(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 252 728 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
06.12.2017 Bulletin 2017/49

(51) Int Cl.:
G08B 25/00 *(2006.01)*

(21) Application number: **17172597.1**

(22) Date of filing: **23.05.2017**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(30) Priority: **23.05.2016 US 201662339980 P**
28.07.2016 US 201662367657 P
04.09.2016 US 201662383432 P

(71) Applicant: **Essence Security International Ltd.**
4672530 Herzlia Pituach (IL)

(72) Inventors:
- **AMIR, Haim**
  4722625 Ramat-HaSharon (IL)
- **AMIR, Ohad**
  4642300 Herzlia (IL)

(74) Representative: **Kramer, Dani et al**
Mathys & Squire LLP
The Shard
32 London Bridge Street
London SE1 9SG (GB)

(54) SYSTEM AND METHOD FOR AN ALARM SYSTEM

(57) An alarm system (100), comprising at least one radio-frequency (RF) transceiver (102) configured to: receive a first disarm RF signal (201) from an alarm control device (103); during a predetermined delay time after receiving the first disarm RF signal, transmit at least one deception RF signal (220) during one or more transmission time slots selected from a plurality of consecutive time slots of the predetermined delay time, and determine whether one or more receive RF signals (250) are received during one or more receiving time slots selected from the plurality of consecutive time slots, the one or more receiving time slots interleaved with the one or more transmission time slots; and at least one signal processor (101), electrically connected to the at least one RF transceiver, configured to determine an alarm system operation according to analysis of the one or more receive RF signals.

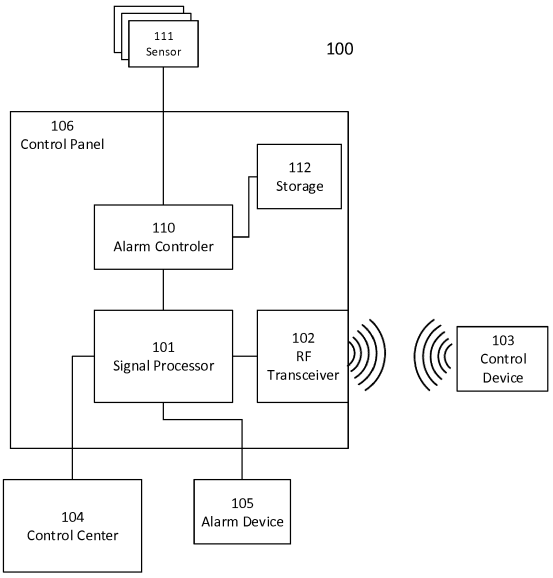


FIG. 1

EP 3 252 728 A1

Description

BACKGROUND

[0001] The present invention, in some embodiments thereof, relates to an alarm system and, more specifically, but not exclusively, to detecting an attempt at unauthorized disarming of an alarm system.

[0002] A typical alarm system installed on premises comprises one or more sensors for detecting motion, presence or intrusion, protecting one or more openings in premises or one or more areas of the premises. The protected areas may be indoors or outdoors. A gate, a door and a window are examples of possible openings protected by a sensor. The one or more sensors are typically connected to a control panel, which may be in communication with a control center. Upon detection of motion on premises, presence of a person or object on premises or an attempt at intruding the premises, for example by detecting opening of a protected opening, at least one of the sensors sends a signal to the control panel which may transmit a signal to the control center. After processing the signal, the control center may take one or more actions, for example calling an emergency center or activating an audio or visual alarm signal.

[0003] Alarm systems are installed in a wide variety of homes, offices, businesses and other locations. A typical alarm system may be in one of a plurality of possible states, including fully disabled, fully active, and partially active. For example, an alarm system may be fully disabled at an office during office business hours. When the alarm system is fully disabled, the one or more sensors may not detect movement, presence or intrusion into premises, or the control panel may not transmit a signal to the control center. An alarm may be fully active at the office after office business hours, when the office may be empty. When the alarm system is fully active, all of the one or more sensors may be active to detect movement, presence or intrusion into premises. At a house, an alarm system may be partially active at night, where some of the one or more sensors are active and some are disabled. For example, in a possible partially active state some sensors protecting exterior openings of the house such as windows and doors may be enabled, whereas other sensors for detecting motion in rooms of the house may be disabled, to allow persons living in the house to move freely in the house. Alternatively, the control panel may receive all sensor indications but may transmit to the control center only the relevant indications.

[0004] In some alarm systems, the plurality of states are controlled using one or more radio frequency (RF) signals. In such systems, the control panel typically includes a signal processor to receive one or more RF signals from a control device, for example a key fob having a plurality of buttons for controlling the state of the alarm system. In such systems, a person may press one of the plurality of buttons of the key fob to instruct the alarm system to change state to a requested state, resulting in the key fob sending an RF signal indicative of the requested state to the signal processor. Upon reception of the signal, the signal processor processes the signal, identifies the requested state and instructs changing the state of the alarm system to the requested state.

SUMMARY

[0005] It is an object of the present invention to provide a system and method for detecting an attempt at unauthorized disarming of an alarm system.

[0006] The foregoing and other objects are achieved by the features of the independent claims. Further implementation forms are apparent from the dependent claims, the description and the figures.

[0007] Aspects and embodiments of the present invention are set out in the appended claims. These and other aspects and embodiments of the invention are also described herein.

[0008] According to a first aspect of the invention, an alarm system, comprises at least one radio-frequency (RF) transceiver and at least one signal processor, electrically connected to the at least one RF transceiver. The at least one RF transceiver is configured to: receive a first disarm RF signal from an alarm control device; and during a predetermined delay time after receiving the first disarm RF signal, transmit at least one deception RF signal during one or more transmission time slots selected from a plurality of consecutive time slots of the predetermined delay time, and determine whether one or more receive RF signals are received during one or more receiving time slots selected from the plurality of consecutive time slots, the one or more receiving time slots interleaved with the one or more transmission time slots. The at least one signal processor is configured to determine an alarm system operation according to analysis of the one or more receive RF signals.

[0009] According to a second aspect of the invention, a method for an alarm system, comprises: receiving a first disarm RF signal from an alarm control device; during a predetermined delay time after receiving the first disarm RF signal, transmitting at least one deception RF signal during one or more transmission time slots selected from a plurality of consecutive time slots of the predetermined delay time, and determining whether one or more receive RF signals are received during one or more receiving time slots selected from the plurality of consecutive time slots, the one or more receiving time slots interleaved with the one or more transmission time slots; and determining an alarm system operation according to analysis of the one or more receive RF signals.

[0010] With reference to the first and second aspects, in a first possible implementation of the first and second aspects of the present invention the analysis comprises: matching at least one of the one or more receive RF signals with a predefined deception signal pattern; producing a true deception detection indication for each one

of the one or more receive RF signals matching the predefined deception signal pattern; and selecting the alarm system operation according to the true deception detection indication. Detecting one deception signal is sufficient to identify an attempted intrusion.

[0011] With reference to the first and second aspects, in a second possible implementation of the first and second aspects of the present invention the analysis comprises: producing a false deception detection indication subject to none of the one or more receive RF signals being received during the one or more receiving time slots or each one of the one or more receive RF signals failing to match the predefined deception signal pattern; and selecting the alarm system operation according to the false deception detection indication. When no RF signals are detected during the receiving slots, or when none of the one or more received RF signals match the predefined deception signal pattern, no deception is detected.

[0012] With reference to the first and second aspects, or to the first and second implementations of the first and second aspects, in a third possible implementation of the first and second aspects of the present invention the at least one signal processor is further configured to: determine the first disarm RF signal is valid, subject to not receiving any of the one or more receive RF signals or producing only false deception detection indications; and receive a second disarm RF signal from the alarm control device after the predetermined delay time. Upon receiving the second disarm RF signal, the alarm system operation comprises at least one of: instructing disarming the alarm system, and transmitting an acknowledgement RF signal to the alarm control device via the at least one RF transceiver. After identifying a valid disarm signal, also the retry may be considered valid.

[0013] With reference to the first and second aspects, in a fourth possible implementation of the first and second aspects of the present invention the transmission time slots are selected at random by the signal processor upon reception of the first disarm RF signal for transmitting the at least one deception RF signal, and the reception time slots comprise all of the plurality of consecutive time slots different from the transmission time slots. Selecting a random pattern of transmitting slots reduces the probability of repeating the same sequence and increases the probability of detecting a recorded deception signal in one of the receiving slots. Listening for received signals during all remaining time slots increases probability of detecting a retransmitted deception sequence.

[0014] With reference to the first and second aspects, in a fifth possible implementation of the first and second aspects of the present invention an amount of the transmission time slots is between 15% and 30% of an amount of the plurality of consecutive time slots. This ratio allows a balance between high probability of detecting a deception and reducing overhead of frequently changing between transmission and reception.

[0015] With reference to the first and second aspects, in a sixth possible implementation of the first and second aspects of the present invention the predetermined delay time is partitioned into 25 consecutive time slots. This amount of consecutive time slots allows a balance between high probability of detecting a deception and reducing overhead of frequently changing between transmission and reception.

[0016] With reference to the first and second aspects, in a seventh possible implementation of the first and second aspects of the present invention the at least one deception RF signal is protected by an error detecting code being a 16-bit cyclic redundancy check. Protecting the at least one deception RF signal reduces the probability of falsely detecting deception. 16-bit cyclic redundancy check is easy to implement and introduces little overhead to processing and bandwidth.

[0017] With reference to the first and second aspects, in an eighth possible implementation of the first and second aspects of the present invention the at least one deception RF signal is encrypted using a method selected from the group of: obfuscation, exclusive-or with a predefined seed word, and exclusive-or with a random seed word. Encrypting the at least one deception RF signal reduces the probability of an unauthorized party distinguishing between the at least one deception RF signal and the disarm RF signal. Obfuscation and exclusive-or are easy to implement and introduce little overhead to processing and bandwidth.

[0018] With reference to the first and second aspects, in a ninth possible implementation of the first and second aspects of the present invention alarm system operation comprises at least one operation selected from the group comprising: notifying a control center operatively connected to said at least one signal processor of an attempted intrusion, subject to producing at least one true deception detection indication and delivering an electrical current to a device capable of emitting an audio signal or a visual signal, electrically connected to said at least one signal processor, subject to producing at least one true deception detection indication.

[0019] With reference to the first and second aspects, or to the first implementation of the first and second aspects, in a tenth possible implementation of the first and second aspects of the present invention the at least one deception RF signal comprises at least one of: an identifier, a time stamp and a random number, for use in identifying an origin of a recorded deception RF signal. Optionally, the identifier consists of 32 binary bits, the time stamp consists of 32 binary bits, and the random number consists of 8 binary bits. Optionally, matching the predefined deception signal pattern comprises detecting in the one received RF signal at least one of: an identifier, a time stamp and a random number.

[0020] With reference to the first and second aspects, or to the first implementation of the first and second aspects, in an eleventh possible implementation of the first and second aspects of the present invention the analysis further comprises: detecting a packet number in the first

disarm RF signal; comparing a difference between the packet number and a previously stored packet number with a predefined threshold number; and producing a true deception detection indication when the difference is greater than the predefined threshold number. Adding a packet number to the disarm RF signal provides an additional means for detecting resending a recorded signal by detecting a repeated packet number.

[0021] Other systems, methods, features, and advantages of the present disclosure will be or become apparent to one with skill in the art upon examination of the following drawings and detailed description. It is intended that all such additional systems, methods, features, and advantages be included within this description, be within the scope of the present disclosure, and be protected by the accompanying claims.

[0022] Unless otherwise defined, all technical and/or scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, exemplary methods and/or materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and are not intended to be necessarily limiting.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0023] Some embodiments of the invention are herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of embodiments of the invention. In this regard, the description taken with the drawings makes apparent to those skilled in the art how embodiments of the invention may be practiced.

[0024] In the drawings:

FIG. 1 is a schematic illustration of an exemplary system according to some embodiments of the present invention;

FIGs. 2A, 2B, 2C, and 2D are schematic illustrations of exemplary RF signals with respect to time, according to some embodiments of the present invention;

FIG. 3 is a flowchart schematically representing an optional flow of operations for detecting an intrusion attempt using interleaved transmission and reception of a deception signal, according to some embodiments of the present invention;

FIG. 4 is a flowchart schematically representing an optional flow of operations for detecting an intrusion attempt using RF signal imperfections of a signal, according to some embodiments of the present invention;

FIG. 5 is a flowchart schematically representing another optional flow of operations for detecting an intrusion attempt using RF signal imperfections of a signal, according to some embodiments of the present invention;

FIG. 6 is a flowchart schematically representing an optional flow of operations for producing reference signal imperfections, according to some embodiments of the present invention; and

FIGs. 7A and 7B are time sequences schematically representing an optional flow of operations for detecting an intrusion attempt using an invalid instruction, according to some embodiments of the present invention.

DETAILED DESCRIPTION

[0025] The present invention, in some embodiments thereof, relates to an alarm system and, more specifically, but not exclusively, to detecting an attempt at unauthorized disarming of an alarm system.

[0026] As used herein, the term "disarm" means "instructing to change to a disabled or a partially active state" and the term "signal" means "RF signal".

[0027] Attempts to intrude into a premises protected by an alarm system may include attempts to break through any component of the alarm system.

[0028] A typical RF signal may be detected and recorded in an identified range of distances from a device sending the RF signal. In an alarm system controlled using one or more radio frequency (RF) signals, a person unauthorized to access the premises may record a legitimate signal sent by an alarm control device instructing to disarm the alarm system, and retransmit the recorded signal at a later time. A typical alarm system cannot distinguish between the original legitimate signal and the recorded signal, and upon reception of the recorded signal the alarm system's signal processer may instruct disarming the alarm system. Thus, a recorded signal may be used to gain unauthorized access to premises.

[0029] Authentication solutions using encrypted signals or including predefined information in one or more signals transmitted by an alarm control device are limited in that they require replacing multiple existing alarm control devices, for example replacing existing key fobs with alarm control devices supporting encryption or predefined information. In addition, alarm control devices supporting encryption or sending predefined information may be more expensive than existing simple alarm control devices such as existing key fobs.

[0030] The present invention, in some embodiments thereof, enables an alarm system to distinguish between a legitimate signal and retransmission of a previously recorded signal, without requiring a specially configured alarm control device, by changing the way the signal processor operates.

[0031] In some embodiments of the present invention, the signal processor, after receiving a disarm signal from

an alarm control device, sends one or more deception signals. An attempt to record the disarm signal will record the one or more deception signals as well. When transmitting the recorded signal, the one or more deception signals are transmitted as well and may be received by the signal processor. In these embodiments, the signal processor interchangeably transmits the one or more deception signals and checks for reception of one or more other signals. When one or more of the other signals are determined to be deception signals, the signal processor determines an attempt at unauthorized intrusion.

[0032] In other embodiments of the present invention, the signal processor analyzes the RF signal imperfections of a received disarm signal for imperfections. A typical signal transmitted by an alarm control device comprises a sequence of digital bits encoded in an analog carrier signal comprising a plurality of sinus signal components. When an RF transceiver encodes digital bits in an analog carrier signal and transmits the resulting RF signal, the transceiver introduces noise into the transmitted signal, including at least one of a frequency imperfection of a sinus signal, a phase imperfection of a sinus signal and an amplitude imperfection of a sinus signal. For example: carrier frequency offset, phase noise, in-phase and quadrature (IQ) imbalance and signal nonlinearity (that is, nonlinear changes in an output signal strength in response to an input signal strength). Such noise, referred to as RF signal imperfections, is signal imperfection of the RF transceiver and may be quantified, combined and normalized, resulting for example in a number between 0 and 1. Two RF transceivers are typically characterized by distinctively different RF signal imperfections. A recorded disarm signal typically comprises a recorded sequence of digital bits. When an unauthorized alarm control device transmits a recorded disarm signal, the unauthorized alarm control device re-encodes the recorded sequence of digital bits in a new analog carrier signal. The RF signal imperfections of the signal transmitted by the unauthorized alarm control device will be different from the RF signal imperfections of the original disarm signal, resulting in the RF imperfections of the signal transmitted by the unauthorized alarm control device being different from the RF imperfections of the original disarm signal. In these embodiments, the signal processor compares the RF imperfections of a received preamble signal to a predetermined set of RF imperfections associated with legitimate transmitters. When the RF imperfections of the received preamble signal do not comply with the predetermined set of RF imperfections, the signal processor determines in these embodiments an attempt at unauthorized intrusion.

[0033] In other embodiments of the present invention, the alarm control device is configured to send a signal indicating an event, and receive a signal including an identification of a function to be executed by the alarm control device. For example the alarm control device may be a key fob, configured to send a signal indicating a button pressed and a duration, for example "short press on button 1", and receive a signal including an encoding of an identification of a function, for example "function 3". A possible function is to turn on a light emitting diode (LED) for a predetermined period of time. Optionally, upon receiving a signal including an encoding of an identification of a function unrecognized by the alarm control device, the alarm control device sends an error message indicating an error and the identification of the unrecognized function. In these embodiments, the signal processor, after receiving a disarm signal from an alarm control device, sends a deception signal including a randomly selected identifier of an invalid function. An attempt to record the disarm signal will record the deception signal as well. When transmitting the recorded signal, the deception signal is transmitted as well and may be received by the signal processor. In these embodiments, after transmitting a deception signal including an invalid-function identifier, the signal processor checks for reception of another signal. When another signal is received, the received signal is processed to extract a possible unknown-function identifier. When an unknown-function identifier is extracted, the extracted identifier is compared with the invalid-function identifier. When the extracted identifier is other than the invalid-function identifier, the signal processor determines in these embodiments an attempt at unauthorized intrusion, since the extracted identifier is assumed to be the result of a pre-recorded signal.

[0034] Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not necessarily limited in its application to the details of construction and the arrangement of the components and/or methods set forth in the following description and/or illustrated in the drawings and/or the Examples. The invention is capable of other embodiments or of being practiced or carried out in various ways.

[0035] The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

[0036] The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing.

[0037] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network.

[0038] The computer readable program instructions

may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

[0039] Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

[0040] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

[0041] Reference is now made to FIG. 1, showing a schematic illustration of an exemplary system 100 according to some embodiments of the present invention. In such embodiments, system 100 comprises one or more sensors 111, for detecting motion within premises, presence within the premises or intrusion into an opening of the premises. One or more sensors 110 may be connected to a control panel 106 comprising alarm controller 110 comprising at least one hardware processor. Optionally, alarm controller 110 is configured to instruct activation of the one or more sensors and disabling the one or more sensors.

[0042] In addition, in such embodiments system 100 comprises a signal processor 101 connected to alarm controller 110 for controlling the system. Signal processor 101 may be electrically connected to alarm controller 110. Optionally, signal processor 101 is connected to alarm controller 110 via a digital communication network, such as a Local Area Network. Optionally, signal processor 101 is electrically connected to alarm controller 110.

[0043] Optionally, signal processor 101 is electrically connected to an RF transceiver 102, for communicating with one or more alarm control devices 103 such as key fobs. Optionally, signal processor 101 comprises at least one hardware processor. In such embodiments RF transceiver 102 receives one or more RF signals from alarm control device 103. Optionally, each of the one or more RF signals encodes a sequence of digital bits in an analog carrier signal. Optionally, one or more of the RF signals is a disarm message, sent from alarm control device 103 to signal processor 101 to instruct disarming alarm system 100. Optionally, signal processor 101 processes the disarm message to determine whether the message is a valid message received from an authorized alarm control device, or an unauthorized intrusion attempt. Upon determining a valid disarm message, signal processor 101 may instruct disarming alarm system 100. Optionally, signal processor 101 instructs alarm controller 110 to disarm the system.

[0044] In some embodiments, signal processor 101 is electrically connected to one or more alarm devices 105 capable of emitting an audio signal such as an alarm sound, and/or a visual signal such as a flashing light, to attract the attention of a person close enough to one or more alarm devices 105 to notice the alarm signal or visual signal. Optionally, upon detecting an intrusion attempt, signal processor 101 drives an electrical current to one or more alarm devices 105 to emit the audio or visual signal. In some embodiments, signal processor 101 is connected to one or more control centers 104, comprising at least one hardware processor. Optionally, upon detecting an intrusion attempt, signal processor 101 notifies control center 104 of the intrusion attempt detection. Following receiving notification of an intrusion attempt detection, control center 104may perform one or more actions such as call a designated person, record an event to an event log, etc.

[0045] In some embodiments, signal processor 101 is electrically connected to a non-volatile digital storage 112 such as a hard disk or an electrically erasable programmable memory, for the purpose of storing reference data used to determine validity of a received message.

[0046] To determine whether a received message is valid, system 100 may implement one or more of the following methods.

[0047] A possible method to detect an intrusion attempt uses interleaved transmission and reception of a deception signal.

[0048] Reference is now made also to FIG. 2A, showing a schematic illustration of an exemplary RF disarm signal transmitted by an alarm control device 103 to a signal processor 101, according to some embodiments of the present invention. Following time line 210, at time 211 alarm control device 103 transmits in such embodiments a first disarm message 201. Optionally, time 212 indicates the time at which alarm control device 103 completed transmission of disarm message 201. Optionally, after a predetermined delay time after time 212, if alarm control device 103 does not receive an acknowledgement signal from signal processor 101 alarm control device 103 transmits a second disarm message 202 at time 214.

[0049] Upon receiving a disarm message, in some embodiments of the present invention signal processor 101 transmits a deception signal. Reference is now made also to FIG. 2B, showing a schematic illustration of a possible deception RF signal transmitted by a signal processor 101 via an RF transceiver 102, according to some embodiments of the present invention. In such embodiments, the predetermined delay time is partitioned into a plurality of consecutive time slots. A non-limiting example of an amount of time slots is 25 time slots. Optionally, time 213 indicates the earliest time at which RF transceiver 102 receiving disarm message 201 can start transmitting. Optionally, signal processor 101 selects a group of transmission time slots from the plurality of consecutive time slots and transmits one or more deception sequences 220 by transmitting in each of the transmission time slots one deception sequence. A recorder recording the signals transmitted to signal processor 101 will record both disarm message 201 and the one or more deception sequences 220. Reference in now made also to FIG. 2C, showing a schematic illustration of a possible recorded RF signal, according to some embodiments of the present invention. In such embodiments, the recorded signal 230 comprises disarm message 201, and the one or more deception sequences 220 transmitted by signal processor 101.

[0050] Optionally, the group of transmission slots is selected at random by signal processor 101 upon receiving a disarm message, and comprises fewer slots than the plurality of consecutive time slots. For example, the amount of transmission slots is between 15% and 30% of the amount of slots in the plurality of consecutive time slots. For example, the amount of transmission slots is 25% of the amount of slots in the plurality of consecutive time slots. For example, when the predetermined delay time is partitioned into 25 time slots, the amount of transmission time slots may be 5.

[0051] In some embodiments, an unauthorized alarm control device transmitting a recorded signal transmits the disarm message originally transmitted by an authorized alarm control device, followed by the one or more disarm sequences as previously transmitted by the signal processor.

[0052] Reference is now made also to FIG. 2D, showing a schematic illustration of a possible retransmitted recorded RF signal, compared to a new deception signal, according to some embodiments of the present invention. In such embodiments, an alarm control device 105 transmits at time 241 a recorded signal 250, comprising a disarm signal 201 originally transmitted by an authorized alarm control device. Optionally, transmission of disarm signal 201 ends at time 242. Upon reception of disarm message 201, signal processor 101 selects a new group of transmit slots from the plurality of consecutive time slots between time 243 and time 244, and transmits via RF transceiver 102 one or more deception signals 260. The new group of transmit slots may be different from the group of transmit slots in the recorded signal. Optionally, RF transceiver 102 listens for received signals in a group of receive time slots selected from the plurality of consecutive time slots such that the receive time slots are different from the new group of transmit time slots and are interleaved with the new group of transmit time slots. In some embodiments the receive time slots are all of the plurality of consecutive time slots not in the new transmit time slots. When transmit time slots are selected at random, there is a probability greater than zero that the new group of transmit time slots is different from the group of time slots in the recorded signal. Depending on the number of time slots and the number of transmit time slots, the probability can exceed 0.99. As a result, signal processor 101 optionally detects one or more recorded deception sequences during the receive time slots, for example in slot 262. Optionally, one or more time slots are both in the new group of transmit time slots and in the group of transmit time slots in the recorded signal, for example slot 261. In such slots, signal processor 101 cannot detect a deception signal, since transceiver 102 is transmitting.

[0053] Detecting a deception signal in a receive time slot indicates a high probability that the disarm signal is a recorded signal retransmitted by an unauthorized alarm control device. Depending on the amount of time slots in the plurality of consecutive time slots and the amount of transmit time slots, detecting no deception signal in any of the receive time slots indicates a high probability that the disarm signal was transmitted by an authorized alarm control device. For example, when the plurality of consecutive time slots comprises 25 time slots and the group of transmit time slots comprises 5 time slots, the probability of repeating the exact same group of time slots is less than 1 in 50,000. Using fewer time slots in the plurality of consecutive time slots increases the probability of repeating an exact same group of time slots. A greater amount of time slots in the plurality of consecutive time slots or a greater amount of transmit slots may increase security by reducing the probability of repeating an exact same group of time slots, but in addition might increase power consumption due to more frequently switching the RF transceiver between transmitting and receiving.

[0054] Following is an optional method implemented by system 100 in some embodiments of the present in-

vention, to detect an intrusion attempt using interleaved transmission and reception of a deception signal.

[0055] Reference is now made also to FIG. 3, showing a flowchart schematically representing an optional flow of operations 300 for detecting an intrusion attempt using interleaved transmission and reception of a deception signal, according to some embodiments of the present invention.

[0056] In such embodiments, an RF transceiver 102 electrically connected to a signal processor 101 receives at 301 a first disarm RF signal from an alarm control device 103. Optionally, after transmitting the first disarm RF message, alarm control device 103 waits for an acknowledgement from signal processor 101 for a predetermined delay time. Optionally, signal processor 101 partitions the predetermined delay time into a plurality of consecutive time slots, for example 25 time slots. During the predetermined delay time, optionally signal processor 101 transmits at 302 one or more deception RF signals during transmission time slots selected from the plurality of consecutive time slots. Optionally, each of the one or more deception RF signals comprises at least one of an identifier, a time stamp and a random number. An identifier may be used to identify the origin of a deception RF signal, and in particular a recorded RF signal. A time stamp may be used to identify an original time of a recorded deception RF signal. A random number may be used to detect repeated deception RF signals, having the same random number. A time stamp and an identifier may each consist of 32 digital bits. A random number may consist of 8 digital bits. Optionally, each of the one or more deception RF signals comprises a packet number in a sequence of packet numbers. The packet number may consist of an 8 bit digital number. When the packet number consists of 8 digital bits, the packet number is a number in a sequence modulo 256.

[0057] In addition, during the predetermined delay time, signal processor 101 optionally intercepts at 303 a plurality of RF signals during receiving time slots selected from the plurality of consecutive time slots and interleaved with the transmission time slots. When one or more receive RF signals are detected in the receive time slots, RF transceiver 102 optionally sends the one or more RF signals to signal processor 101. Optionally, signal processor 101 receives the one or more RF signals and analyzes the first disarm RF signal and the one or more RF signals to produce at least one deception detection indication. In some embodiments, analyzing the one or more RF signals comprises matching at 304 at least one of the one or more RF signals with a predefined deception signal pattern. In embodiments where the one or more deception sequences comprise at least one of an identifier, a time stamp and a random number, matching one of the RF signals with the predefined deception signal pattern comprises detecting in the one RF signal at least one of an identifier, a time stamp and a random number. When one of the RF signals matches the predefined deception signal pattern, signal processor 101 produces at 305 a true deception detection indication. In embodiments where the first disarm RF message comprises a packet number, signal processor 101 may store a last packet number received. In such embodiments, analyzing the first disarm RF message comprises detecting a packet number in the first disarm RF message and comparing a difference between the stored packet number and the detected packet number with a predefined threshold number. When the difference is greater than the predefined threshold number, signal processor 101 optionally produces a true deception detection indication.

[0058] At 314, signal processor 101 optionally determines an alarm system operation according to the at least one deception detection indication. Examples of an alarm system operation are processing a message, sending an acknowledgement signal, instructing disarming the alarm system, sounding an alarm and notifying a control center. When at least one true deception detection indication is produced, signal processor 101 optionally determines an intrusion attempt at 308. Optionally, signal processor 101 next notifies control center 104 at 309. Optionally, at 310 signal processor 101 delivers an electrical current to one or more alarm devices 105 capable of emitting an audio signal or a visual signal.

[0059] When no true deception detection indication is produced, signal processor 101 optionally determines a valid first disarm RF signal. Optionally, signal processor 101 determines a valid first disarm RF signal when no RF signals are received in the receive time slots. In some embodiments, after the predefined delay time alarm control device 103 sends a second disarm RF signal. Optionally, signal processor 101 receives the second disarm signal via RF transceiver 102 at 311 after determining a valid first disarm RF signal, and at 312 optionally sends alarm control device 103 an acknowledgment RF signal. Optionally, signal processor 101 instructs disarming the alarm system at 313.

[0060] In some embodiments the at least one deception RF signal is protected by an error detecting code. Optionally, the error detecting code is a 16-bit cyclic-redundancy-check. In some embodiments the at least one deception RF signal is encrypted. Optionally, the at least one deception RF signal is encrypted using obfuscation. Optionally, the at least one deception RF signal is encrypted using exclusive-or with a predefined seed word or with a random seed word.

[0061] Up to a predetermined number of RF signals received during one or more of the receive time slots and not recognized as a deception RF signal may be discarded and ignored by signal processor 101.

[0062] Another possible method to detect an intrusion attempt uses RF imperfections of a signal. Following is an optional method implemented by the system in some embodiments of the present invention, to detect an intrusion attempt using RF imperfections of a signal.

[0063] Reference is now made also to FIG. 4, showing a flowchart schematically representing an optional flow

of operations 400 for detecting an intrusion attempt using RF imperfections of a signal, according to some embodiments of the present invention. In some embodiments, a signal transmitted by an alarm control device comprises a sequence of digital bits encoded in an analog carrier signal. Optionally, the signal comprises a preamble and/or a code word before a message. Optionally, an RF transceiver 102 receives at 401 a preamble RF signal from an alarm control device 103. The preamble RF signal comprises a sequence of preamble digital bits encoded in an analog preamble carrier signal. Optionally, RF transceiver 102 sends the received preamble RF signal to a signal processor 101 and at 402 signal processor 101 analyzes the preamble RF signal to determine a plurality of preamble imperfections of the analog preamble carrier signal. Examples of preamble imperfections are an offset of a frequency of the analog preamble carrier signal, a phase noise in the analog preamble carrier signal, an IQ imbalance in the analog preamble carrier signal, and nonlinearity on the analog preamble carrier signal. For example, a level of sinus signal inaccuracy in the sinuses making up the analog preamble carrier signal's (that is, an offset of a frequency of the analog preamble carrier signal) may be expressed as a normalized range of numbers. For example, a sub-range between 0 and 1, for example 0.7-0.72. At 403, the signal processor optionally compares the plurality of preamble imperfections to a plurality of reference preamble imperfections to determine preamble compliance. In some embodiments signal processor 101 uses a correlator having a sample rate of 16 bits per second to compare the plurality of preamble imperfections to the plurality of reference preamble imperfections. At 404 signal processor 101 optionally selects an alarm system operation to perform according to the preamble compliance. When the plurality of preamble imperfections do not comply with the plurality of reference preamble imperfections, signal processor 101 optionally determines an intrusion attempt at 407. Optionally, signal processor 101 next notifies a control center 104 at 410. Optionally, at 411 signal processor 101 delivers an electrical current to one or more alarm devices 105 capable of emitting an audio signal or a visual signal.

[0064] When the plurality of preamble signal imperfections comply with the reference plurality of preamble signal imperfections, signal processor 101 optionally determines a valid message. When a message is received at 408 after determining a valid message, signal processor 101 at 409 optionally processes the message. When the message is a disarm message, signal processor 101 optionally instructs disarming the alarm system, for example by instructing an alarm controller 110.

[0065] Optionally, RF transceiver 102 receives a synchronization word (sync-word) after the preamble. Reference is now made also to FIG. 5, showing a flowchart schematically representing another optional flow of operations 500 for detecting an intrusion attempt using RF signal imperfections of a signal, according to some embodiments of the present invention. In such embodiments, after receiving the preamble RF signal, signal processor 101 receives via RF transceiver 102 a sync-word RF signal at 501. The sync-word RF signal comprises a sequence of sync-word digital bits encoded in an analog sync-word carrier signal. Optionally, at 502 signal processor 101 analyzes the sync-word RF signal to determine a plurality of sync-word signal imperfections of the analog sync-word carrier signal. Examples of sync-word signal imperfections are an offset of a frequency of the analog sync-word carrier signal, a phase noise in the analog sync-word carrier signal, an IQ imbalance in the analog sync-word carrier signal and nonlinearity on the analog sync-word carrier signal. For example, a level of sinus signal inaccuracy in the sinuses making up the analog sync-word carrier signal's (that is, an offset of a frequency of the analog code-word carrier signal) may be expressed as a range. For example, a sub-range between 0 and 1, for example 0.7-0.72. At 506, signal processor 101 optionally compares the plurality of sync-word signal imperfections to a plurality of reference sync-word signal imperfections to determine sync-word compliance. In some embodiments signal processor 101 uses a correlator having a sample rate of 16 bits per second to compare the plurality of sync-word signal imperfections to the plurality of reference sync-word signal imperfections. At 503 signal processor 101 optionally selects an alarm system operation to perform according to the sync-word compliance. When the plurality of sync-word signal imperfections do not comply with the plurality of reference sync-word signal imperfections, signal processor 101 optionally determines an intrusion attempt at 407. Optionally, signal processor 101 next notifies control center 104 at 410. Optionally, at 411 signal processor 101 delivers an electrical current to one or more alarm devices 105 capable of emitting an audio signal or a visual signal.

[0066] When the plurality of sync-word signal imperfections comply with the reference plurality of sync-word signal imperfections, signal processor 101 optionally determines a valid message. When a message is received at 408 after determining a valid message, signal processor 101 at 409 optionally processes the message. When the message is a disarm message, signal processor 101 optionally instructs disarming the alarm system, for example by instructing alarm controller 110.

[0067] In some other embodiments, signal processor 101 determines a valid message when only one of the sync-word compliance and preamble compliance is true.

[0068] In some embodiments, reference signal imperfections are produced by analyzing a reference signal transmitted by an authorized alarm control device. Reference is now made to FIG. 6, showing a flowchart schematically representing an optional flow of operations 600 for producing reference signal imperfections, according to some embodiments of the present invention. In such embodiments, signal processor 101 may receive at 601 via RF transceiver 102 a reference RF signal, encoding a sequence of reference digital bits in an analog refer-

ence carrier signal. Signal processor 101 optionally processes the analog reference carrier signal at 602 to obtain a plurality of reference preamble signal imperfections, and at 603 optionally stores the plurality of reference preamble signal imperfections in non-volatile storage 112. Similarly, to produce a plurality of sync-word signal imperfections, signal processor 101 optionally processes the analog reference carrier signal at 602 to obtain a plurality of sync-word preamble signal imperfections, and at 603 optionally stores the plurality of reference sync-word signal imperfections in non-volatile storage 112.

[0069] Another possible method to detect an intrusion attempt uses unsupported alarm control device instructions. Following is an optional method implemented by the system in some embodiments of the present invention, to detect an intrusion attempt using unsupported alarm control device instructions.

[0070] Reference is now made also to FIGs. 7A and 7B, showing time sequences schematically representing an optional flow of operations for detecting an intrusion attempt using an unsupported instruction, according to some embodiments of the present invention. In such embodiments the alarm control device has a predefined set of supported instructions. An unsupported instruction is an instruction not in the predefined set of supported instructions. When the alarm control device receives a signal from the signal processor instructing an unsupported instruction, the alarm control device optionally transmits to the signal processor an error RF signal message including an indication of the unsupported instruction. This protocol is used in some embodiments to create a deception signal.

[0071] Reference is now made also to FIG. 7A, showing a time sequence schematically representing an optional flow of operations for detecting an intrusion attempt using an unsupported instruction with regard to an authorized alarm control device, according to some embodiments of the present invention. In such embodiments, RF transceiver 702 receives at 710 a first disarm RF signal from an alarm control device 701, and transmits at 711 a deception RF signal comprising an unsupported instruction X selected from a group of predefined instructions known to be unsupported by alarm control device 701. Optionally, unsupported instruction X is selected at random from the group of predefined unsupported instructions. When alarm control device 701 is authorized, the alarm control device optionally transmits at 712 an error RF response comprising the unsupported instruction X received from RF transceiver 702. The RF transceiver optionally sends the error RF response to signal processor 703 at 713. Optionally, signal processor 703 receives the error RF response and extracts at 714 the returned unsupported instruction. At 715 signal processor 703 optionally compares the returned unsupported instruction to the unsupported instruction X. Next, signal processor 703 optionally selects an alarm system operation to output according to the unsupported instruction compliance. When the returned unsupported instruction complies with X, for example is equal to X, at 716 signal processor 703 optionally determines a valid disarm message. Optionally, at 717 signal processor 703 sends alarm control device 701 via RF transceiver 702 a response RF signal comprising a supported instruction selected from the alarm control device's predefined set of supported instructions. Optionally, signal processor 703 instructs disarming the alarm system, for example by instructing an alarm controller.

[0072] A sequence of signals including a disarm message and an RF response signal indicating an erroneous instruction may be recorded and retransmitted by an unauthorized alarm control device. Reference is now made also to FIG. 7B, showing a time sequence schematically representing an optional flow of operations for detecting an intrusion attempt using an unsupported instruction with regard to an unauthorized alarm control device, according to some embodiments of the present invention. In such embodiments, in response to received recorded first disarm RF signal at 710, signal processor 703 transmits at 721 a deception RF signal comprising another unsupported instruction Y selected from a group of predefined instructions known to be unsupported by alarm control device 701. Optionally, unsupported instruction Y is selected at random from the group of predefined unsupported instructions. When alarm control device 701 is unauthorized, the alarm control device optionally transmits at 712 a recorded error RF response comprising the recorded unsupported instruction X. The RF transceiver optionally sends the error RF response to signal processor 703 at 713. Optionally, signal processor 703 receives the error RF response and extracts at 714 the returned unsupported instruction. At 715 signal processor 703 optionally compares the returned unsupported instruction to the unsupported instruction Y. Next, signal processor 703 optionally selects an alarm system operation to output according to the unsupported instruction compliance. When the returned unsupported instruction (X) does not comply with Y, for example is different from Y, at 724 signal processor 703 optionally determines an intrusion attempt. Optionally, the signal processor next notifies a control center. Optionally, the signal processor delivers an electrical current to one or more alarm devices capable of emitting an audio signal or a visual signal.

[0073] Typically, an alarm control device supports only several functions, typically fewer than 100. When the unsupported instruction is represented by a 16-bit digital word and an unsupported instruction transmitted by the transceiver to the alarm control device is selected at random, the probability of selecting the same unsupported instruction recorded is close to 2^16. Comparing a received unsupported instruction indication to a transmitted unsupported instruction indication has a high probability of detecting a recorded error RF signal.

[0074] A possible alarm system comprises at least one radio-frequency (RF) transceiver configured to receive a preamble RF signal from an alarm control device, the preamble RF signal comprising a sequence of preamble

digital bits encoded in an analog preamble carrier signal; and at least one signal processor electrically connected to the at least one RF transceiver, configured to: analyze the preamble RF signal to determine a plurality of preamble signal imperfections of the analog preamble carrier signal, the preamble signal imperfections comprising at least one of a frequency imperfection of a sinus signal, an amplitude imperfection of a sinus signal and a phase imperfection of a sinus signal; compare the plurality of preamble signal imperfections with a plurality of reference preamble signal imperfections to determine a preamble compliance; receive via the at least one RF transceiver a message RF signal from the alarm control device, the message RF signal comprising a sequence of message digital bits encoded in an analog message carrier signal; and perform an alarm system operation according to the preamble compliance.

[0075] Optionally, the at least one signal processor is further configured to determine an intrusion attempt, subject to at least one of the plurality of preamble signal imperfections failing to comply with the plurality of reference preamble signal imperfections.

[0076] Optionally, the at least one signal processor is further configured to determine a valid message subject to the plurality of preamble signal imperfections complying with the plurality of reference preamble signal imperfections; and wherein the alarm system operation comprises processing the message RF signal.

[0077] Optionally, the plurality of reference preamble signal imperfections comprises at least one preamble characteristic selected from the group of: a carrier frequency offset, a phase noise, an in-phase and quadrature imbalance (IQ imbalance), and a signal nonlinearity.

[0078] Optionally, the at least one signal processor is further configured to: receive via the at least one RF transceiver after the preamble signal a synchronization-word (sync-word) RF signal from the alarm control device, the sync-word RF signal comprising a sequence of sync-word digital bits encoded in an analog sync-word carrier signal; analyze the analog sync-word carrier signal to determine a plurality of sync-word signal imperfections of the sync-word signal, the sync-word signal imperfections comprising at least one of a frequency imperfection of a sinus signal, an amplitude imperfection of a sinus signal and a phase imperfection of a sinus signal; compare the plurality of sync-word signal imperfections with a plurality of reference sync-word signal imperfections to determine a sync-word compliance; and perform the alarm system operation according to the preamble compliance and the sync-word compliance.

[0079] Optionally, the at least one signal processor is further configured to determine an intrusion attempt, subject to at least one of the plurality of sync-word signal imperfections failing to comply with the plurality of reference sync-word signal imperfections, or at least one of the plurality of signal imperfections failing to comply with the plurality of reference signal imperfections.

[0080] Optionally, the at least one signal processor is further configured to determine a valid message subject to the plurality of preamble signal imperfections complying with the plurality of reference preamble signal imperfections and the plurality of sync-word signal imperfections complying with the plurality of reference sync-word signal imperfection, and the alarm system operation comprises processing the message RF signal.

[0081] Optionally, the plurality of reference sync-word signal imperfections comprises at least one sync-word characteristic selected from the group of: a carrier frequency offset, a phase noise, an IQ imbalance, and a signal nonlinearity.

[0082] Optionally, the alarm system operation comprises notifying a control center comprising at least one hardware processor upon the attempted intrusion being determined.

[0083] Optionally, the alarm system further comprises a device capable of emitting an audio signal or a visual signal, electrically connected to the at least one signal processor; and the alarm system operation comprises delivering an electrical current to the device upon the attempted intrusion being determined.

[0084] Optionally, the alarm system further comprises a non-volatile digital storage electrically coupled with the at least one signal processor; and the at least one signal processor is further configured to: receiving via the at least one RF transceiver a reference RF signal, encoding a sequence of reference digital bits in an analog reference carrier signal; process the analog reference carrier signal to obtain the plurality of reference preamble signal imperfections; and store the reference preamble signal imperfections in the non-volatile digital storage.

[0085] Optionally, the compare is using a correlator having a sample rate of 16 bits per second.

[0086] A possible method for an alarm system comprises: receiving a preamble RF signal from an alarm control device, the preamble RF signal comprising a sequence of preamble digital bits encoded in an analog preamble carrier signal; analyzing the preamble RF signal to determine a plurality of preamble signal imperfections of the analog preamble carrier signal, the preamble signal imperfections comprising at least one of a frequency imperfection of a sinus signal, an amplitude imperfection of a sinus signal and a phase imperfection of a sinus signal; comparing the plurality of preamble signal imperfections with a plurality of reference preamble signal imperfections to determine a preamble compliance; receiving via the at least one RF transceiver a message RF signal from the alarm control device, the message RF signal comprising a sequence of message digital bits encoded in an analog message carrier signal; and performing an alarm system operation according to the preamble compliance.

[0087] A possible alarm system, comprises at least one radio-frequency (RF) transceiver configured to: receive a first disarm RF signal from an alarm control device; transmit, after receiving the first disarm RF signal, a deception RF signal to the alarm control device, the decep-

tion RF signal comprising an unsupported instruction selected from a group of predefined instructions unsupported by the alarm control device; and receive an error RF response from said alarm control device, the error RF response comprising an indication of a returned unsupported instruction; and at least one signal processor electrically connected to the at least one RF transceiver, configured to: receive the error RF response from the RF transceiver; extract the returned unsupported instruction from the error RF response; compare the returned unsupported instruction to the unsupported instruction to determine a compliance; and output an alarm system operation according to the compliance.

[0088] Optionally, the at least one signal processor is further configured to determine an intrusion attempt, subject to the returned unsupported instruction differing from with the unsupported instruction.

[0089] Optionally, the at least one signal processor is further configured to determine a valid disarm message subject to subject to the returned unsupported instruction being equal to the unsupported instruction; and the alarm system operation comprises at least one of a group of: instructing disarming said alarm system and transmitting via said at least one RF transceiver a response RF signal comprising a supported instruction.

[0090] Optionally, the alarm system operation comprises notifying a control center comprising at least one hardware processor upon the attempted intrusion being detected.

[0091] Optionally, the alarm system further comprises a device capable of emitting an audio signal or a visual signal, electrically connected to the at least one signal processor; and the alarm system operation comprises delivering an electrical current to the device upon the attempted intrusion being detected.

[0092] Optionally, the unsupported instruction is selected at random from the group of predefined instructions; and the unsupported instruction is represented as a 16 bit digital word.

[0093] A possible method for an alarm system comprises: receiving a first disarm RF signal from an alarm control device; transmitting, after receiving the first disarm RF signal, a deception RF signal to the alarm control device, the deception RF signal comprising an unsupported instruction selected from a group of predefined instructions unsupported by the alarm control device; receiving an error RF response from the alarm control device, the error RF response comprising an indication of a returned unsupported instruction; extracting the returned unsupported instruction from the error RF response; comparing the returned unsupported instruction to the unsupported instruction to determine a compliance; and outputting an alarm system operation according to the compliance.

[0094] The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

[0095] It is expected that during the life of a patent maturing from this application many relevant alarm control devices will be developed and the scope of the term "alarm control device" is intended to include all such new technologies a priori.

[0096] As used herein the term "about" refers to $\pm$ 10 %.

[0097] The terms "comprises", "comprising", "includes", "including", "having" and their conjugates mean "including but not limited to". This term encompasses the terms "consisting of" and "consisting essentially of".

[0098] The phrase "consisting essentially of" means that the composition or method may include additional ingredients and/or steps, but only if the additional ingredients and/or steps do not materially alter the basic and novel characteristics of the claimed composition or method.

[0099] As used herein, the singular form "a", "an" and "the" include plural references unless the context clearly dictates otherwise. For example, the term "a compound" or "at least one compound" may include a plurality of compounds, including mixtures thereof.

[0100] The word "exemplary" is used herein to mean "serving as an example, instance or illustration". Any embodiment described as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments and/or to exclude the incorporation of features from other embodiments.

[0101] The word "optionally" is used herein to mean "is provided in some embodiments and not provided in other embodiments". Any particular embodiment of the invention may include a plurality of "optional" features unless such features conflict.

[0102] Throughout this application, various embodiments of this invention may be presented in a range format. It should be understood that the description in range format is merely for convenience and brevity and should not be construed as an inflexible limitation on the scope of the invention. Accordingly, the description of a range should be considered to have specifically disclosed all the possible subranges as well as individual numerical values within that range. For example, description of a range such as from 1 to 6 should be considered to have specifically disclosed subranges such as from 1 to 3, from 1 to 4, from 1 to 5, from 2 to 4, from 2 to 6, from 3 to 6 etc., as well as individual numbers within that range, for example, 1, 2, 3, 4, 5, and 6. This applies regardless of the breadth of the range.

[0103] Whenever a numerical range is indicated herein, it is meant to include any cited numeral (fractional or

integral) within the indicated range. The phrases "ranging/ranges between" a first indicate number and a second indicate number and "ranging/ranges from" a first indicate number "to" a second indicate number are used herein interchangeably and are meant to include the first and second indicated numbers and all the fractional and integral numerals therebetween.

[0104] It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable subcombination or as suitable in any other described embodiment of the invention. Certain features described in the context of various embodiments are not to be considered essential features of those embodiments, unless the embodiment is inoperative without those elements.

[0105] All publications, patents and patent applications mentioned in this specification are herein incorporated in their entirety by reference into the specification, to the same extent as if each individual publication, patent or patent application was specifically and individually indicated to be incorporated herein by reference. In addition, citation or identification of any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention. To the extent that section headings are used, they should not be construed as necessarily limiting.

[0106] It will be understood that the invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

[0107] Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

[0108] Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.

Claims

1. An alarm system (100), comprising:

at least one radio-frequency (RF) transceiver (102) configured to:

receive a first disarm RF signal (201) from an alarm control device (103);
during a predetermined delay time after receiving said first disarm RF signal, transmit at least one deception RF signal (220) during one or more transmission time slots selected from a plurality of consecutive time slots of said predetermined delay time, and determine whether one or more receive RF signals (250) are received during one or more receiving time slots selected from said plurality of consecutive time slots, said one or more receiving time slots interleaved with said one or more transmission time slots; and

at least one signal processor (101), electrically connected to said at least one RF transceiver, configured to:

determine an alarm system operation according to analysis of said one or more receive RF signals.

2. The system (100) of claim 1, wherein said analysis comprises:

matching at least one of said one or more receive RF signals (250) with a predefined deception signal pattern;
producing a true deception detection indication for each one of said one or more receive RF signals matching said predefined deception signal pattern; and
selecting said alarm system operation according to said true deception detection indication.

3. The system (100) of claim 1 or 2, wherein said analysis comprises:

producing a false deception detection indication subject to none of said one or more receive RF signals (250) being received during said one or more receiving time slots or each one of said one or more receive RF signals failing to match said predefined deception signal pattern ; and
selecting said alarm system operation according to said false deception detection indication.

4. The system (100) of any preceding claim, wherein said at least one signal processor (101) is further configured to:

determine said first disarm RF signal (201) is valid, subject to not receiving any of said one or more receive RF signals (250) or producing only false deception detection indication; and
receive a second disarm RF signal (202) from said alarm control device (103) after said predetermined delay time;
wherein, upon receiving said second disarm RF signal, said alarm system operation comprises at least one of: instructing disarming said alarm system, and transmitting an acknowledgement RF signal to said alarm control device via said at least one RF transceiver (102).

5. The system (100) of any preceding claim, wherein said transmission time slots are selected at random by said signal processor (101) upon reception of said first disarm RF signal (201) for transmitting said at least one deception RF signal (220); and
wherein said reception time slots comprise all of said plurality of consecutive time slots different from said transmission time slots.

6. The system (100) of any preceding claim, wherein an amount of said transmission time slots is between 15% and 30% of an amount of said plurality of consecutive time slots.

7. The system (100) of any preceding claim, wherein said predetermined delay time is partitioned into 25 consecutive time slots.

8. The system (100) of any preceding claim" wherein at least one deception RF signal (220) comprises at least one of: an identifier, a time stamp and a random number, for use in identifying an origin of a recorded deception RF signal.

9. The system (100) of claim 8, wherein said identifier consists of 32 binary bits, wherein said time stamp consists of 32 binary bits, and
wherein said random number consists of 8 binary bits.

10. The system (100) of claim 8 or 9, wherein said matching said predefined deception signal pattern comprises detecting in said one received RF signal (250) at least one of: an identifier, a time stamp and a random number.

11. The system (100) of any preceding claim, wherein said at least one deception RF signal (220) is protected by an error detecting code being a 16-bit cyclic redundancy check.

12. The system (100) of any preceding claim, wherein said at least one deception RF signal (220) is encrypted using a method selected from the group of: obfuscation, exclusive-or with a predefined seed word, and exclusive-or with a random seed word.

13. The system (100) of any preceding claim" wherein said analysis further comprises:

detecting a packet number in said first disarm RF signal (201);
comparing a difference between said packet number and a previously stored packet number with a predefined threshold number; and
producing a true deception detection indication when said difference is greater than said predefined threshold number.

14. The system (100) of any preceding claim" wherein said alarm system operation comprises at least one operation selected from the group comprising: notifying a control center (104) operatively connected to said at least one signal processor (101) of an attempted intrusion, subject to producing at least one true deception detection indication and delivering an electrical current to a device (105) capable of emitting an audio signal or a visual signal, electrically connected to said at least one signal processor (101), subject to producing at least one true deception detection indication.

15. A method for an alarm system (100), comprising:

receiving a first disarm RF signal (201) from an alarm control device (103);
during a predetermined delay time after receiving said first disarm RF signal, transmitting at least one deception RF signal (220) during one or more transmission time slots selected from a plurality of consecutive time slots of said predetermined delay time, and determining whether one or more receive RF signals (250) are received during one or more receiving time slots selected from said plurality of consecutive time slots, said one or more receiving time slots interleaved with said one or more transmission time slots; and
determining an alarm system operation according to analysis of said one or more receive RF signals.

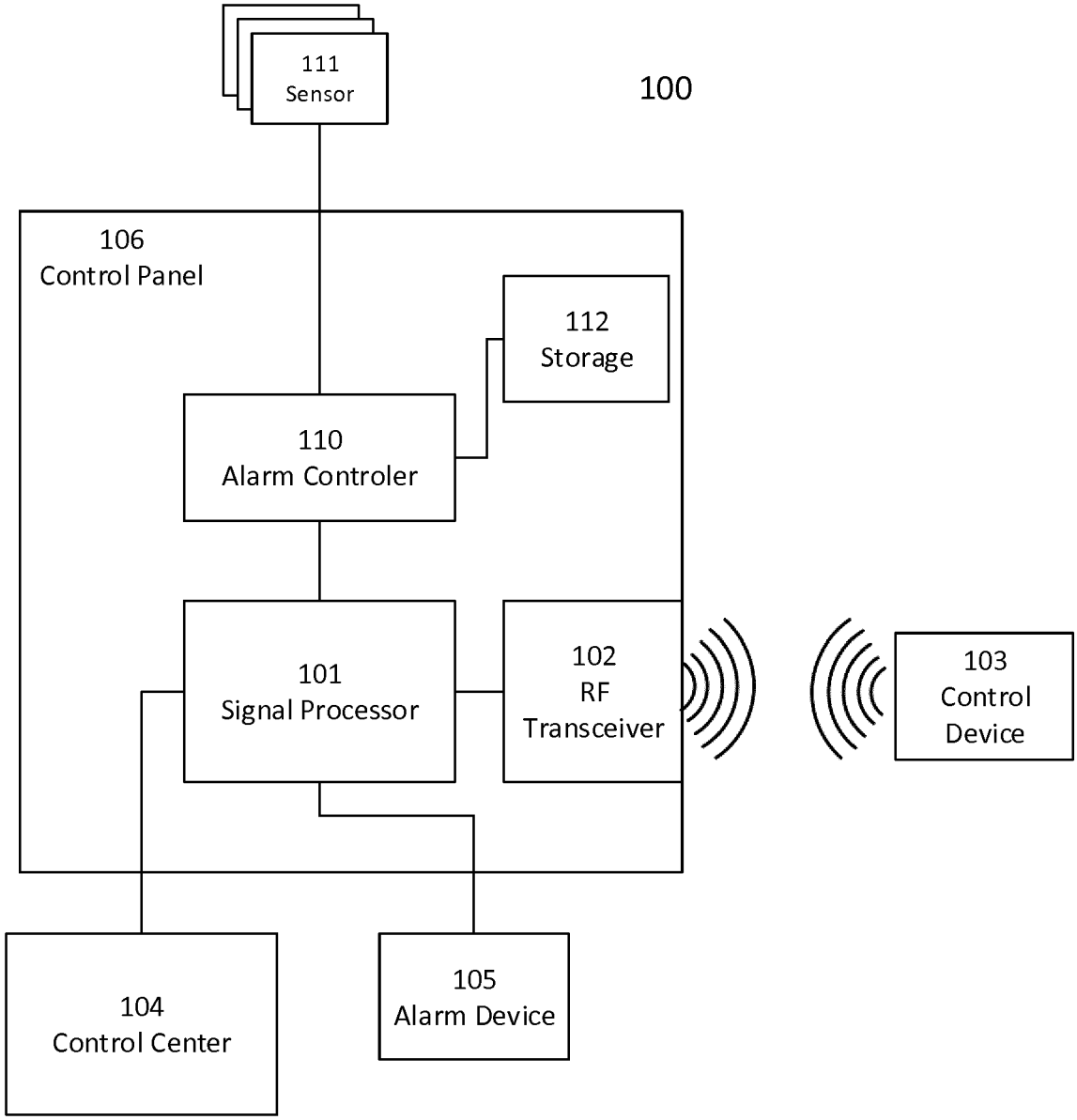

111
Sensor
100
106
Control Panel
112
Storage
110
Alarm Controler
101
Signal Processor
102
RF
Transceiver
103
Control
Device
104
Control Center
105
Alarm Device

FIG. 1

FIG. 2A

FIG. 2B

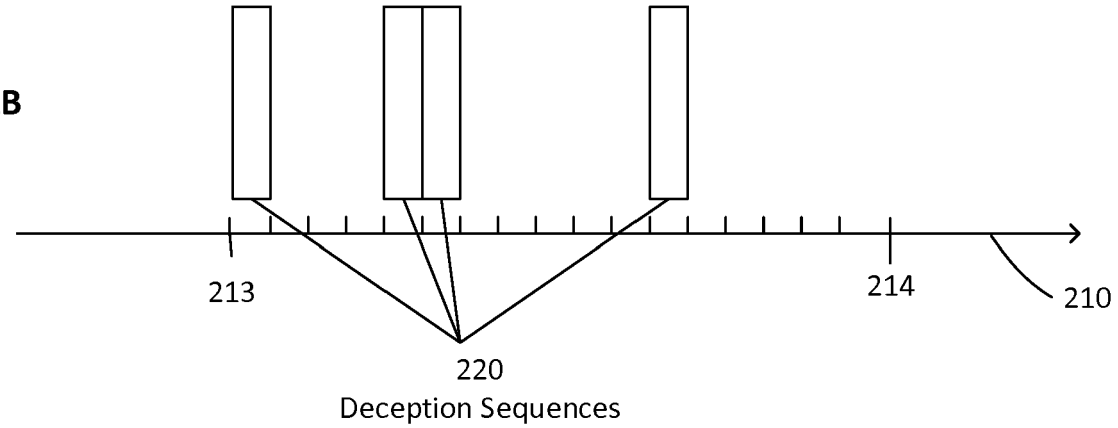
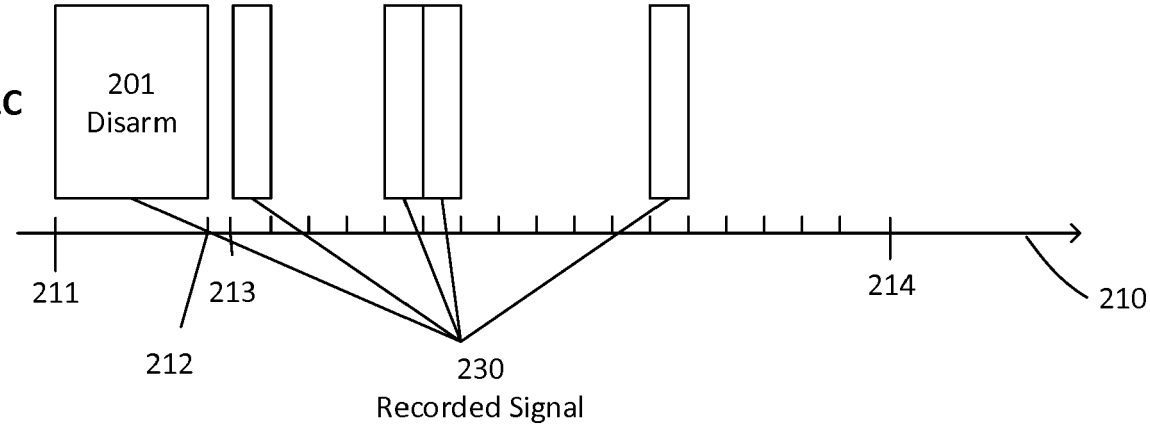


FIG. 2C



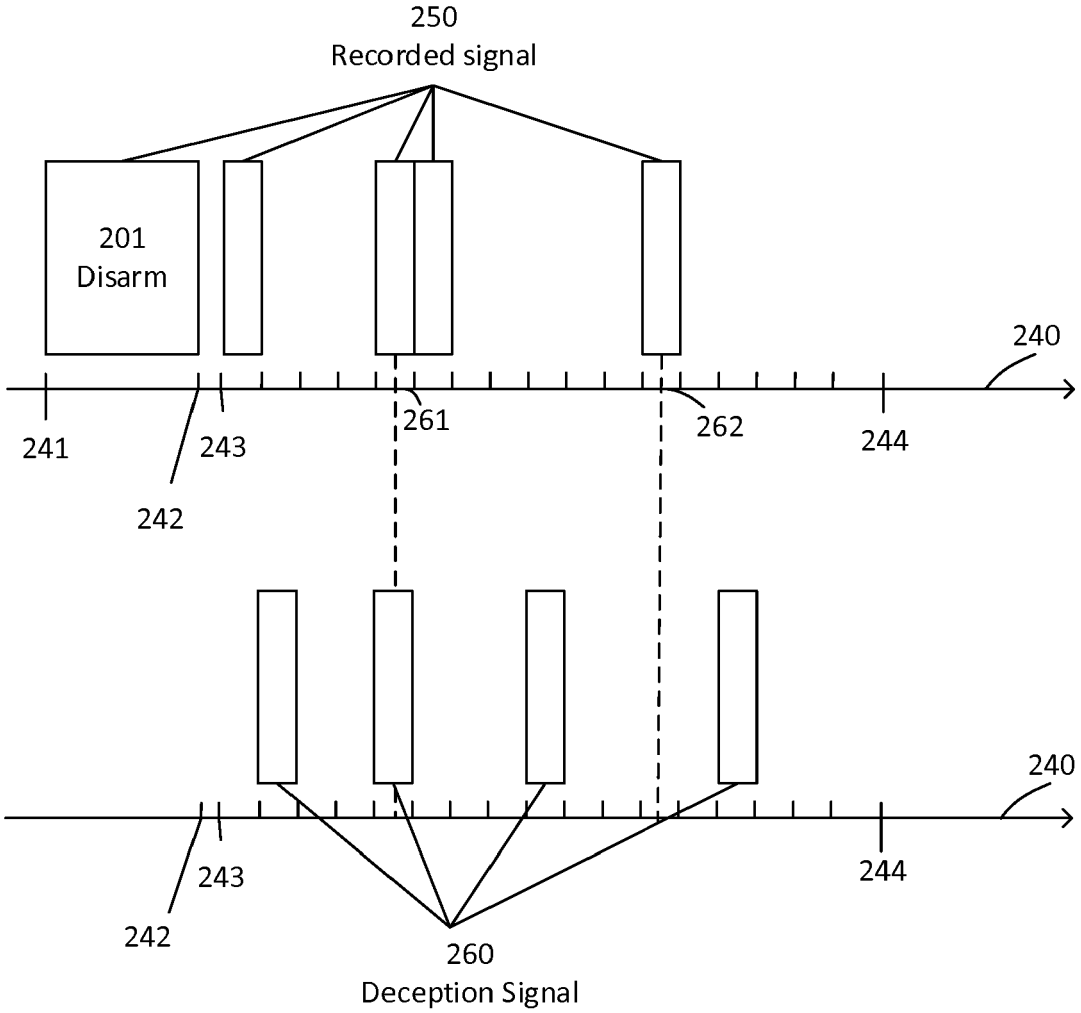

250
Recorded signal
201
Disarm
240
241
242
243
261
262
244
240
242
243
244
260
Deception Signal

FIG. 2D

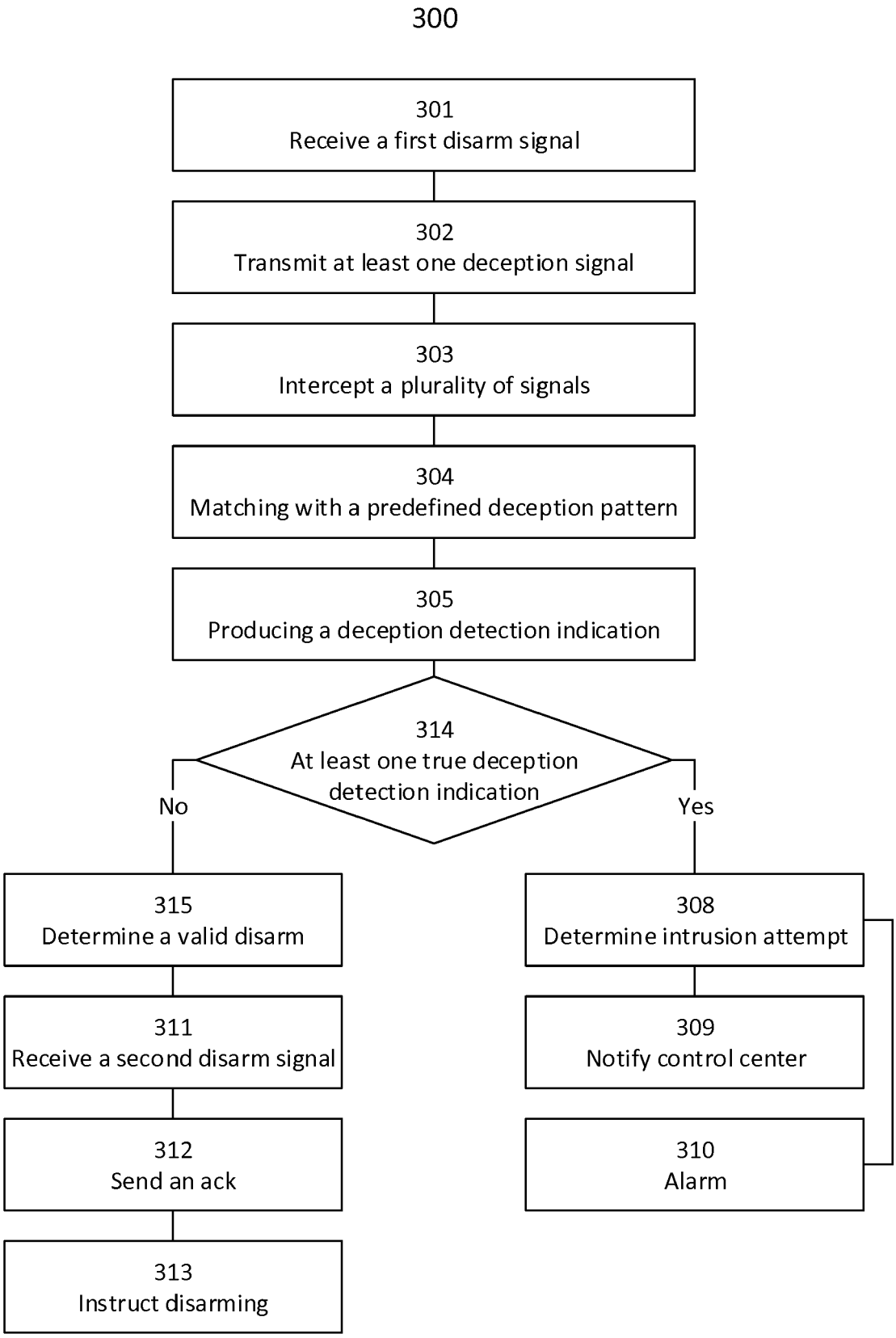

300
301
Receive a first disarm signal
302
Transmit at least one deception signal
303
Intercept a plurality of signals
304
Matching with a predefined deception pattern
305
Producing a deception detection indication
314
At least one true deception detection indication
No
Yes
315
Determine a valid disarm
311
Receive a second disarm signal
312
Send an ack
313
Instruct disarming
308
Determine intrusion attempt
309
Notify control center
310
Alarm

FIG. 3

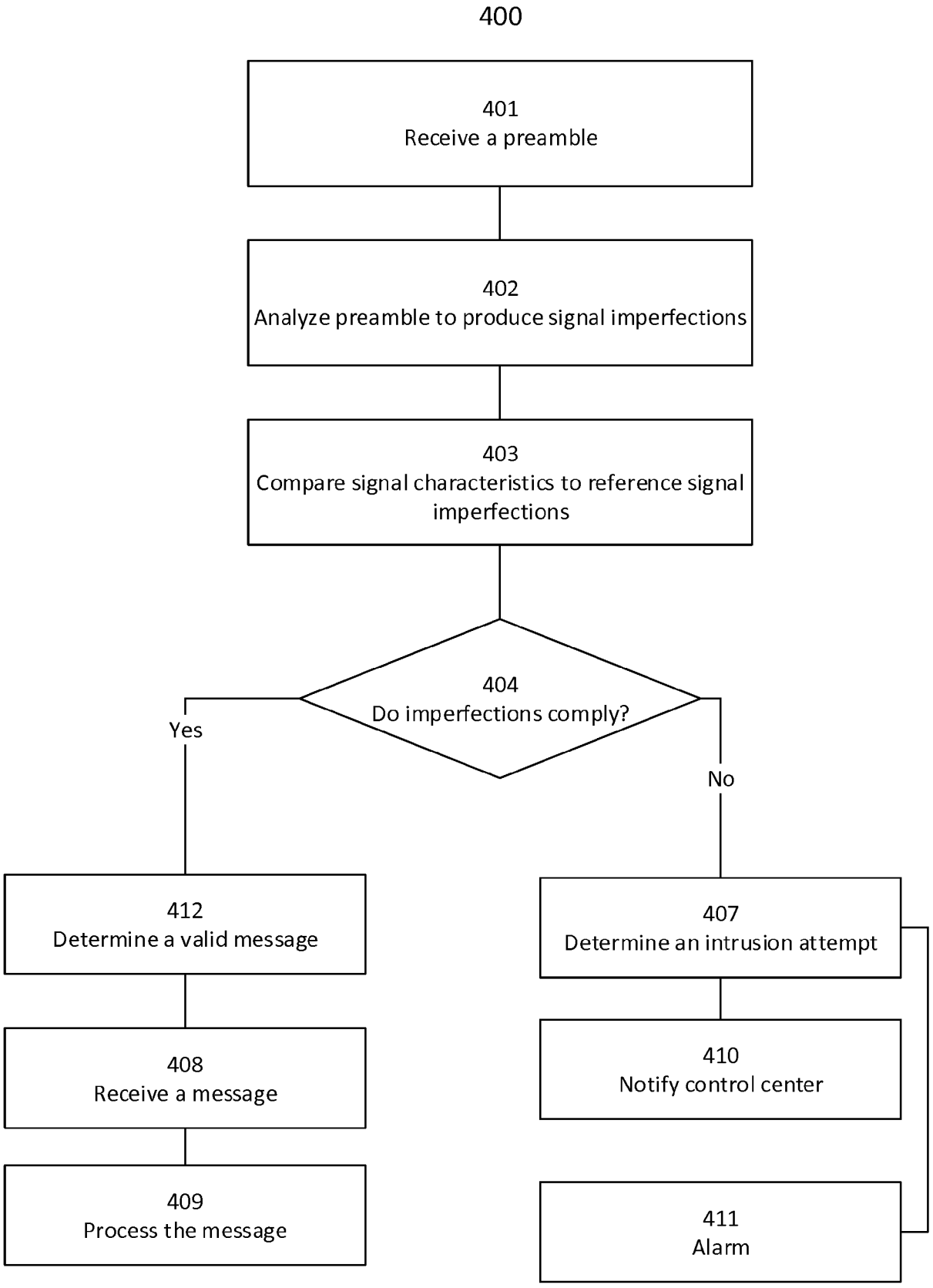

400
401
Receive a preamble
402
Analyze preamble to produce signal imperfections
403
Compare signal characteristics to reference signal imperfections
404
Do imperfections comply?
Yes
No
412
Determine a valid message
408
Receive a message
409
Process the message
407
Determine an intrusion attempt
410
Notify control center
411
Alarm

FIG. 4

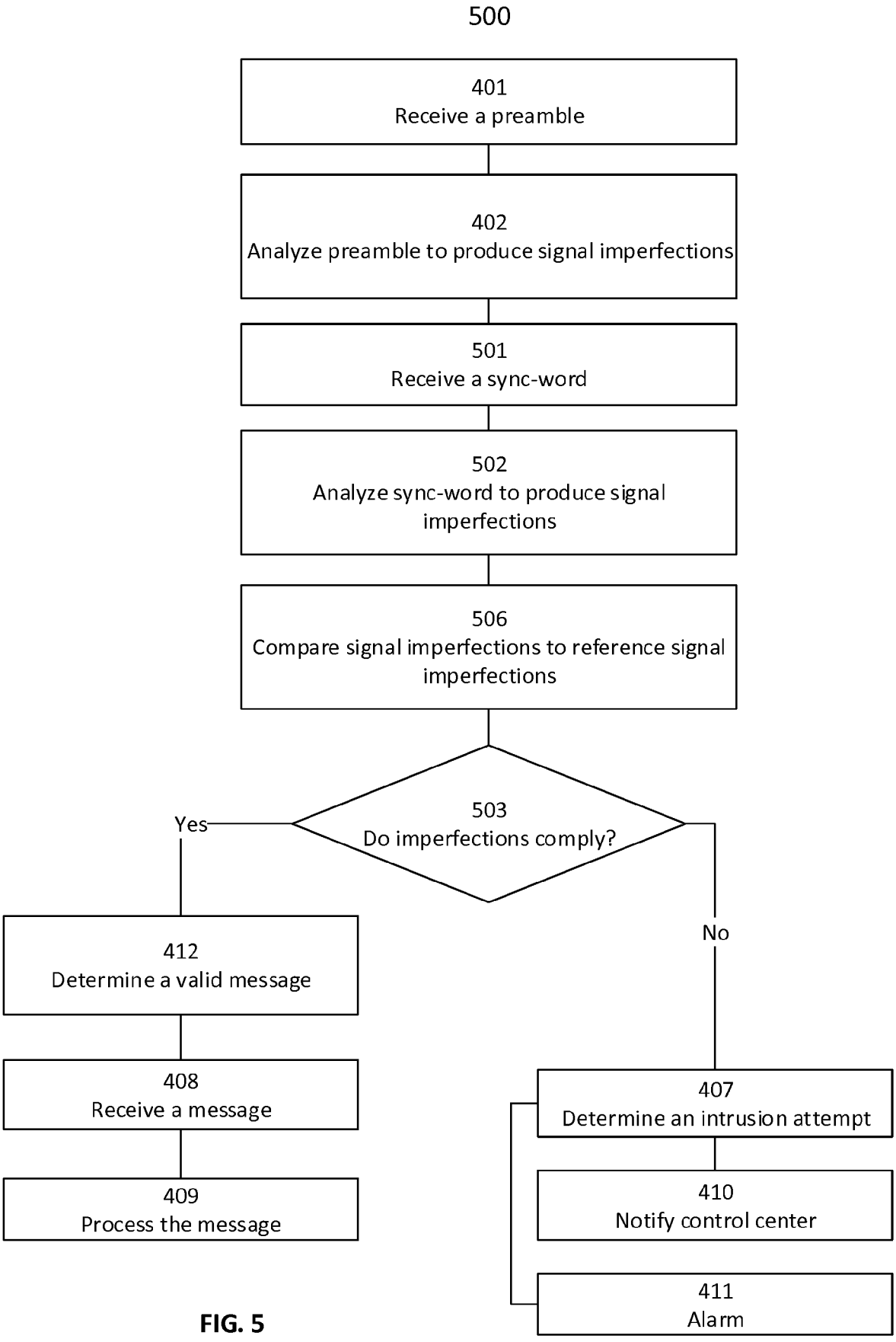

500
401
Receive a preamble
402
Analyze preamble to produce signal imperfections
501
Receive a sync-word
502
Analyze sync-word to produce signal imperfections
506
Compare signal imperfections to reference signal imperfections
503
Do imperfections comply?
Yes
No
412
Determine a valid message
408
Receive a message
409
Process the message
407
Determine an intrusion attempt
410
Notify control center
411
Alarm

FIG. 5

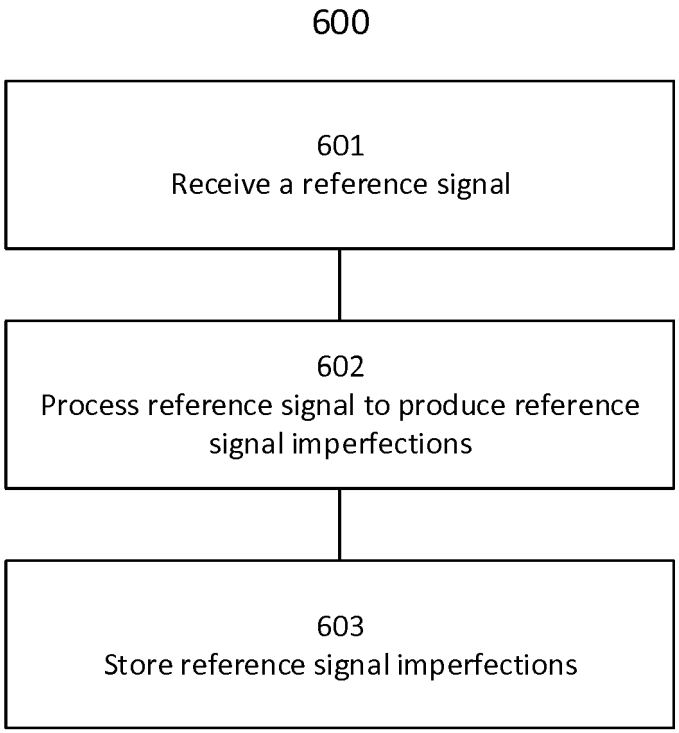

600
601
Receive a reference signal
602
Process reference signal to produce reference signal imperfections
603
Store reference signal imperfections

FIG. 6

FIG. 7A

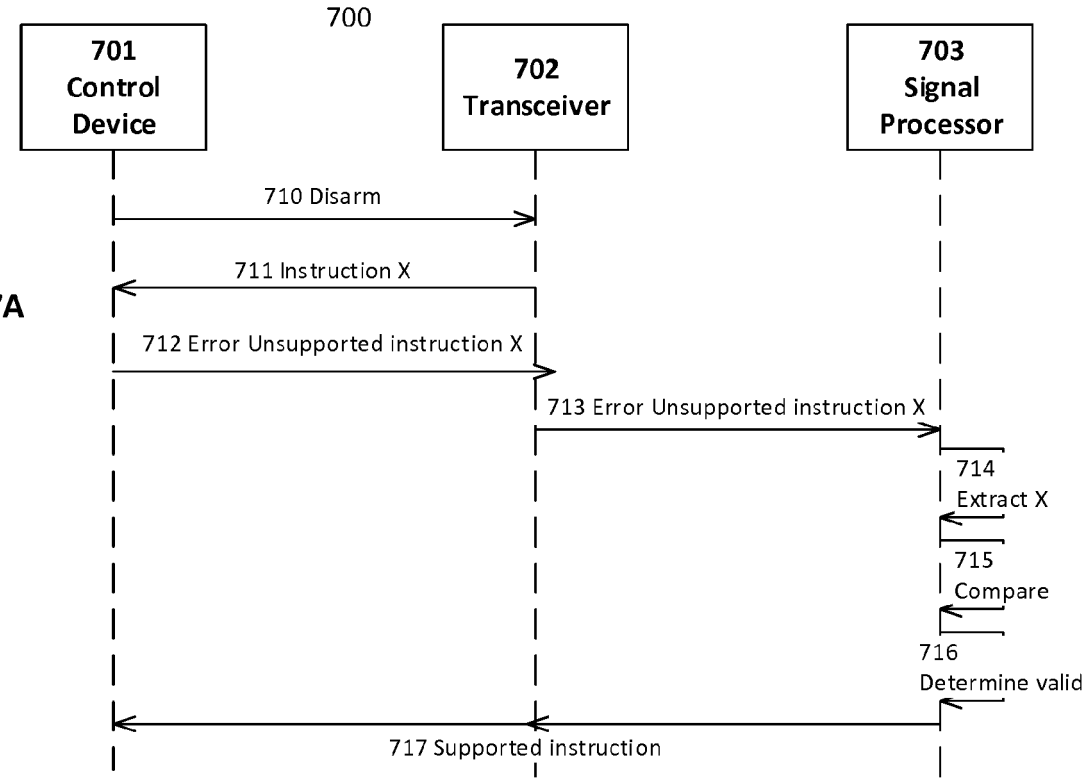
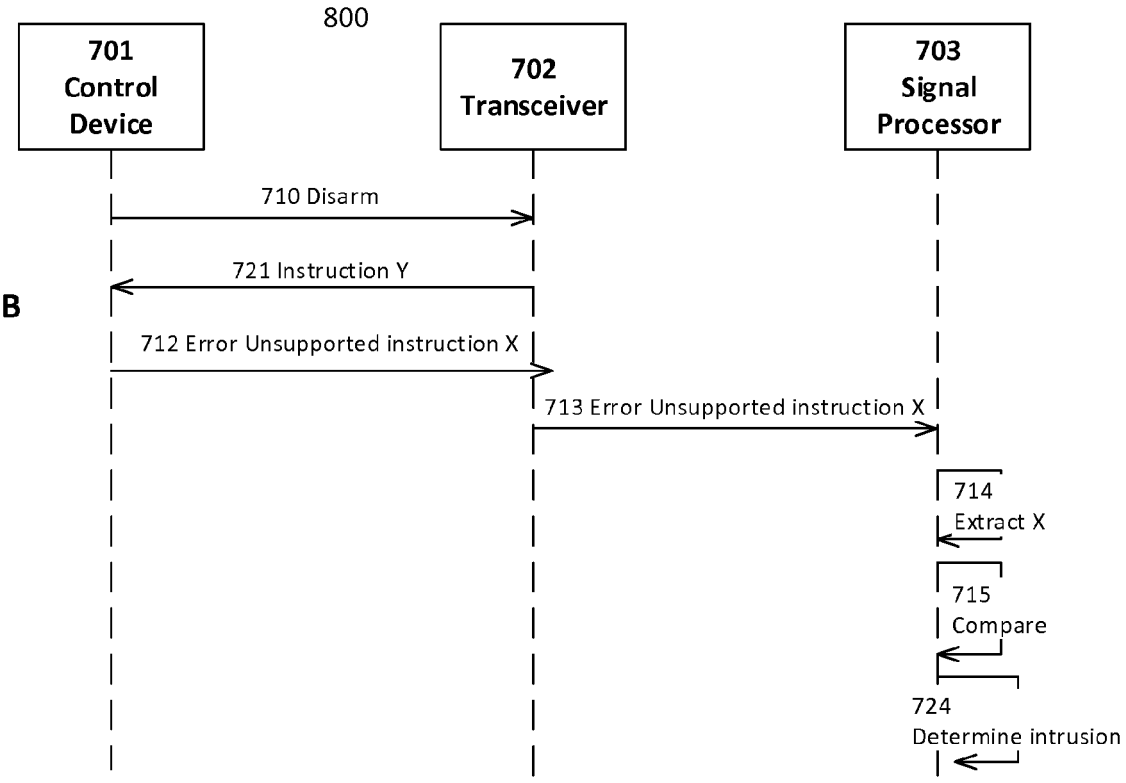

700
701 Control Device
702 Transceiver
703 Signal Processor
710 Disarm
711 Instruction X
712 Error Unsupported instruction X
713 Error Unsupported instruction X
714 Extract X
715 Compare
716 Determine valid
717 Supported instruction

FIG. 7B


800
701 Control Device
702 Transceiver
703 Signal Processor
710 Disarm
721 Instruction Y
712 Error Unsupported instruction X
713 Error Unsupported instruction X
714 Extract X
715 Compare
724 Determine intrusion

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 17 17 2597

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2005/237185 A1 (BROWN MATTHEW [CA] ET AL) 27 October 2005 (2005-10-27) * the whole document *	1-15	INV. G08B25/00
A	EP 2 114 055 A1 (HONEYWELL INT INC [US]) 4 November 2009 (2009-11-04) * the whole document *	1-15	
A	US 2004/160324 A1 (STILP LOUIS A [US]) 19 August 2004 (2004-08-19) * the whole document *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G08B
B60R

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	11 October 2017	Seisdedos, Marta

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 17 17 2597

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-10-2017

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005237185 A1	27-10-2005	NONE	
EP 2114055 A1	04-11-2009	CA 2654657 A1	11-09-2009
		CN 101534503 A	16-09-2009
		EP 2114055 A1	04-11-2009
		US 2009232307 A1	17-09-2009
US 2004160324 A1	19-08-2004	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82