated drone dispatch:** The integrated security system according to the present disclosure can automatically dispatch drones for surveillance in response to specific triggers or detected threats, ensuring timely assessment and response to potential incidents.

[0018] **Dynamic adaptation of surveillance:** The integrated security system according to the present disclosure can dynamically adjust the surveillance coverage of the drones and security cameras based on the identified threat levels, environmental conditions, or predefined schedules.

[0019] **Collaborative data sharing between substations:** The integrated security system according to the present disclosure establishes a secure communication network that enables data sharing between different substations, allowing for better overall situational awareness and more efficient responses to potential security threats.

BRIEF DESCRIPTION OF THE DRAWING

[0020] **FIG. 1(A)** and **FIG. 1(B)** are schematic diagrams showing an illustrative prior art uncoded and coded DFOS systems.

[0021] **FIG. 2** is a schematic flow diagram showing illustrative advanced features and operation of systems and methods according to aspects of the present disclosure.

[0022] **FIG. 3** is a schematic flow diagram showing illustrative operational flow of systems and methods according to aspects of the present disclosure.

[0023] **FIG. 4** is a schematic feature diagram in hierarchical format showing illustrative features of systems and methods according to aspects of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

[0024] The following merely illustrates the principles of this disclosure. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the disclosure and are included within its spirit and scope.

[0025] Furthermore, all examples and conditional language recited herein are intended to be only for pedagogical purposes to aid the reader in understanding the principles of the disclosure and the concepts contributed by the inventor(s) to furthering the art and are to be construed as being without limitation to such specifically recited examples and conditions.

[0026] Moreover, all statements herein reciting principles, aspects, and embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0027] Thus, for example, it will be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative circuitry embodying the principles of the disclosure.

[0028] Unless otherwise explicitly specified herein, the FIGs comprising the drawing are not drawn to scale.

[0029] By way of some additional background, we note that distributed fiber optic sensing systems convert the fiber to an array of sensors distributed along the length of the fiber. In effect, the fiber becomes a sensor, while the interrogator generates/injects laser light energy into the fiber and senses/detects events along the fiber length.

[0030] As those skilled in the art will understand and appreciate, DFOS technology can be deployed to continuously monitor vehicle movement, human traffic, excavating activity, seismic activity, temperatures, structural integrity, liquid and gas leaks, and many other conditions and activities. It is

used around the world to monitor power stations, telecom networks, railways, roads, bridges, international borders, critical infrastructure, terrestrial and subsea power and pipelines, and downhole applications in oil, gas, and enhanced geothermal electricity generation. Advantageously, distributed fiber optic sensing is not constrained by line of sight or remote power access and - depending on system configuration - can be deployed in continuous lengths exceeding 30 miles with sensing/detection at every point along its length. As such, cost per sensing point over great distances typically cannot be matched by competing technologies.

[0031] Distributed fiber optic sensing measures changes in "backscattering" of light occurring in an optical sensing fiber when the sensing fiber encounters environmental changes including vibration, strain, or temperature change events. As noted, the sensing fiber serves as sensor over its entire length, delivering real time information on physical/environmental surroundings, and fiber integrity/security. Furthermore, distributed fiber optic sensing data pinpoints a precise location of events and conditions occurring at or near the sensing fiber.

[0032] A schematic diagram illustrating the generalized arrangement and operation of a distributed fiber optic sensing system that may advantageously include artificial intelligence / machine learning (AI/ML) analysis is shown illustratively in **FIG. 1(A)**. With reference to **FIG. 1(A),** one may observe an optical sensing fiber that in turn is connected to an interrogator. While not shown in detail, the interrogator may include a coded DFOS system that may employ a coherent receiver arrangement known in the art such as that illustrated in **FIG. 1(B)**.

[0033] As is known, contemporary interrogators are systems that generate an input signal to the optical sensing fiber and detects / analyzes reflected / backscattered and subsequently received signal(s). The received signals are analyzed, and an output is generated which is indicative of the environmental conditions encountered along the length of the fiber. The backscattered signal(s) so received may result from reflections in the fiber, such as Raman backscattering, Rayleigh backscattering, and Brillion backscattering.

[0034] As will be appreciated, a contemporary DFOS system includes the interrogator that periodically generates optical pulses (or any coded signal) and injects them into an optical sensing fiber. The injected optical pulse signal is conveyed along the length optical fiber.

[0035] At locations along the length of the fiber, a small portion of signal is backscattered/reflected and conveyed back to the interrogator wherein it is received. The backscattered/reflected signal carries information the interrogator uses to detect, such as a power level change that indicates – for example - a mechanical vibration.

[0036] The received backscattered signal is converted to electrical domain and processed inside the interrogator. Based on the pulse injection time and the time the received signal is detected, the interrogator determines at which location along the length of the optical sensing fiber the received signal is returning from, thus able to sense the activity of each location along the length of the optical sensing fiber. Classification methods may be further used to detect and locate events or other environmental conditions including acoustic and/or vibrational and/or thermal along the length of the optical sensing fiber.

[0037] Of particular interest, distributed acoustic sensing (DAS) is a technology that uses fiber optic cables as linear acoustic sensors. Unlike traditional point sensors, which measure acoustic vibrations at discrete locations, DAS can provide a continuous acoustic / vibration profile along the entire length of the cable. This makes it ideal for applications where it's important to monitor acoustic / vibration changes over a large area or distance.

[0038] Distributed acoustic sensing / distributed vibration sensing (DAS/DVS), also sometimes known as just distributed acoustic sensing (DAS), is a technology that uses optical fibers as widespread vibration and acoustic wave detectors. Like distributed temperature sensing (DTS), DAS/DVS allows for continuous monitoring over long distances, but instead of measuring temperature, it measures vibrations and sounds along the fiber.

[0039] DAS/DVS operates as follows.

[0040] Light pulses are sent through the fiber optic sensor cable.

[0041] As the light travels through the cable, vibrations and sounds cause the fiber to stretch and contract slightly.

[0042] These tiny changes in the fiber's length affect how the light interacts with the material, causing a shift in the backscattered light's frequency.

[0043] By analyzing the frequency shift of the backscattered light, the DAS/DVS system can determine the location and intensity of the vibrations or sounds along the fiber optic cable.

[0044] Similar to DTS, DAS/DVS offers several advantages over traditional point-based vibration sensors: High spatial resolution: It can measure vibrations with high granularity, pinpointing the exact location of the source along the cable; Long distances: It can monitor vibrations over large areas, covering several kilometers with a single fiber optic sensor cable; Continuous monitoring: It provides a continuous picture of vibration activity, allowing for better detection of anomalies and trends; Immune to electromagnetic interference (EMI): Fiber optic cables are not affected by electrical noise, making them suitable for use in environments with strong electromagnetic fields.

[0045] DAS/DVS technology has a wide range of applications, including: **Structural health monitoring:** Monitoring bridges, buildings, and other structures for damage or safety concerns; **Pipeline monitoring:** Detecting leaks, blockages, and other anomalies in pipelines for oil, gas, and other fluids; **Perimeter security:** Detecting intrusions and other activities along fences, pipelines, or other borders; **Geophysics:** Studying seismic activity, landslides, and other geological phenomena; and **Machine health monitoring:** Monitoring the health of machinery by detecting abnormal vibrations indicative of potential problems.

[0046] With the above in mind, we note again that a motivating application of systems and methods according to aspects of the present disclosure is critical infrastructure monitoring and in particular power station/substation monitoring with integrated systems and methods including distributed acoustic sensing (DAS), drones, and security cameras for enhanced monitoring, detection, and response capabilities.

[0047] As we shall show and describe systems and methods according to aspects of the present disclosure advantageously provide an integrated security system and operational method for substation monitoring and detection that effectively combines the strengths of distributed acoustic sensing (DAS), drones, and security cameras for comprehensive protection. The integrated security system comprises the following interoperating components.

[0048] A DAS system configured to monitor vibrations and acoustic signals along the length of fiber optic cables. The DAS system may be installed along a substation perimeter, as well as around critical equipment within the substation. This advantageously enables the detection of attempted breaches, equipment tampering, or potential equipment failure, providing real-time alerts to any unusual activity.

[0049] One or more drones equipped with advanced sensors for aerial surveillance. These drones enable rapid response to incidents, providing expanded coverage of the substation and its surroundings. These drones can be equipped with sensors such as infrared, thermal imaging, or light detecting and ranging (LiDAR) sensors, allowing them to detect potential security threats in various environmental conditions and at different times of day.

[0050] A plurality of security cameras installed throughout the substation to capture real-time video feeds and provide visual confirmation of activities. The security cameras can have advanced features such as pan-tilt-zoom (PTZ) capabilities for wide-area coverage, infrared or thermal imaging for low-light conditions, and weather-resistant enclosures for protection against adverse weather.

[0051] A central control system for integrating and analyzing data from the DAS system, drones, and security cameras. The central control system utilizes a novel advanced algorithm, named Substation Security Analytics (SSA), specifically designed for the unique challenges associated with substation security monitoring and detection. The SSA algorithm incorporates artificial intelligence (AI) and machine learning (ML) techniques to process the collected data and identify potential security threats. The SSA algorithm is based on a multi-modal fusion approach, which combines data from the DAS system, drones, and security cameras in a complementary manner. The algorithm first extracts relevant features from the raw data, such as acoustic signatures, visual cues, and motion patterns. It then applies AI and ML techniques, such as deep learning and decision trees, to classify the extracted

features and detect potential security threats. The algorithm advantageously learns from historical data, allowing it to adapt and improve its performance over time.

[0052] Anomaly detection and pattern recognition: The SSA algorithm according to the present disclosure includes advanced algorithms that can identify unusual activities or patterns, such as trespassing or potential equipment failure, by analyzing historical data and establishing baseline behavior.

[0053] Automated drone dispatch: The integrated security system according to the present disclosure can automatically dispatch drones for surveillance in response to specific triggers or detected threats, ensuring timely assessment and response to potential incidents.

[0054] Dynamic adaptation of surveillance: The integrated security system according to the present disclosure can dynamically adjust the surveillance coverage of the drones and security cameras based on the identified threat levels, environmental conditions, or predefined schedules.

[0055] Collaborative data sharing between substations: The integrated security system according to the present disclosure establishes a secure communication network that enables data sharing between different substations, allowing for better overall situational awareness and more efficient responses to potential security threats.

[0056] Particularly inventive aspects of systems and methods according to aspects of the present disclosure include the following.

[0057] Integration of distributed acoustic sensing (DAS), drones, and security cameras: This combination of technologies provides comprehensive coverage and monitoring capabilities, addressing the limitations of traditional security measures.

[0058] Multi-modal fusion approach in the Substation Security Analytics (SSA) algorithm: By combining data from the DAS system, drones, and security cameras in a complementary manner, the algorithm can effectively analyze and identify potential security threats.

[0059] Use of artificial intelligence (AI) and machine learning (ML) techniques in the SSA algorithm: These techniques enable the system to adapt and improve its performance over time, resulting in a more accurate and efficient security solution.

[0060] Advanced sensors on drones: Equipping drones with infrared, thermal imaging, or LiDAR sensors allows for enhanced detection capabilities in various environmental conditions and at different times of day.

[0061] Advanced features in security cameras: Incorporating pan-tilt-zoom (PTZ) capabilities, infrared or thermal imaging, and weather-resistant enclosures ensures wide-area coverage, low-light detection, and protection against adverse weather.

[0062] Anomaly detection and pattern recognition: The SSA algorithm incorporates advanced algorithms that can identify unusual activities or patterns, such as trespassing or potential equipment failure, by analyzing historical data and establishing baseline behavior.

[0063] Automated drone dispatch: The integrated security system can automatically dispatch drones for surveillance in response to specific triggers or detected threats, ensuring timely assessment and response to potential incidents.

[0064] Dynamic adaptation of surveillance: The integrated security system can dynamically adjust the surveillance coverage of the drones and security cameras based on the identified threat levels, environmental conditions, or predefined schedules.

[0065] Collaborative data sharing between substations: The integrated security system establishes a secure communication network that enables data sharing between different substations, allowing for better overall situational awareness and more efficient responses to potential security threats.

[0066] By incorporating these inventive features, integrated security systems and methods according to aspects of the present disclosure effectively address challenges associated with substation security monitoring and detection, providing comprehensive protection and enhancing the overall reliability of the power distribution system.

[0067] **FIG. 2** is a schematic flow diagram showing illustrative advanced features and operation of systems and methods according to aspects of the present disclosure. An illustrative step by step description of the operation of systems and methods according to the present disclosure includes the following.

[0068] **Step 1: Set up the DAS system**

[0069] Assess the substation layout and identify critical areas that require monitoring.

[0070] Install fiber optic cables along the substation perimeter and around critical equipment within the substation, ensuring proper cable routing and protection.

[0071] Connect the DAS system to the fiber optic cables and configure it to continuously monitor vibrations and acoustic signals.

[0072] Perform initial calibration and testing to ensure optimal performance.

[0073] **Step 2: Install security cameras**

[0074] Conduct a site survey to identify strategic locations for security camera installation, considering factors such as coverage, visibility, and potential blind spots.

[0075] Install security cameras with advanced features, ensuring proper mounting, alignment, and secure connections.

[0076] Connect the cameras to the central control system and configure them for continuous monitoring and recording.

[0077] Test the camera feeds to ensure proper image quality, coverage, and functionality.

[0078] Step 3: Deploy drones

[0079] Select appropriate drone models with the necessary payload capacity and flight endurance to carry advanced sensors and cover the required surveillance area.

[0080] Equip the drones with advanced sensors such as infrared, thermal imaging, or LiDAR sensors to enable detection of potential security threats in various environmental conditions and at different times of day.

[0081] Establish a secure and convenient storage location within the substation for easy drone access when required.

[0082] Configure the drones to communicate with the central control system and test their functionality.

[0083] Step 4: Set up the central control system

[0084] Set up the hardware and software infrastructure required for the central control system, including servers, networking equipment, and user interfaces.

[0085] Configure the central control system to integrate data from the DAS system, drones, and security cameras for real-time analysis.

[0086] Test the central control system to ensure proper data integration, processing, and functionality.

[0087] Step 5: SSA algorithm development

[0088] Develop and implement the SSA algorithm, which utilizes machine learning techniques to process the collected data and identify potential security threats. The SSA algorithm should be based on a multi-modal fusion approach, which combines data from the DAS system, drones, and security cameras in a complementary manner. The algorithm should first extract relevant features from the raw data, such as acoustic signatures, visual cues, and motion patterns. It should then apply AI and

ML techniques, such as deep learning and decision trees, to classify the extracted features and detect potential security threats. The algorithm should be capable of learning from historical data, allowing it to adapt and improve its performance over time.

[0089] **FIG. 3** is a schematic flow diagram showing illustrative SSA operational flow of systems and methods according to aspects of the present disclosure. With reference to that figure, the following operational flow is performed.

[0090] **Collect data from DAS, drones, and security cameras:** The first step in the SSA algorithm is to collect data from various sources, including distributed acoustic sensing (DAS) systems, drones, and security cameras. These data sources capture different types of information, such as acoustic signals, visual cues, and motion patterns, that can be used to detect potential security threats.

[0091] **Preprocess data to ensure accuracy and consistency:** Before the collected data can be used for threat detection, it must be preprocessed to ensure accuracy and consistency. This includes applying techniques such as noise filtering and correction, feature scaling, data augmentation, feature selection, feature engineering, and spatial and temporal alignment.

[0092] **Utilize multi-modal fusion to combine features from DAS, drones, and security cameras:** Once the data has been preprocessed, the next step is to use multi-modal fusion to combine features from the different data sources. This involves feature weighting, feature selection, feature extraction, deep feature learning, and attention mechanisms.

[0093] **Apply supervised or unsupervised learning techniques:** Depending on whether the collected data is labeled or not, the SSA algorithm can apply supervised or unsupervised learning techniques. Supervised learning techniques include classification, object detection, instance segmentation, anomaly detection, and threat assessment, while unsupervised learning techniques include clustering, outlier detection, dimensionality reduction, generative modeling, and adversarial learning.

[0094] **Deploy the model for real-time threat assessment and response:** Once the model has been trained and validated, it can be deployed for real-time threat assessment and response. This involves decision making, action selection, and policy optimization.

[0095] **Use the results of the model to generate alerts and notifications for security personnel and law enforcement:** The results of the model can be used to generate alerts and notifications for security personnel and law enforcement. This allows them to take appropriate actions, such as dispatching a security team, notifying law enforcement, initiating backup power, or triggering physical defenses.

[0096] **Continuously update and refine the model based on new data and feedback:** The SSA algorithm should be continuously updated and refined based on new data and feedback. This includes using techniques such as active learning, online learning, and adaptive learning to improve the accuracy and effectiveness of the model over time.

[0097] **Evaluate the performance of the model regularly and adjust hyperparameters and configurations accordingly:** Finally, the performance of the model should be evaluated regularly, and hyperparameters and configurations should be adjusted accordingly. This ensures that the model remains accurate and effective in detecting potential security threats.

[0098] **Step 6: Alert and notification system**

[0099] Develop an alert and notification system that generates alarms or alerts based on predefined criteria and sends notifications to security personnel or law enforcement as necessary. Configure the alert and notification system to be responsive and timely, ensuring that potential security threats are identified and addressed promptly. Develop and test communication protocols and response plans to ensure that the appropriate parties are notified and action is taken in the event of an incident.

[0100] **Step 7: Incident response procedures**

[0101] Once the SSA algorithm generates alerts and notifications, the incident response procedures come into play. The incident response procedures involve a set of guidelines and protocols that define how to respond to security incidents in the substation. The incident response procedures should be well-defined and clearly communicated to all relevant personnel, including security staff, operations

staff, and management. The procedures should cover a wide range of scenarios, including breaches, equipment tampering, vandalism, theft, and natural disasters.

[0102] The incident response procedures should include the following steps:

[0103] **Verify the alert:** Once an alert is generated, the first step is to verify the alert to ensure that it is a legitimate threat. This involves reviewing the data collected by the DAS, drones, and security cameras and comparing it to the SSA algorithm's output.

[0104] **Notify the relevant personnel:** Once the alert has been verified, the relevant personnel should be notified immediately. This includes security staff, operations staff, and management, as well as law enforcement agencies if necessary.

[0105] **Assess the situation:** The next step is to assess the situation and determine the severity of the threat. This includes evaluating the potential impact on the substation's operations, equipment, and personnel, as well as the potential risk to public safety and the environment.

[0106] **Initiate appropriate response measures:** Based on the severity of the threat, appropriate response measures should be initiated. This may include dispatching a security team, notifying law enforcement, initiating backup power, or triggering physical defenses.

[0107] **Document the incident:** Once the incident has been resolved, it should be documented in detail. This includes recording the date and time of the incident, the type of incident, the actions taken, and the outcome.

[0108] **Review and update the incident response procedures:** Finally, the incident response procedures should be reviewed and updated regularly to ensure that they remain up-to-date and effective. This includes incorporating lessons learned from previous incidents and incorporating new security technologies and best practices.

[0109] **FIG. 4** is a schematic feature diagram in hierarchical format showing illustrative features of systems and methods according to aspects of the present disclosure.

[0110] While we have presented our inventive concepts and description using specific examples, our invention is not so limited. Accordingly, the scope of our invention should be considered in view of the following claims.

Claims

1. An integrated security system comprising:
   a distributed fiber optic sensing system;
   one or more aerial drones; and
   one or more security cameras;
   wherein the integrated security system is configured to receive, integrate, and analyze data produced by the distributed fiber optic sensing system, the one or more aerial drones, and the one or more security cameras.

2. The system of claim 1 wherein the distributed fiber optic sensing system (DFOS) is a distributed acoustic sensing / distributed vibration sensing (DAS/DVS) system.

3. The system of claim 2 wherein the one or more aerial drones provide real-time video feeds for visual confirmation of incidents.

4. The system of claim 3 wherein the one or more security cameras provide real-time video feeds for visual confirmation of activities.

5. The system of claim 4 configured to provide machine learning and artificial intelligence techniques to the data received from the distributed fiber optic sensing system, the one or more aerial drones, and the one or more security cameras.

6. The system of claim 5 configured to extract relevant features from the received data including acoustic signatures, visual cues, and motion patterns.

7. The system of claim 6 configured to classify the extracted relevant features.

8. The system of claim 7 configured to detect potential security threats from the classified extracted relevant features.

9. The system of claim 8 configured to learn from historical data received from the distributed fiber optic sensing system, the one or more aerial drones, and the one or more security cameras.

10. The system of claim 9 configured to respond to detected potential security threats by initiating incident response procedures.

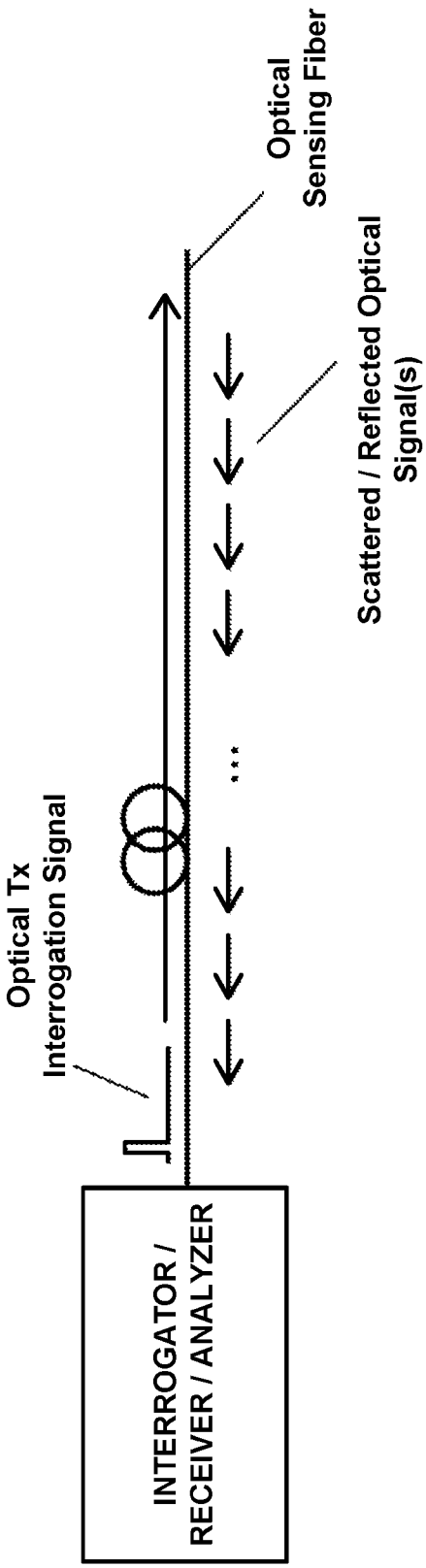

Optical Sensing Fiber
Scattered / Reflected Optical Signal(s)
Optical Tx Interrogation Signal
INTERROGATOR / RECEIVER / ANALYZER

FIG. 1(A)

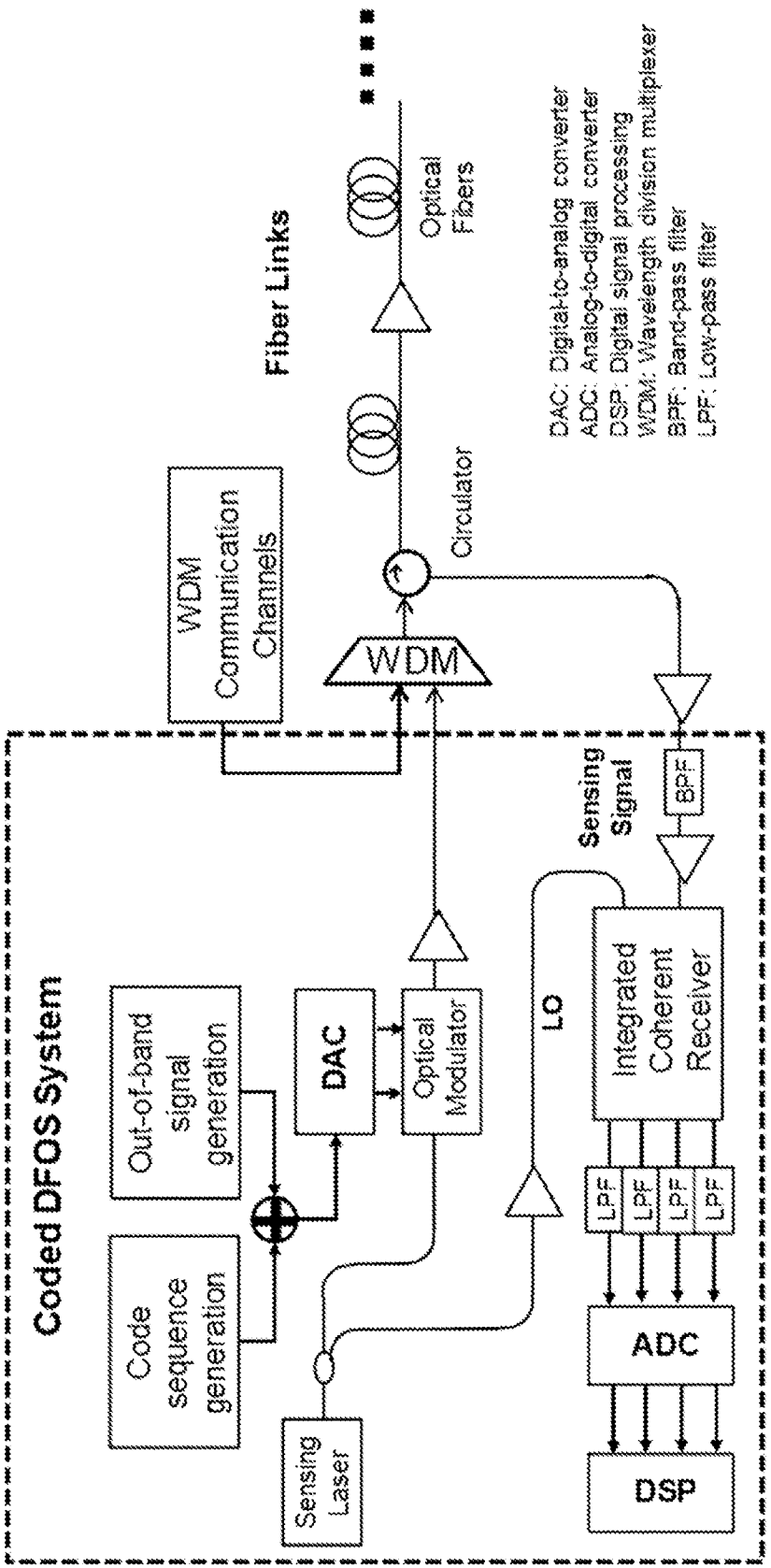

Coded DFOS System
Code sequence generation
Out-of-band signal generation
DAC
Optical Modulator
Sensing Laser
WDM Communication Channels
WDM
Circulator
Fiber Links
Optical Fibers
LO
Sensing Signal
BPF
Integrated Coherent Receiver
LPF
LPF
LPF
LPF
ADC
DSP
DAC: Digital-to-analog converter
ADC: Analog-to-digital converter
DSP: Digital signal processing
WDM: Wavelength division multiplexer
BPF: Band-pass filter
LPF: Low-pass filter

FIG. 1(B)

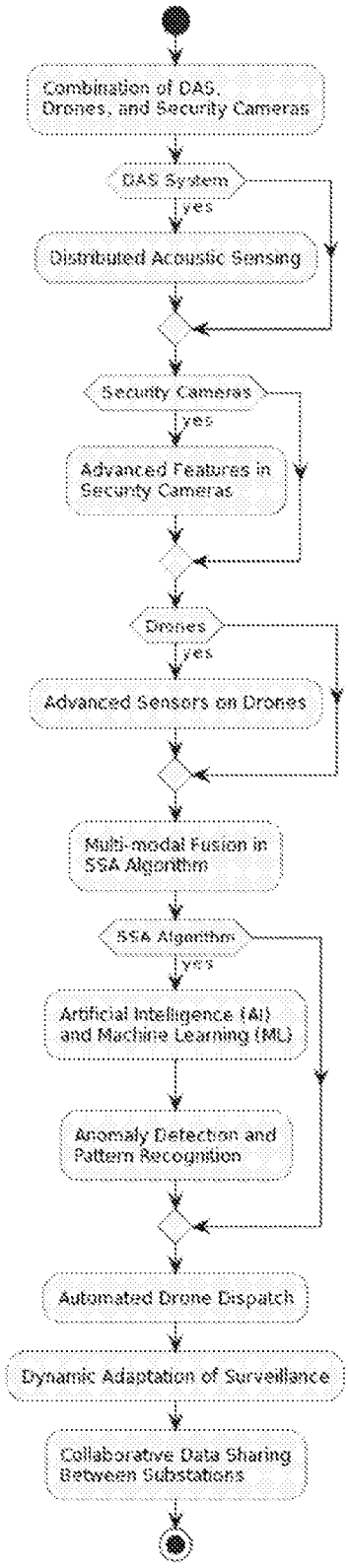

Combination of DAS, Drones, and Security Cameras
DAS System
yes
Distributed Acoustic Sensing
Security Cameras
yes
Advanced Features in Security Cameras
Drones
yes
Advanced Sensors on Drones
Multi-modal Fusion in SSA Algorithm
SSA Algorithm
yes
Artificial Intelligence (AI) and Machine Learning (ML)
Anomaly Detection and Pattern Recognition
Automated Drone Dispatch
Dynamic Adaptation of Surveillance
Collaborative Data Sharing Between Substations

FIG. 2

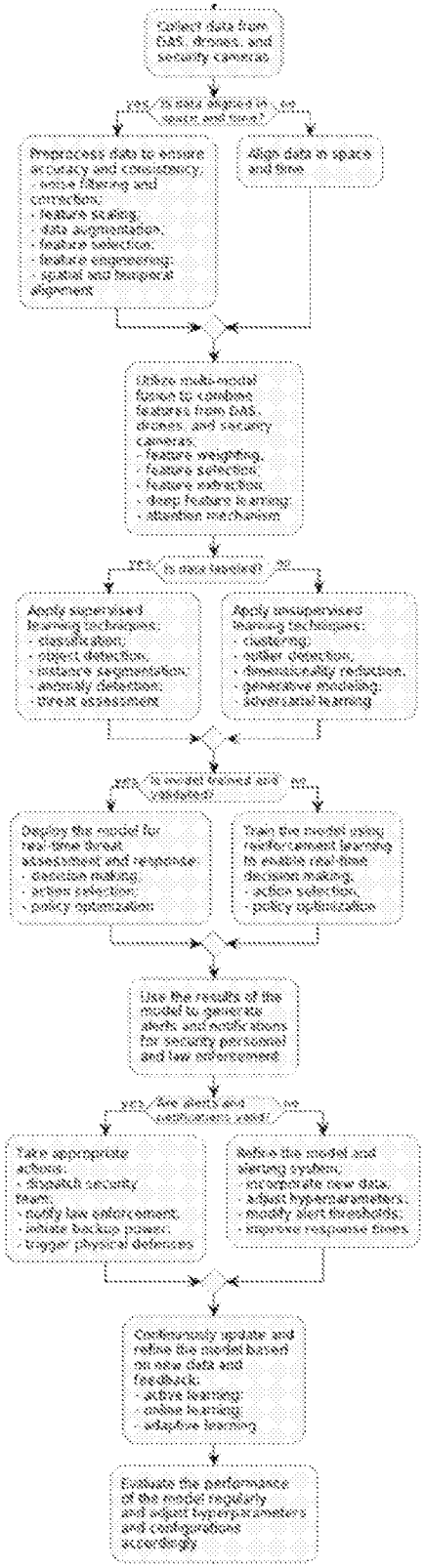

Collect data from UAS, drones, and security cameras
Is data aligned in space and time?
yes
no
Preprocess data to ensure accuracy and consistency:
- noise filtering and correction,
- feature scaling,
- data augmentation,
- feature selection,
- feature engineering,
- spatial and temporal alignment
Align data in space and time
Utilize multi-modal fusion to combine features from UAS, drones, and security cameras:
- feature weighting,
- feature selection,
- feature extraction,
- deep feature learning,
- attention mechanism
Is more needed?
yes
no
Apply supervised learning techniques:
- classification,
- object detection,
- instance segmentation,
- anomaly detection,
- threat assessment
Apply unsupervised learning techniques:
- clustering,
- outlier detection,
- dimensionality reduction,
- generative modeling,
- adversarial learning
Is model trained and validated?
yes
no
Deploy the model for real-time threat assessment and response:
- decision making,
- action selection,
- policy optimization
Train the model using reinforcement learning to enable real-time decision making:
- action selection,
- policy optimization
Use the results of the model to generate alerts and notifications for security personnel and law enforcement
Are alerts and notifications valid?
yes
no
Take appropriate actions:
- dispatch security team,
- notify law enforcement,
- initiate backup power,
- trigger physical defenses
Refine the model and alerting system:
- incorporate new data,
- adjust hyperparameters,
- modify alert thresholds,
- improve response times
Continuously update and refine the model based on new data and feedback:
- active learning,
- online learning,
- adaptive learning
Evaluate the performance of the model regularly and adjust hyperparameters and configurations accordingly

FIG. 3

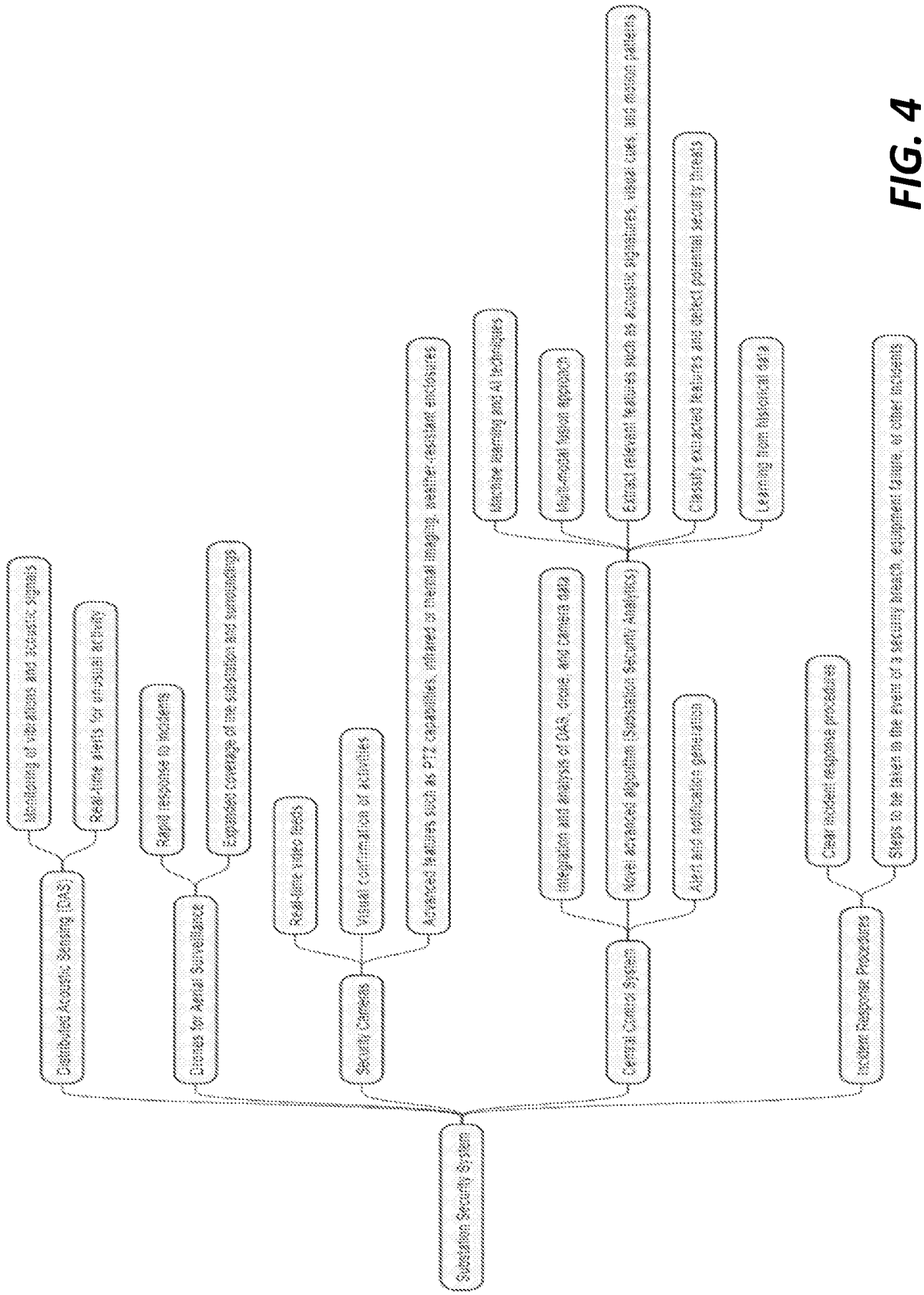

Perimeter Security System
Distributed Acoustic Sensing (DAS)
Monitoring of vibrations and acoustic signals
Real-time alerts for unusual activity
Drones for Aerial Surveillance
Rapid response to incidents
Expanded coverage of the perimeter and surroundings
Security Cameras
Real-time video feeds
Visual confirmation of activities
Advanced features such as PTZ capabilities, infrared or thermal imaging, weather-resistant enclosures
Central Control System
Integration and analysis of DAS, drone, and camera data
Machine learning and AI techniques
Rule-based logic approach
Most advanced algorithm (Specialist Security Analysis)
Extract relevant features such as acoustic signatures, visual cues, and motion patterns
Alert and notification generation
Classify extracted features and detect potential security threats
Learning from historical data
Incident Response Procedures
Clear incident response procedures
Steps to be taken in the event of a security breach, equipment failure, or other incidents

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2024/054324

A. CLASSIFICATION OF SUBJECT MATTER

G08B 13/186(2006.01)i; **G08B 13/196**(2006.01)i; **G08B 13/16**(2006.01)i; **B64C 39/02**(2006.01)i; **G01H 9/00**(2006.01)i; **B64U 101/31**(2023.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G08B 13/186(2006.01); G01D 5/353(2006.01); G01H 9/00(2006.01); G05D 1/10(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: distributed fiber optic sensing system, drone, camera, machine learning

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2022-0317707 A1 (NEC CORPORATION) 06 October 2022 (2022-10-06) paragraphs [0039]-[0081], claims 1, 4 and figure 3	1-4
Y		5-10
Y	US 2023-0236043 A1 (FIBER SENSE LIMITED) 27 July 2023 (2023-07-27) paragraph [0062] and claims 1, 11-12	5-10
A	US 2020-0249076 A1 (NEC LABORATORIES AMERICA, INC.) 06 August 2020 (2020-08-06) claim 1 and figure 1	1-10
A	WO 2022-061422 A1 (FIBER SENSE PTY LTD.) 31 March 2022 (2022-03-31) claim 1 and figures 1A-1B	1-10
A	WO 2020-097682 A1 (ENGLUND, MARK ANDREW) 22 May 2020 (2020-05-22) claim 1 and figures 1A-2	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2025	**14 February 2025**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**LEE, Kang Ha**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5687**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2024/054324

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2022-0317707 A1	06 October 2022	JP 7298693 B2	27 June 2023
		US 11914399 B2	27 February 2024
		US 2024-0061446 A1	22 February 2024
		WO 2021-024388 A1	11 February 2021
US 2023-0236043 A1	27 July 2023	EP 3538850 A1	18 September 2019
		EP 3538850 B1	08 January 2025
		JP 2019-537721 A	26 December 2019
		JP 6974457 B2	01 December 2021
		US 11555717 B2	17 January 2023
		US 11867539 B2	09 January 2024
		US 2020-0191613 A1	18 June 2020
		WO 2018-085893 A1	17 May 2018
US 2020-0249076 A1	06 August 2020	JP 2022-509678 A	21 January 2022
		JP 2022-515184 A	17 February 2022
		JP 7220288 B2	09 February 2023
		US 10917168 B2	09 February 2021
		US 11391622 B2	19 July 2022
		US 2020-0200592 A1	25 June 2020
		WO 2020-132169 A1	25 June 2020
		WO 2020-163577 A1	13 August 2020
WO 2022-061422 A1	31 March 2022	EP 4217683 A1	02 August 2023
		JP 2023-543063 A	12 October 2023
		US 2023-0358562 A1	09 November 2023
WO 2020-097682 A1	22 May 2020	EP 3881034 A1	22 September 2021
		EP 3881034 B1	24 April 2024
		JP 2022-507455 A	18 January 2022
		JP 7483702 B2	15 May 2024
		US 2022-0018980 A1	20 January 2022