ГАЛУЗЬ ТЕХНІКИ

Цей опис загалом стосується безпілотних літальних систем. Зокрема, цей опис стосується краудсорсингового виявлення та відстеження безпілотних літальних систем.

РІВЕНЬ ТЕХНІКИ

Швидко поширюються недорогі невеликі безпілотні літальні системи (БПЛС), як-от дрони. Було запропоновано та впроваджено численні застосування для БПЛС, наприклад, перевірки інфраструктури та комунальних послуг, спостереження, доставка пакетів, міська мобільність тощо. У той час як більшість випадків використання БПЛС є корисними, деякі БПЛС можуть бути використані з поганою метою, і ці БПЛС можуть становити серйозну загрозу для широкого спектру цілей. На жаль, виявлення, розпізнавання та оцінка загрози БПЛС можуть бути складними, особливо тому, що БПЛС часто літають на малих висотах.

EP 3 140 710 A1 розкриває системи та методи для безпеки безпілотних літальних апаратів (БПЛА). Система аутентифікації може використовуватися для підтвердження ідентифікації БПЛА та/або користувача та забезпечення захищеного зв'язку між користувачами та БПЛА. Надається система відстеження, яка використовуючи один або кілька реєстраторів, відстежує політ БПЛА в області, керованій системою повітряного контролю. Реєстратори можуть бути портативними. Система відстеження отримує інформацію, зібрану з одного або кількох реєстраторів, та визначає положення БПЛА. Потім визначається, чи становить БПЛА загрозу, і може бути надане сповіщення оператору БПЛА, системі повітряного контролю або будь-якій іншій стороні.

US 2020/106818 A1 розкриває систему зв'язку дронів, яка включає дрон з множинністю датчиків, де кожен з множинності датчиків збирає потік даних. Наземна система керування зв'язується з дроном та множинністю датчиків. Щонайменше один пристрій зв'язку входить до комплектації. Сервер зв'язку зв'язується з дроном, наземною системою керування та щонайменше одним пристроєм зв'язку. Кожний потік даних від множинності датчиків передається на сервер зв'язку, а сервер зв'язку передає потік наземній системі керування та щонайменше одному пристрою зв'язку в реальному часі.

US 2020/162489 A1 розкриває метод для виявлення події безпеки та оцінки загрози, зокрема стосовно знаходження літальних апаратів в захищеному повітряному просторі. Отримується сигнал про виявлену подію безпеки. Вибирається один або більше датчиків на основі виявленої події безпеки і використовується для виявлення додаткової інформації. Визначається рівень ризику, пов'язаний з виявленою подією безпеки, і автоматично викликається відповідь.

WO 2019/032162 A2 розкриває систему та метод для ідентифікації безпілотної літальної системи (БПЛС) виявленого в певному місці.

Цей опис стосується краудсорсингового виявлення та відстеження безпілотних літальних систем.

Передбачений спосіб, як зазначено в доданому пункті 1 формули винаходу.

Передбачений пристрій, як зазначено в доданому пункті 6 формули винаходу.

Передбачений постійний машиночитаний носій, як зазначено в доданому пункті 11 формули винаходу.

Інші технічні характеристики можуть бути легко зрозумілі фахівцю в цій галузі техніки з наведених нижче фігур, опису та формули винаходу.

КОРОТКИЙ ОПИС ГРАФІЧНИХ МАТЕРІАЛІВ

Для більш повного розуміння цього винаходу далі дається посилання на нижченаведений опис у поєднанні з супровідними графічними матеріалами, в яких:

на фіг. 1 проілюстровано типову систему для краудсорсингового виявлення та відстеження безпілотних літальних систем (БПЛС) згідно з цим описом;

на фіг. 2 проілюстровано типовий пристрій для краудсорсингового виявлення та відстеження БПЛС згідно з цим описом;

на фіг. 3 проілюстровано типове середовище, в якому краудсорсингове виявлення та відстеження БПЛС можна виконувати згідно з цим описом;

на фіг. 4 проілюстровано типове геопросторове представлення рішення стосовно протидії БПЛС, в якому краудсорсингове виявлення та відстеження БПЛС можна виконувати згідно з цим описом; і

на фіг. 5 проілюстровано типовий спосіб краудсорсингового виявлення та відстеження БПЛС згідно з цим описом.

ДЕТАЛЬНИЙ ОПИС ВИНАХОДУ

Фіг. 1-5, описані нижче, та різні варіанти здійснення, що використовуються для опису принципів цього винаходу в цьому патентному документі, наведені лише як ілюстрація та не мають вважатися обмеженням обсягу винаходу. Фахівцям в цій галузі техніки буде зрозуміло, що принципи цього винаходу можуть бути реалізовані в будь-якому типі прийнятним чином організованого пристрою чи системи.

Як зазначалося вище, швидко поширюються безпілотні літальні системи, або "БПЛС", як-от дрони або інші безпілотні літальні апарати. Було запропоновано та реалізовано численні корисні застосування для БПЛС. Однак деякі БПЛС можуть бути використані з поганою метою, і ці БПЛС можуть становити серйозну загрозу для широкого спектру цілей. На жаль, виявлення, розпізнавання та оцінка загрози БПЛС можуть бути складними, особливо тому, що БПЛС часто літають на малих висотах. Крім того, БПЛС часто літають у середовищах із високим рівнем перешкод з обмеженою видимістю, а невеликі БПЛС легко транспортуються в різні місця розташування, де їх можна запускати як спливаючі загрози з короткими часовими рамками атаки. Крім того, традиційне обладнання для виявлення, розпізнавання, оцінки та пом'якшення наслідків є дорогим і вимагає інтенсивної ручної праці, що обмежує їх використання.

Деякі наявні підходи до виявлення БПЛС орієнтуються на кооперативний зв'язок, наприклад, коли БПЛС або його оператор надає інформацію про БПЛС (наприклад, план польоту, зарезервований повітряний простір і положення апарату) зацікавленій стороні, яка спостерігає за БПЛС. Ці підходи зосереджені передусім на сприянні юридичним, комерційним та рекреаційним суб'єктам. Однак ці підходи неадекватні або неефективні для боротьби з суб'єктами, які не відповідають вимогам, не співпрацюють та/або є ворожими. У таких випадках часто необхідно

виявляти та оцінювати БПЛС без інформації, добровільно наданої БПЛС або її оператором. Можливо, можна захистити населені зони або зони з критичною інфраструктурою за допомогою датчиків виявлення, як-от радар або високоефективні системи формування зображень. Однак ці рішення, як правило, вважаються надто дорогими з точки зору придбання, укомплектування персоналом і підтримки для широкомасштабного розгортання в міських або приміських зонах, особливо з огляду на обмежену видимість на малих висотах і середовища з високим рівнем перешкод, як-от міські або приміські "каньйони", що виникли в результаті створення штучних споруд.

В цьому описі запропоновано системи та способи краудсорсингового виявлення та відстеження БПЛС. Як описано більш детально нижче, описані системи та способи забезпечують централізованому об'єкту відстеження БПЛС можливість прийому інформації про одну або більше БПЛС від мобільних пристроїв кількох користувачів, як-от користувачі в групі. На основі прийнятої інформації об'єкт відстеження БПЛС може виконати оцінку кожної БПЛС. Об'єкт відстеження БПЛС також може надсилати сповіщення про свої оцінки щонайменше деяким користувачам, і об'єкт відстеження БПЛС може додатково надсилати інформацію про оцінку іншим об'єктам, наприклад співробітникам правоохоронних органів.

Хоча цей опис стосується БПЛС, слід розуміти, що описані в цьому документі принципи також застосовуються до інших типів апаратів у зонах з обмеженим покриттям датчиків. Наприклад, описані варіанти здійснення також можна використовувати з пілотованими літальними апаратами (наприклад, літальним апаратом на малих висотах) і апаратами в інших областях (наприклад, морський або наземний рух).

На фіг. 1 проілюстровано типову систему 100 для краудсорсингового виявлення та відстеження БПЛС згідно з цим описом. Як показано на фіг. 1, система 100 містить кілька користувацьких пристроїв 102a-102d, щонайменше одну мережу 104, щонайменше один сервер 106 і щонайменше одну базу 108 даних. Однак слід зауважити, що в цьому разі також можуть використовуватися інші комбінації та розташування компонентів.

У цьому прикладі кожен користувацький пристрій 102a-102d з'єднаний або зв'язується з мережею 104 Зв'язок між кожним користувацьким пристроєм 102a-102d і мережею 104 може відбуватися будь-яким прийнятним способом, наприклад через дротове або бездротове з'єднання. Кожен користувацький пристрій 102a-102d являє собою будь-який прийнятний пристрій або систему, яка використовується щонайменше одним користувачем для надання інформації на сервер 106 або базу 108 даних, або для прийому інформації від сервера 106 або бази 108 даних. Ілюстративні типи інформації можуть включати в себе фотографії БПЛС, дані про місце розташування БПЛС, сигнали зв'язку або керування, пов'язані з БПЛС, тощо.

У системі 100 може використовуватися будь-яка прийнятна кількість (кількості) і тип(-и) користувацьких пристроїв 102a-102d. У цьому конкретному прикладі користувацький пристрій 102a являє собою настільний комп'ютер, користувацький пристрій 102b являє собою портативний комп'ютер, користувацький пристрій 102c являє собою смартфон, а користувацький пристрій 102d являє собою планшетний комп'ютер. Однак в системі 100 можуть використовуватися будь-які інші або додаткові типи користувацьких пристроїв. Кожен користувацький пристрій 102a-102d містить будь-яку прийнятну структуру, виконану з можливістю передачі та/або прийому інформації.

Мережа 104 полегшує зв'язок між різними компонентами системи 100. Наприклад, мережа 104 може передавати пакети Інтернет-протоколу (IP), кадри ретрансляції кадрів, елементи режиму асинхронної передачі (ATM) або іншу прийнятну інформацію між мережевими адресами. Мережа 104 може включати в себе одну або більше локальних мереж (LAN), міських мереж (MAN), глобальних мереж (WAN), всю глобальну мережу або її частину, як-от Інтернет, або будь-яку іншу систему або системи зв'язку в одному або більше місцях розташування. Мережа 104 також може працювати згідно з будь-яким відповідним протоколом або протоколами зв'язку.

Сервер 106 з'єднаний із мережею 104 і з'єднаний або іншим чином зв'язаний із базою 108 даних. Сервер 106 підтримує запит інформації із бази 108 даних і обробку цієї інформації. Звичайно, база 108 даних також може використовуватися всередині сервера 106 для зберігання інформації, і в цьому випадку сам сервер 106 може зберігати інформацію. Серед іншого, сервер 106 обробляє інформацію, яка використовується для краудсорсингового виявлення та відстеження БПЛС. Приклади операцій обробки сервера 106 наведено нижче.

Сервер 106 містить будь-яку прийнятну структуру, виконану з можливістю обробки інформації для краудсорсингового виявлення та відстеження БПЛС. У деяких варіантах здійснення сервер 106 містить один або більше процесорів, один або більше типів пам'яті та один або більше інтерфейсів зв'язку. Однак, слід зауважити, що сервер 106 може бути реалізований у будь-який прийнятний спосіб для виконання описаних функцій. Також слід зауважити, що хоча в цьому випадку пристрій(-ої), що фактично реалізує сервер 106, описано як сервер, він може являти собою один або більше настільних комп'ютерів, портативних комп'ютерів, серверних комп'ютерів або інших обчислювальних пристроїв або пристроїв чи систем обробки даних. У деяких варіантах здійснення сервер 106 може включати в себе хмарне середовище обробки або бути його частиною.

База 108 даних зберігає різну інформацію, яка використовується, створюється або збирається сервером 106 і користувацькими пристроями 102a-102d. Наприклад, база 108 даних може зберігати фотографії БПЛС, дані про місце розташування та траєкторію польоту (наприклад, шлях або траєкторію) БПЛС, сигнали зв'язку або керування, пов'язані з БПЛС, тощо. У деяких випадках щонайменше частина інформації, яка має зберігатися базою 108 даних, може бути прийнята від користувацьких пристроїв 102a-102d прямо або опосередковано, наприклад через сервер 106. У деяких випадках інформація може надходити від таких датчиків, як радари або високоефективні системи формування зображень.

Існує ряд можливих способів реалізації системи 100, щоб забезпечити описані функціональні можливості для краудсорсингового виявлення та відстеження БПЛС. Наприклад, у деяких варіантах здійснення сервер 106 і база 108 даних належать спільному об'єкту, керуються або управляються ним. В інших варіантах здійснення сервер 106 і база 108 даних належать різним об'єктам, керуються або управляються ними. Однак слід зауважити, що цей опис не обмежується будь-якою конкретною організаційною реалізацією.

Хоча на фіг. 1 проілюстровано один приклад системи 100 для краудсорсингового виявлення та відстеження

БПЛС, у фіг. 1 можуть бути внесені різні зміни. Наприклад, система 100 може містити будь-яку кількість користувацьких пристроїв 102a--102d, мереж 104, серверів 106 і баз 108 даних. Крім того, хоча на фіг. 1 проілюстровано, що одна база 108 даних з'єднана з мережею 104, будь-яка кількість баз 108 даних може перебувати в будь-якому місці розташування або місцях розташування, доступних для сервера 106, причому кожна база 108 даних може бути з'єднана прямо або опосередковано з сервером 106. Крім того, хоча на фіг. 1 проілюстровано одне типове робоче середовище, в якому можуть використовувати краудсорсингове виявлення та відстеження БПЛС, цю функціональну можливість можна використовувати в будь-якій іншій прийнятній системі.

На фіг. 2 проілюстровано типовий пристрій 200 для краудсорсингового виявлення та відстеження БПЛС згідно з цим описом. Один або більше екземплярів пристрою 200 можна, наприклад, використовувати для щонайменше часткової реалізації функціональних можливостей сервера 106, зображеного на фіг. 1. Однак функціональні можливості сервера 106 можуть бути реалізовані в будь-який інший прийнятний спосіб. Крім того, таке саме або аналогічне компонування компонентів можна використовувати для щонайменше часткової реалізації функціональних можливостей одного або більше користувацьких пристроїв 102a-102d, зображених на фіг. 1. Однак функціональні можливості кожного користувацького пристрою 102a-102d можуть бути реалізовані в будь-який інший прийнятний спосіб.

Як показано на фіг. 2, пристрій 200 позначає обчислювальний пристрій або систему, яка містить щонайменше один пристрій 202 обробки, щонайменше один запам'ятовувальний пристрій 204, щонайменше один блок 206 зв'язку і щонайменше один блок 208 вводу-виводу. Пристрій 202 обробки може виконувати команди, які можуть бути завантажені в пам'ять 210. Пристрій 202 обробки містить будь-яку прийнятну кількість(-ості) і тип(-и) процесорів або інших пристроїв у будь-якому прийнятному компонуванні. Приклади типів пристроїв 202 обробки включають у себе один або більше мікропроцесорів, мікроконтролерів, процесорів цифрових сигналів (DSP), спеціалізованих інтегральних схем (ASIC), програмованих користувачем вентильних матриць (FPGA) або дискретних схем.

Пам'ять 210 і постійне сховище 212 є прикладами запам'ятовувальних пристроїв 204, які являють собою будь-яку структуру(-и), виконану з можливістю зберігання та полегшення пошуку інформації (як-от дані, програмний код та/або інша прийнятна інформація на тимчасовій або постійній основі). Пам'ять 210 може являти собою оперативний запам'ятовувальний пристрій або будь-який інший прийнятний енергозалежний або енергонезалежний запам'ятовувальний пристрій(-ої). Постійне сховище 212 може містити один або більше компонентів або пристроїв, що підтримують довгострокове зберігання даних, як-от постійний запам'ятовувальний пристрій, жорсткий диск, флеш-пам'ять або оптичний диск.

Блок 206 зв'язку підтримує зв'язок з іншими системами або пристроями. Наприклад, блок 206 зв'язку може включати в себе плату мережевого інтерфейсу або бездротовий прийомопередавач, який полегшує зв'язок через дротову або бездротову мережу, як-от мережа 104. Блок 206 зв'язку може підтримувати зв'язок через будь-який прийнятний фізичний або бездротовий канал(-и) зв'язку.

Блок 208 вводу-виводу забезпечує ввід і вивід даних. Наприклад, блок 208 вводу-виводу може забезпечувати з'єднання для вводу користувача за допомогою клавіатури, миші, кнопкової панелі, сенсорного екрану або іншого прийнятного пристрою вводу. Блок 208 вводу-виводу також може забезпечувати з'єднання для необов'язкового "додаткового" сенсорного пристрою 214, як-от датчик або камера, який можна додати як аксесуар до пристрою 200. Блок 208 вводу-виводу також може надсилати вивідні дані на дисплей, принтер або інший прийнятний пристрій виводу. Однак, слід зауважити, що блок 208 вводу-виводу може бути опущений, якщо пристрій 200 не потребує локального вводу-виводу, наприклад, коли до пристрою 200 можна отримати віддалений доступ.

У деяких варіантах здійснення команди, що виконуються пристроєм 202 обробки, можуть включати в себе команди, які реалізують функціональні можливості сервера 106. Наприклад, команди, що виконуються пристроєм 202 обробки, можуть включати в себе команди для краудсорсингового виявлення та відстеження БПЛС. В інших варіантах здійснення команди, що виконуються пристроєм 202 обробки, можуть включати в себе команди, які реалізують функціональні можливості користувацьких пристроїв 102a-102d. Наприклад, команди, що виконуються пристроєм 202 обробки, можуть включати в себе команди для надання інформації, пов'язаної з БПЛС, на сервер 106 і для прийому сповіщень, пов'язаних з БПЛС, від сервера 106.

Хоча на фіг. 2 проілюстровано один приклад пристрою 200 для краудсорсингового виявлення та відстеження БПЛС, у фіг. 2 можуть бути внесені різні зміни. Наприклад, обчислювальні пристрої/системи та мобільні пристрої мають широку різноманітність конфігурацій, причому фіг. 2 не обмежує цей винахід будь-яким конкретним обчислювальним пристроєм чи системою або будь-яким конкретним мобільним пристроєм.

На фіг. 3 проілюстровано типове середовище 300, в якому краудсорсингове виявлення та відстеження БПЛС можуть виконуватися згідно з цим описом. Для простоти пояснення описано, що середовище 300 використовується з системою 100 на фіг. 1, яка може бути реалізована за допомогою одного або більше пристроїв 200 на фіг. 2. Однак середовище 300 може включати в себе використання будь-якого прийнятного пристрою(-їв) у будь-якій прийнятній системі(-ах).

Як показано на фіг. 3, середовище 300 включає в себе щонайменше одного користувача 302, який перебуває в зоні, де пролітає БПЛС 306. Хоча на фіг. 3 проілюстровано лише одного користувача 302, слід розуміти, що середовище 300 зазвичай включає в себе більш ніж одного користувача 302 і може включати в себе багато (наприклад, десятки, сотні або тисячі) користувачів 302, які перебувають в зоні поблизу БПЛС 306 або її траєкторії польоту. Крім того, хоча на фіг. 3 проілюстровано лише одну БПЛС 306, слід розуміти, що середовище 300 може включати в себе кілька БПЛС 306, де один або більше користувачів 302 перебувають в зоні поблизу кожної БПЛС 306 або її траєкторії польоту.

Кожен користувач 302 володіє мобільним пристроєм 304 або має до нього доступ. Кожен мобільний пристрій 304 являє собою обчислювальний пристрій або систему, яка здатна виявляти та відстежувати БПЛС, наприклад БПЛС 306. У деяких варіантах здійснення кожен мобільний пристрій 304 містить один або більше датчиків (як-от камера, датчик Wi-Fi, датчик BLUETOOTH, мікрофон тощо), виконаних із можливістю сприйняття або виявлення

інформації про БПЛС 306. Приклади типів мобільних пристроїв 304 можуть включати в себе мобільні телефони, планшетні комп'ютери, портативні комп'ютери тощо. У деяких варіантах здійснення мобільний пристрій 304 являє собою (або представлений ним) один із користувацьких пристроїв 102a-102d на фіг. 1 або пристрій 200 на фіг. 2, описаний вище.

Кожен мобільний пристрій 304 може містити програму (або "додаток") 305, встановлену на мобільному пристрої 304. Додаток 305 забезпечує графічний користувацький інтерфейс (GUI - англ.: graphical user interface) для взаємодії з користувачем 302 і програмні команди для виявлення та відстеження БПЛС. Додаток 305 також полегшує зв'язок між мобільним пристроєм 304 і сервером 310 через мережу 308 для обміну інформацією про БПЛС 306. У деяких варіантах здійснення додаток 305 забезпечено об'єктом 312, який збирає та обробляє інформацію, пов'язану з виявленням і відстеженням БПЛС. У конкретних варіантах здійснення додаток 305 видається за ліцензією кожному користувачеві 302 і встановлюється на кожному мобільному пристрої 304 як частина спільної бізнес-моделі "freemium". У такій бізнес-моделі кожен користувач 302 вважається "просьюмером" (сполучення англійських слів "producer" (виробник) і "consumer" (споживач)), оскільки користувач 302 як створює пов'язану з БПЛС інформацію для використання сервером 310, так і приймає пов'язану з БПЛС інформацію від сервера 310.

Додаток 305 дозволяє залучати багато користувачів 302, щоб вони приєдналися до спільноти та використовували технології зондування малого радіусу дії, які вже доступні в їхніх мобільних пристроях 304, для пошуку маловисотних БПЛС, як-от БПЛС 306. У деяких варіантах здійснення додаток 305 може надавати винагороду кожному користувачеві 302, який надає корисну інформацію про БПЛС 306. Наприклад, винагородою може бути кредит на покупку в додатку, доступ до інформації про помічений БПЛС 306 тощо.

У цьому прикладі БПЛС 306 являє собою невелику БПЛС, яка зазвичай працює на малих висотах і може працювати в одній або більше зонах з обмеженою видимістю, наприклад у міських або приміських зонах. У середовищі 300 БПЛС 306 перебуває в польоті та рухається по траєкторії польоту. Оскільки інформація про БПЛС 306 може бути не відразу або легко відома об'єкту 312, середовище 300 дозволяє користувачам 302 використовувати свої мобільні пристрої 304 для збору інформації про БПЛС 306 і надавати інформацію на сервер 310, який належить об'єкту 312 або керується ним.

Сервер 310 являє собою обчислювальний пристрій або систему, яка виконана з можливістю обробки інформації для виявлення та відстеження БПЛС, наприклад БПЛС 306. У деяких варіантах здійснення сервер 310 являє собою (або представлений ним) сервер 106 на фіг. 1 або пристрій 200 на фіг. 2, описаний вище. У деяких варіантах здійснення сервер 310 може являти собою хмарний сервер або групу серверів або інших обчислювальних пристроїв.

Сервер 310 виконує відстеження БПЛС 306 шляхом прийому, кореляції та обробки інформації про БПЛС 306 (як-от зображення або відео, аудіозаписи, виявлення сигналу керування, спостереження або коментарі користувача, отримані через GUI додатку 305, тощо) від мобільних пристроїв 304. У деяких варіантах здійснення інформацію можна отримати з кількох положень або кутів вимірювання. Крім того, в деяких варіантах здійснення інформація може мати тег GPS або іншим чином корелювати з інформацією про місце розташування. Сервер 310 може обробляти зібрану інформацію за допомогою алгоритму оцінки шляху, який може створювати деталі шляху БПЛС 306. Деталі шляху можуть описувати попередній і розрахунковий майбутній шлях БПЛС 306, наприклад його висоту, траєкторію польоту, швидкість тощо. Залежно від прийнятої інформації, сервер 310 може використовувати кілька елементів даних в одному або більше алгоритмах тріангуляції, щоб визначити місце розташування БПЛС 306 і відстежувати її траєкторію польоту. Наприклад, обробку кількох зображень або відеозаписів, отриманих із різних місць розташування, можна використовувати разом із алгоритмами тріангуляції для визначення місця розташування БПЛС 306. Точність відстеження може залежати від кількості та просторового розподілу мобільних пристроїв 304, якості вхідних даних датчиків і наявності інших джерел інформації для конкретного контакту БПЛС.

За допомогою інформації, прийнятої від мобільних пристроїв 304, сервер 310 також може виконувати розпізнавання БПЛС 306, наприклад, ідентифікуючи її конкретну марку, модель і корисне(-і) навантаження (якщо є). Наприклад, сервер 310 може використовувати алгоритми розпізнавання зображень і аудіо, а також спостереження людей, які вводяться через GUI додатку 305. Сервер 310 також може виконувати розпізнавання ймовірних намірів, оцінку потенційної загрози та надавати рекомендацію щодо прийнятних дій із пом'якшення наслідків одному або більше суб'єктам у спектрі. Наприклад, промисловим операторам може знадобитися тимчасово припинити роботу своїх БПЛС, правоохоронним органам може знадобитися знайти наземну станцію керування БПЛС 306 і оштрафувати або заарештувати оператора БПЛС, або федеральним агентствам може знадобитися застосувати кінетичні чи некінетичні лічильники. Крім того, сервер 310 може виконувати виявлення, визначення місця розташування та ідентифікацію наземної станції керування та оператора БПЛС 306. Це можна виконати аналогічним чином, як і у випадку розпізнавання самої БПЛС 306.

Сервер 310 виконаний із можливістю розпізнавання і оцінки потенційних загроз за допомогою одного або більше алгоритмів, як-от ті, що використовують об'єктно-орієнтоване виробництво (OBP - англ.: object-based production), орієнтовану на діяльність розвідку (ABI - англ.: activity-based intelligence) або і те, і інше. Такі алгоритми можуть виконувати початкову оцінку БПЛС 306 та її потенційну загрозу. На основі початкової оцінки сервер 310 може передати завдання іншому уповноваженому суб'єкту для подальшої оцінки загроз або пом'якшення наслідків або припинити передачу завдання, якщо оцінка вказує на низьку загрозу. У деяких випадках сервер 310 також може надсилати конкретні сповіщення одному або більше користувачам 302, щоб запитати додаткову інформацію або рекомендувати дію, як-от "шукати сховок" або "ваші польотні операції".

У деяких варіантах здійснення інформація, що надана на сервер 310, може бути агрегована як набір даних, який може задіяти один або більше алгоритмів або підпрограм штучного інтелекту (AI - англ.: artificial intelligence) або інших алгоритмів або підпрограм машинного навчання (ML - англ.: machine learning). Точність алгоритмів або підпрограм AI/ML може підвищуватися з часом, оскільки мережа користувачів 302 і мобільних пристроїв 304

зростає, таким чином забезпечуючи більшу довідкову базу даних для навчання та оцінки. Зокрема, краудсорсинг із кількома спостереженнями від кількох мобільних пристроїв 304 може задіяти спосіб підтвердження базової правдивості даних датчиків і даних людино-машинного інтерфейсу (HMI - англ.: human-machine interface), а також рішення щодо розпізнавання та оцінки загроз. Крім того, в деяких варіантах здійснення агрегований набір даних може бути упакований як продукт або послуга, які можна продавати, ліцензувати або іншим чином пропонувати зацікавленим сторонам.

Виявлення та збір інформації про БПЛС 306 може бути ініційовано щонайменше одним із користувачів 302, наприклад, коли один або більше користувачів 302 спостерігають за польотом БПЛС 306. В інших випадках ініціатором запуску процесу може бути інша стороння система (наприклад, безпілотна система керування рухом (UTM - англ.: unmanned traffic management), радарна система, система оптичного відстеження, така як мультиспектральна система наведення (MTS - англ.: Multi-Spectral Targeting System) від RAYTHEON TECHNOLOGIES CORP. тощо), що виявляє присутність неідентифікованого об'єкта. Потім ця стороння система може дати запит серверу 310 на надсилання геопросторового сповіщення про попередження користувачам 302 через додаток 305 на їхніх мобільних пристроях 304. В інших випадках тригером для запуску процесу може бути публікація в соціальних мережах про політ БПЛС в певній зоні, що може автоматично створювати геопросторове сповіщення про попередження для користувачів 302 через додаток 305.

Як один конкретний приклад, користувач 302 може спостерігати БПЛС 306 і повідомляти про спостереження на сервер 310 через мережу 308 за допомогою додатку 305. Потім сервер 310 може надіслати сповіщення групі користувачів 302 в поблизькій зоні (наприклад, у радіусі 1 кілометр від користувача 302, який спостерігає) через додаток 305. Сповіщення інформує групу користувачів 302 про будь-яку відому інформацію про БПЛС 306 і дає запит користувачам 302 на пошук БПЛС 306 і запис будь-якої можливої інформації про БПЛС 306. Наприклад, користувачі 302 можуть отримувати фотографії або відео БПЛС 306, робити аудіозаписи звуків, які видає БПЛС 306, створювати текстові коментарі про БПЛС 306 тощо. У деяких варіантах здійснення додаток 305 може контролювати один або більше внутрішніх датчиків мобільного пристрою 304 (наприклад, GPS, IMU, компас тощо), один або більше зовнішніх "додаткових" датчиків (як-от сенсорний пристрій 214) або інші додатки геопросторової зйомки (з відкритим вихідним кодом або з ліцензією), щоб отримувати інформацію (напрямок, пеленг тощо), яку можна використовувати для розрахунків створення траєкторій. Потім користувачі 302 або мобільний пристрій 304 повідомляють інформацію про БПЛС 306 на сервер 310 через додаток 305.

Сервер 310 приймає інформацію, у тому числі будь-яку інформацію про місце розташування, про БПЛС 306 і перевіряє геопросторову інформацію про простір навколо БПЛС 306, щоб визначити, чи є вразливі зони (як-от багатолюдні заходи, важливі активи, військова база тощо). Сервер 310 також сповіщає групу користувачів 302 у більшій зоні (наприклад, у радіусі 5 кілометрів від БПЛС 306) для пошуку контролера або оператора БПЛС 306. Наприклад, користувачі 302 можуть використовувати свої мобільні пристрої 304 для електронного визначення мережі або смуги передачі (як-от Wi-Fi, радіочастота (РЧ), стільниковий зв'язок тощо), в якій зв'язуються контролер і БПЛС 306. Користувачі 302 також можуть просто ходити й візуально шукати контролера або оператора БПЛС і повідомляти інформацію на сервер 310 через додаток 305.

Як тільки сервер 310 отримує інформацію про БПЛС 306 або її контролера/оператора, сервер 310 виконує оцінку БПЛС 306 і її потенційної загрози. У деяких варіантах здійснення оцінка БПЛС 306 може бути виконана за допомогою методів машинного навчання. На основі оцінки сервер 310 може передати завдання іншому уповноваженому суб'єкту для подальшої оцінки загроз або пом'якшення наслідків або припинити передачу завдання, якщо оцінка вказує на низьку загрозу. Сервер 310 може також або альтернативно надсилати інформацію про оцінку БПЛС 306 одному або більше користувачам 302, або одній або більше зацікавлених третіх сторін. Зацікавлені треті сторони можуть включати в себе співробітників правоохоронних органів, організації, відповідальні за бізнес-активи поблизу БПЛС 306 або її траєкторію польоту, власників майна тощо.

У деяких варіантах здійснення бізнес-модель freemium може включати в себе послугу на основі передплати, що надається об'єктом 312. У межах послуги на основі передплати абоненти можуть приймати більший рівень інформації про БПЛС 306. Абоненти можуть включати в себе одного або більше користувачів 302. Інші абоненти можуть включати в себе тих, хто, можливо, не зацікавлений у пошуку БПЛС, але хотів би знати про БПЛС поблизу. Наприклад, абонент може являти собою знаменитість, яка хоче знати, коли БПЛС перебуває поблизу його або її будинку. Однак слід зауважити, що підходи, описані в цьому патентному документі, не обмежуються будь-якою конкретною бізнес-моделлю чи іншим варіантом реалізації для заохочення користувачів до участі.

У середовищі 300 сервер 310 може використовувати інформацію з мобільних пристроїв 304 або з інших різнотипних джерел даних (наприклад, геопросторове відображення, бази даних кримінальних записів тощо) для інтеграції та стиснення циклу розвідки, циклу розслідування підозрілої діяльності правоохоронних органів і військового "ланцюга знищення" для спливаючих загроз БПЛС та підвищення ефективності процесів оцінки загроз та прийняття рішень щодо дій. У звичайних підходах існують численні фактори неефективності процесів, які виникають через відсутність освіти, чітких ролей, відповідальності, повноважень і рішень щодо пом'якшення наслідків. Це перешкоджає своєчасному та ефективному сповіщенню, визначенню та відповідному пом'якшенню потенційних загроз усіма суб'єктами спільноти. Середовище 300 інтегрує та стискає всі три процеси шляхом визначення чітких ролей, обов'язків, повноважень та рішень щодо пом'якшення наслідків для різних суб'єктів (у тому числі як нетрадиційних, так і традиційних суб'єктів) і шляхом зменшення конфліктів та часу, пов'язаних зі зв'язком і координацією між суб'єктами в ланцюгу знищення. Наприклад, інформація про БПЛС, що надається мобільними пристроями 304 на сервер 310, може заповнити прогалини в покритті традиційного датчика ланцюга знищення.

Середовище 300 переносить більшу частину витрат на придбання інфраструктури зондування, укомплектування і підтримку на велику потенційну мережу користувачів 302, кожен з яких має доступ до свого власного незалежного мобільного пристрою 304. Це вирішує проблеми необхідності масштабування та витрат на розгортання, укомплектування та підтримку інфраструктури зондування на низькій висоті. У міру зростання

мережі користувачів 302 збільшується масштаб покриття, що забезпечується середовищем 300. Це може бути особливо вигідним у випадку вразливих цілей, як-от великі публічні заходи.

Хоча на фіг. 3 проілюстровано один приклад середовища 300, в якому може виконуватися краудсорсингове виявлення та відстеження БПЛС, у фіг. 3 можуть бути внесені різні зміни. Наприклад, робочі середовища мають широку різноманітність конфігурацій, і фіг. 3 не обмежує цей опис будь-яким конкретним середовищем.

На фіг. 4 проілюстровано типове геопросторове представлення рішення 400 стосовно протидії БПЛС, в якому краудсорсингове виявлення та відстеження БПЛС можуть виконуватися згідно з цим описом. Для простоти пояснення описано, що рішення 400 стосовно протидії БПЛС використовується з середовищем 300 на фіг. 3 і може включати в себе систему 100 на фіг. 1. Однак рішення 400 стосовно протидії БПЛС може включати в себе використання будь-якого прийнятного пристрою(-їв), середовища (середовищ) і системи (систем).

Як показано на фіг. 4, рішення 400 стосовно протидії БПЛС включає в себе кілька груп суб'єктів 401-404. Суб'єкти 401 включають у себе традиційну протиповітряну оборону (як-от військова) для захисту від літаків, ракет тощо. Суб'єкти 402 включають у себе нові суб'єкти протиповітряної оборони, як-от військова поліція. Суб'єкти 403 включають у себе місцеві невійськові органи влади, як-от місцеві правоохоронні органи (як-от сили цивільної поліції). Суб'єкти 404 включають у себе приватні суб'єкти, як-от підприємства, промисловість, комунальні служби, зацікавлені особи (наприклад, знаменитості або особи, які дуже цінують свою конфіденційність) тощо.

Кожна група суб'єктів 401-404 має одну або більше протидій, до яких суб'єкти 401-404 можуть вдатися у випадку виявлення БПЛС. Наприклад, обидва суб'єкти 401 і 402 мають повноваження для заборони, коли спостерігається БПЛС, наприклад знищення БПЛС, втручання в роботу БПЛС тощо. Тип виконаної заборони може залежати від того, наскільки близько перебуває БПЛС до конкретного захищеного активу 406. Наприклад, залежно від того, чи входить БПЛС в зону 407 спостереження, зону 408 взаємодії або заборонену зону 409, пов'язану з активом 406, тип заборони може стати більш значущим. Кожна з зон 407-409 може бути визначена радіусом від активу 406. У деяких варіантах здійснення суб'єкти 403 і 404 не мають повноважень виконувати будь-які заборони БПЛС. Однак суб'єкти 403 і 404 можуть віддавати накази людям і підприємствам (наприклад, наказ перейти в укриття).

Рішення 400 стосовно протидії БПЛС також визначається висотними зонами 411-413, причому висотна зона 411 являє собою малу висоту (наприклад, менш ніж 400 футів), висотна зона 412 являє собою середню висоту (наприклад, від 400 футів до 2000 футів), а висотна зона 413 являє собою велику висоту (наприклад, понад 2000 футів). Звичайно, ці значення є лише прикладами, а інші варіанти здійснення можуть включати в себе різні кількості висотних зон при різних порогових значеннях. У деяких випадках описані в цьому документі системи краудсорсингового виявлення та відстеження можуть бути виконані в зоні 411 малої висоти та в зоні 407 спостереження, як показано пунктирними лініями, позначеними позицією 415. Однак можливі й інші випадки використання систем і способів краудсорсингового виявлення та відстеження.

Хоча на фіг. 4 проілюстровано один із прикладів рішення 400 стосовно протидії БПЛС, в якому може виконуватися краудсорсингове виявлення та відстеження БПЛС, у фіг. 4 можуть бути внесені різні зміни. Наприклад, рішення 400 може включати в себе будь-яку прийнятну кількість суб'єктів, зон спостереження, висотних зон і протидії.

На фіг. 5 проілюстровано спосіб згідно з цим описом. Для простоти пояснення спосіб 500 на фіг. 5 можна описати як такий, що виконується в середовищі 300 за допомогою системи 100, яка може бути реалізована за допомогою одного або більше пристроїв 200, зображених на фіг. 2. Однак спосіб 500 може включати в себе використання будь-якого прийнятного пристрою(-їв) і системи (систем) у будь-якому прийнятному середовищі(-ах).

Як показано на фіг. 5, на етапі 502 приймається сповіщення (перше сповіщення) про БПЛС, що пролітає в зоні. Сповіщення приймається від щонайменше одного з кількох користувачів або від сторонньої системи, яка виявляє присутність неідентифікованого об'єкта в зоні. Це може включати в себе, наприклад, прийом сервером 310 сповіщення про БПЛС 306 від щонайменше одного з користувачів 302 або сторонньої системи.

На етапі 504 інше сповіщення (друге сповіщення) надсилається кільком мобільним пристроям кількох користувачів, розташованих у зоні. Сповіщення дає запит користувачам на пошук БПЛС. У деяких варіантах здійснення сповіщення надається користувачам через додаток, встановлений на мобільних пристроях. Це може включати в себе, наприклад, надсилання сервером 310 сповіщення мобільним пристроям 304, яке надається користувачам 302 через додаток 305.

Ще одне сповіщення (третє сповіщення) надсилається кільком мобільним пристроям та іншим мобільним пристроям інших користувачів, розташованих у більшій зоні, на етапі 506. Сповіщення дає запит кільком користувачам та іншим користувачам на пошук контролера БПЛС або оператора БПЛС. Це може включати в себе, наприклад, надсилання сервером 310 сповіщення мобільним пристроям 304 в більшій зоні.

На етапі 508 інформація про БПЛС приймається від одного або більше мобільних пристроїв одного або більше користувачів. Інформацію отримують за допомогою одного або більше мобільних пристроїв. У деяких варіантах здійснення інформація про БПЛС включає в себе одне або більше зображень або відео БПЛС, отриманих за допомогою мобільних пристроїв, інформацію про сигнал бездротового керування від БПЛС або контролера БПЛС, виявленого за допомогою мобільних пристроїв, дані про місце розташування БПЛС, отримані за допомогою мобільних пристроїв, дані про відстеження БПЛС або їх комбінацію. Це може включати в себе, наприклад, прийом сервером 310 інформації про БПЛС 306 від мобільних пристроїв 304.

Оцінку БПЛС визначають на етапі 510 на основі інформації про БПЛС, прийнятої від одного або більше мобільних пристроїв та/або інших різнотипних джерел даних. Це може включати в себе, наприклад, визначення сервером 310 оцінки БПЛС 306 на основі інформації, прийнятої від мобільних пристроїв 304.

На етапі 512 загальне сповіщення (четверте сповіщення) надсилається щонайменше деяким із кількох мобільних пристроїв. Сповіщення містить інформацію щодо оцінки БПЛС. Це може включати в себе, наприклад, надсилання сервером 310 сповіщення про оцінку щонайменше деяким із мобільних пристроїв 304. Інформація

про оцінку, надіслана мобільним пристроям 304, може являти собою відносно загальну інформацію про БПЛС 306 (хоча вона при потребі може бути більш детальною).

На етапі 514 детальне сповіщення надсилається одній або більше третім сторонам. Сповіщення містить більш детальну інформацію щодо оцінки БПЛС, як-от конкретна детальна ідентифікаційна інформація або детальна оцінка загрози, яку становить БПЛС. Одна або більше третіх сторін можуть включати в себе щонайменше одного абонента послуги, пов'язаної із виявленням БПЛС, співробітників правоохоронних органів, щонайменше одного власника нерухомості, щонайменше один об'єкт, відповідальний за бізнес-актив поблизу БПЛС або її траєкторію польоту, або їх комбінацію. Це може включати в себе, наприклад, надсилання сервером 310 детального звітного сповіщення третім сторонам.

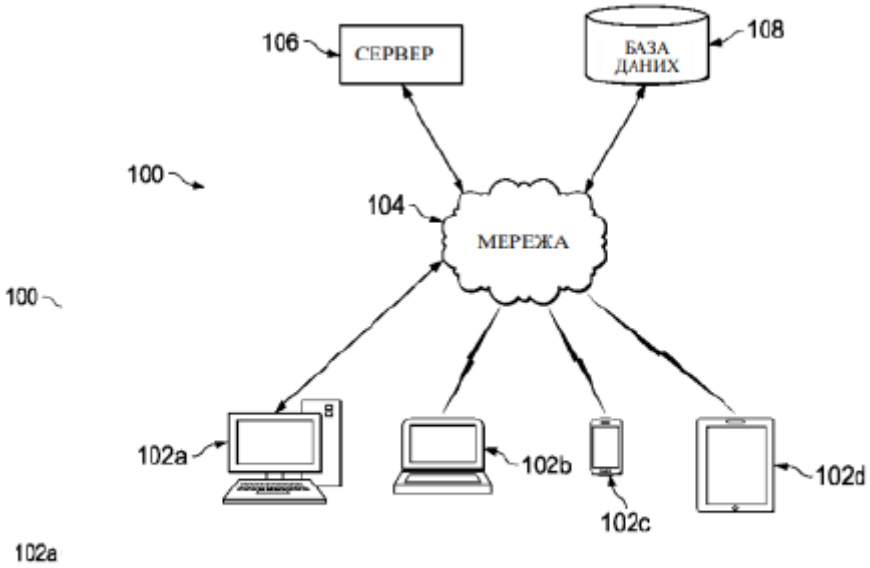
Серед іншого, у варіантах здійснення, описаних вище, пропонується розширення протиповітряної оборони за участю нетрадиційних суб'єктів, у тому числі цивільних, комерційних і правоохоронних суб'єктів. У деяких випадках інформація про БПЛС, зібрана в описаних варіантах здійснення, може заповнити прогалини у військовому ланцюгу знищення, циклі розвідки розвідувального співтовариства (IC - англ.: Intelligence Community) і циклі розслідування за звітом підозрілої діяльності правоохоронних органів. Крім того, в деяких випадках зібрану інформацію можна надавати традиційним або інституційним суб'єктам ланцюга знищення або іншим співробітникам правоохоронних органів, які мають додаткові активні повноваження щодо пом'якшення наслідків.

У деяких варіантах здійснення різні функції, описані в цьому патентному документі, реалізуються або підтримуються комп'ютерною програмою, яка формується з машиночитаного програмного коду й втілюється в машиночитаному носії. Фраза "машиночитаний програмний код" включає в себе будь-який тип комп'ютерного коду, у тому числі вихідний код, об'єктний код і виконуваний код. Фраза "машиночитаний носій" включає в себе будь-який тип носія, до якого може мати доступ комп'ютер, як-от постійний запам'ятовувальний пристрій (ROM), оперативний запам'ятовувальний пристрій (RAM), жорсткий диск, компакт-диск (CD), цифровий відеодиск (DVD) або будь-який інший тип пам'яті. "Постійний" машиночитаний носій виключає дротові, бездротові, оптичні чи інші канали зв'язку, які передають перехідні електричні або інші сигнали. Постійний машиночитаний носій включає в себе носій, на якому дані можуть зберігатися постійно, і носій, на якому дані можуть зберігатися та пізніше перезаписуватися, наприклад перезаписуваний оптичний диск або запам'ятовувальний пристрій, що стирається.

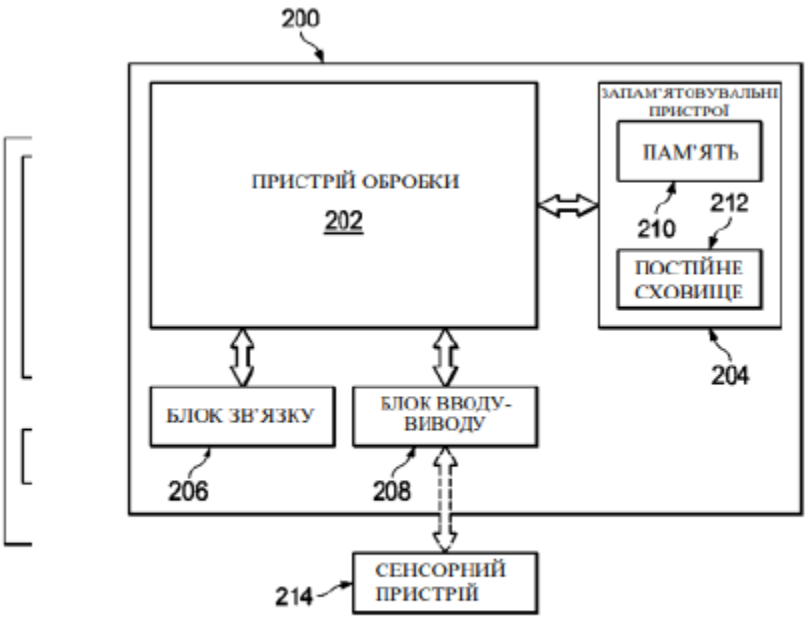
Може бути корисним викласти визначення певних слів і фраз, які використовуються в цьому патентному документі. Терміни "додаток" і "програма" стосуються однієї або більше комп'ютерних програм, програмних компонентів, наборів команд, процедур, функцій, об'єктів, класів, екземплярів, пов'язаних даних або їх частини, виконаних із можливістю реалізації в прийнятному комп'ютерному коді (у тому числі вихідному коді, об'єктному коді або виконуваному коді). Термін "зв'язуватися", а також його похідні охоплюють як прямий, так і непрямий зв'язок. Терміни "включати в себе" і "містити", а також їхні похідні означають включення без обмежень. Термін "або" є включним, означаючи "та/або". Фраза "пов'язаний з", а також її похідні можуть означати таке: включати, бути включеним всередині, взаємно зв'язуватися з, містити, міститися всередині, з'єднуватися з, зв'язуватися з, бути виконаним із можливістю зв'язку з, співпрацювати з, чергуватися, зіставляти, бути близьким до, бути пов'язаним з, мати властивість, мати взаємозв'язок з тощо. Фраза "щонайменше один з" у разі використання з переліком елементів означає, що можуть використовуватися різні комбінації одного або більше перелічених елементів і може знадобитися лише один елемент у переліку. Наприклад, "щонайменше один із: A, B і C" включає в себе будь-яку з таких комбінацій: A, B, C, A і B, A і C, B і C, а також A і B і C.

Опис у цій заявці не слід сприймати як такий, що означає, що будь-який окремий елемент, етап або функція є суттєвим або критичним елементом, який має бути включений в обсяг формули винаходу. Обсяг запатентованого об'єкта винаходу визначається лише дозволеною формулою винаходу.

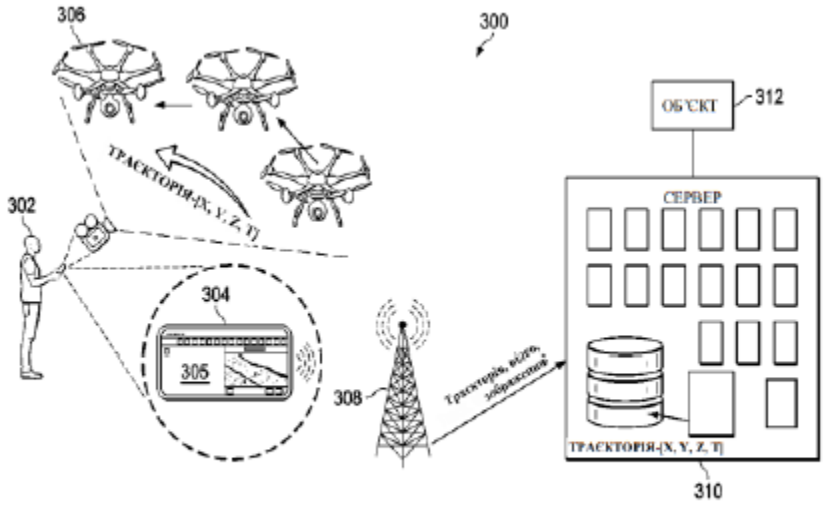
Хоча в цьому описі описано певні варіанти здійснення та загалом пов'язані з ними способи, зміни та перестановки цих варіантів здійснення та способів будуть очевидні для фахівців у цій галузі техніки. Відповідно, вищенаведений опис типових варіантів здійснення не визначає та не обмежує цього винаходу. Інші зміни, заміни та модифікації також можливі без відходу від обсягу цього опису, як визначено подальшою формулою винаходу.


106
СЕРВЕР
108
БАЗА ДАНИХ
100
104
МЕРЕЖА
100
102a
102b
102c
102d
102a

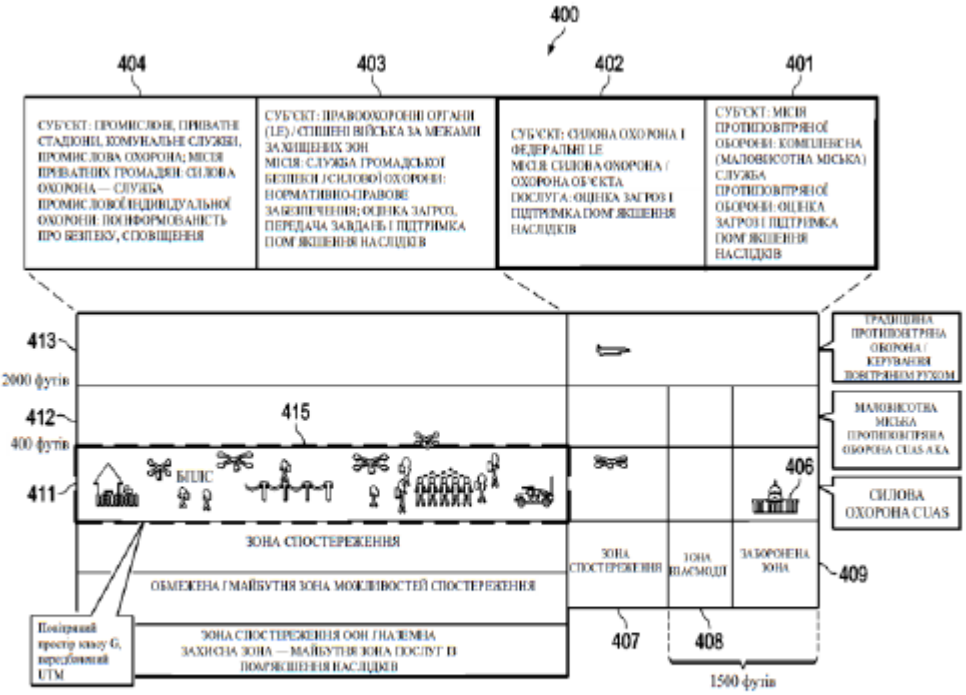
Фіг. 1


200
ЗАПАМ'ЯТОВУВАЛЬНІ ПРИСТРОЇ
ПРИСТРІЙ ОБРОБКИ
202
ПАМ'ЯТЬ
210
212
ПОСТІЙНЕ СХОВИЩЕ
204
БЛОК ЗВ'ЯЗКУ
БЛОК ВВОДУ-ВИВОДУ
206
208
СЕНСОРНИЙ ПРИСТРІЙ
214

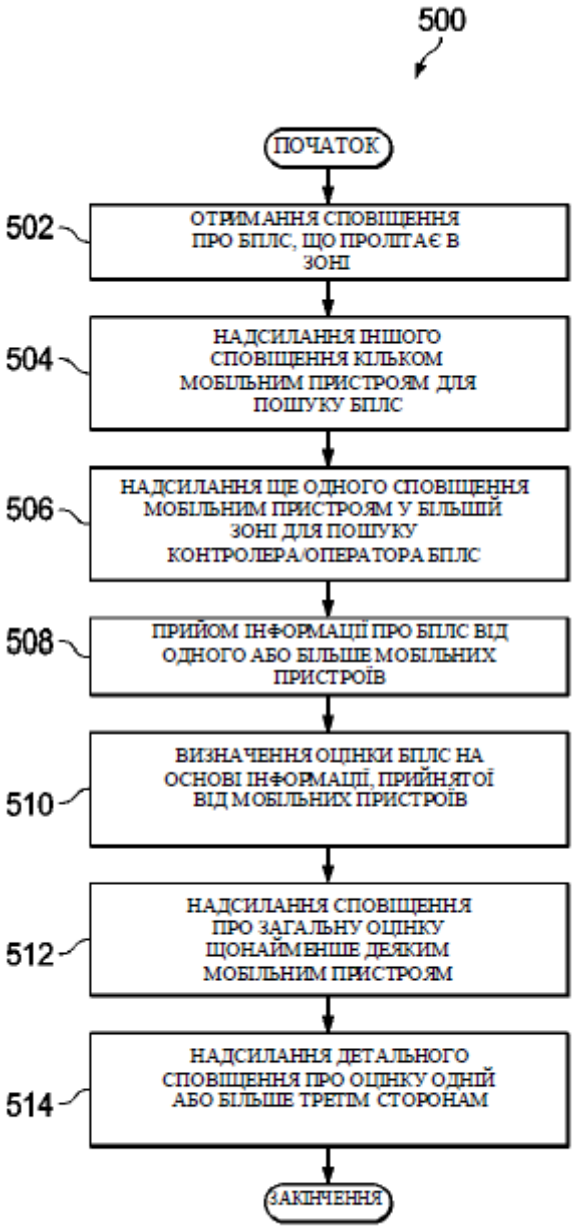
Фіг. 2


306
300
ОБ'ЄКТ
312
ТРАЄКТОРІЯ-[X, Y, Z, T]
302
СЕРВЕР
304
305
308
Траєкторія, відео, зображення
ТРАЄКТОРІЯ-[X, Y, Z, T]
310

Фіг. 3


400
404
403
402
401
СУБ'ЄКТ: ПРОМИСЛОВЕ, ПРИВАТНЕ СТАДІОНІ, КОМУНАЛЬНІ СЛУЖБИ, ПРОМИСЛОВА ОХОРОНА; МІСІЯ ПРИВАТНИХ ГРОМАДЯН: СИЛОВА ОХОРОНА — СЛУЖБА ПРОМИСЛОВОЇ/ІНДИВІДУАЛЬНОЇ ОХОРОНИ: ПОІНФОРМОВАНІСТЬ ПРО БЕЗПЕКУ, СПОВІЩЕННЯ
СУБ'ЄКТ: ПРАВООХОРОННІ ОРГАНИ (LE)/СТИШЕНІ ВІЙСЬКА ЗА МЕЖАМИ ЗАХИЩЕНИХ ЗОН
МІСІЯ: СЛУЖБА ГРОМАДСЬКОЇ БЕЗПЕКИ/СИЛОВОЇ ОХОРОНИ: НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ; ОЦІНКА ЗАГРОЗ, ПЕРЕДАЧА ЗАВДАНЬ І ПІДТРИМКА ПОМ'ЯКШЕННЯ НАСЛІДКІВ
СУБ'ЄКТ: СИЛОВА ОХОРОНА І ФЕДЕРАЛЬНІ LE
МІСІЯ: СИЛОВА ОХОРОНА / ОХОРОНА ОБ'ЄКТА
ПОСЛУГА: ОЦІНКА ЗАГРОЗ І ПІДТРИМКА ПОМ'ЯКШЕННЯ НАСЛІДКІВ
СУБ'ЄКТ: МІСІЯ ПРОТИПОВІТРЯНОЇ ОБОРОНИ: КОМПЛЕКСНА (МАЛОВИСОТНА МІСЬКА) СЛУЖБА ПРОТИПОВІТРЯНОЇ ОБОРОНИ: ОЦІНКА ЗАГРОЗ І ПІДТРИМКА ПОМ'ЯКШЕННЯ НАСЛІДКІВ
413
2000 футів
412
400 футів
411
415
БПЛІС
406
ТРАДИЦІЙНА ПРОТИПОВІТРЯНА ОБОРОНА / КЕРУВАННЯ ПОВІТРЯНИМ РУХОМ
МАЛОВИСОТНА МІСЬКА ПРОТИПОВІТРЯНА ОБОРОНА CUAS AKA
СИЛОВА ОХОРОНА CUAS
ЗОНА СПОСТЕРЕЖЕННЯ
ОБМЕЖЕНА ГМАЙБУТНЯ ЗОНА МОЖЛИВОСТЕЙ СПОСТЕРЕЖЕННЯ
ЗОНА СПОСТЕРЕЖЕННЯ ООН ГНАЛЕМІА ЗАХИСНА ЗОНА — МАЙБУТНЯ ЗОНА ПОСЛУГ ТА ПОМ'ЯКШЕННЯ НАСЛІДКІВ
Полярний простір кінцу G, передбачений UTM
ЗОНА СПОСТЕРЕЖЕННЯ
ЗОНА ПЛАСМОДІЇ
ЗАБОРОНЕНА ЗОНА
409
407
408
1500 футів

Фіг. 4


500
ПОЧАТОК
502
ОТРИМАННЯ СПОВІЩЕННЯ ПРО БПЛС, ЩО ПРОЛІТАЄ В ЗОНІ
504
НАДСИЛАННЯ ІНШОГО СПОВІЩЕННЯ КІЛЬКОМ МОБІЛЬНИМ ПРИСТРОЯМ ДЛЯ ПОШУКУ БПЛС
506
НАДСИЛАННЯ ЩЕ ОДНОГО СПОВІЩЕННЯ МОБІЛЬНИМ ПРИСТРОЯМ У БІЛЬШІЙ ЗОНІ ДЛЯ ПОШУКУ КОНТРОЛЕРА/ОПЕРАТОРА БПЛС
508
ПРИЙОМ ІНФОРМАЦІЇ ПРО БПЛС ВІД ОДНОГО АБО БІЛЬШЕ МОБІЛЬНИХ ПРИСТРОЇВ
510
ВИЗНАЧЕННЯ ОЦІНКИ БПЛС НА ОСНОВІ ІНФОРМАЦІЇ, ПРИЙНЯТОЇ ВІД МОБІЛЬНИХ ПРИСТРОЇВ
512
НАДСИЛАННЯ СПОВІЩЕННЯ ПРО ЗАГАЛЬНУ ОЦІНКУ ЩОНАЙМЕНШЕ ДЕЯКИМ МОБІЛЬНИМ ПРИСТРОЯМ
514
НАДСИЛАННЯ ДЕТАЛЬНОГО СПОВІЩЕННЯ ПРО ОЦІНКУ ОДНІЙ АБО БІЛЬШЕ ТРЕТІМ СТОРОНАМ
ЗАКІНЧЕННЯ

Фіг. 5