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

(11) **EP 3 923 257 A1**

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.12.2021 Bulletin 2021/50

(51) Int Cl.:
G08B 13/08 *(2006.01)* ***G08B 29/18*** *(2006.01)*

(21) Application number: **21178718.9**

(22) Date of filing: **10.06.2021**

(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:
KH MA MD TN

(30) Priority: **10.06.2020 GB 202008824**

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

(72) Inventors:
- **MENIS, Boaz**
  Herzliya Pituach 4672530 (IL)
- **TUGENDHAFT, Nissim**
  Herzliya Pituach 4672530 (IL)

(74) Representative: **Adamson, Katherine Louise**
Marks & Clerk LLP
40 Torphichen Street
Edinburgh EH3 8JB (GB)

(54) SECURITY DEVICE, SYSTEM AND METHOD

(57) A security device (102) is use at an access point of a premises. The security device comprises a sensor (212) configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration. The security device further comprises a processor (204) configured to operate in a tamper detection mode. The operating in the tamper detection mode comprises processing the sensor output to detect at least one tamper event. The processor (204) is configured to disable the tamper detection mode in response to a determination that the access point is in a closed state.

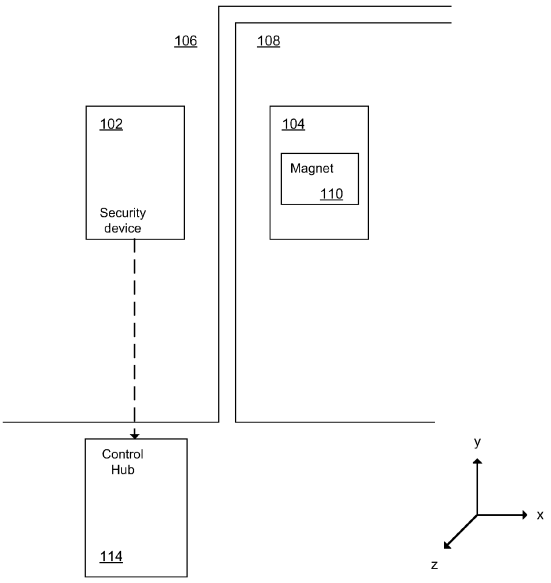

FIG. 1

EP 3 923 257 A1

Description

Technical Field

[0001] The present invention relates to a device, system and method for premises security, for example a security device having inbuilt tamper detection.

Background

[0002] A premises may have multiple openable and/or closable access points, for example doors and/or windows. An access point may comprise any point in the premises that may be used to access the premises, whether or not it is intended as a point of entry. For example, an openable window may not be intended to be used to enter to the premises, but may provide a potential access point to an intruder trying to enter the premises, or at least to a body part, e.g. an arm, of the intruder.

[0003] Typically, an access point comprises at least two components, wherein at least one of the components is moveable so that there is a relative movement of one of the components with respect to the other. Relative movement of the components results in the opening and closing of the access point.

[0004] In many cases, a first component of the access point is a moveable barrier, for example a door, gate or window. A second component of the access point is a fixed component, for example a door frame, gate frame or window frame. The moveable barrier is moveable between open and closed states for respectively entering or blocking entry to the space.

[0005] A security device may be used to detect a change of state of the access point. The security device may be mounted on the access point. The security device may be battery operated. The security device may transmit a wireless signal to another device, for example to a control hub of a security system, when a change of state of the access point is detected. In some circumstances, a wireless signal may be transmitted only when the change of state is relevant to security, for example, when the change of state is an unauthorised opening of the access point.

[0006] The security device may be mounted on the access point. The security device may be mounted to a frame of the access point, for example a door or window frame. Alternatively, the security device may be mounted on the moveable barrier. In some circumstances, the security device is mounted on one moveable barrier, and the access point comprises a further moveable barrier, for example in the case of two sliding doors.

[0007] The security device may be part of a system that also comprises a second device. The security device may be mounted to a first component of the access point and the second device may be mounted to a second, different component of the access point. Separation of the security device from the second device may be detected to detect an open or closed state of the access point. For example, the security device may comprise a magnetic sensor and the second device may comprise a magnet, or vice versa.

[0008] Alternatively, the security device may be configured to detect a change of the state of the access point without use of any such second device. For example, the change of state may be identified based on sensed kinematics and/or orientation of a moveable barrier of the access point, for example using a multi-axis accelerometer.

[0009] There is a known risk that a security device may be tampered with to prevent detection of the change of state. For example, the tampering may be by physically removing the security device from its installed position. In some circumstances, the security device may be adhesively mounted. The tampering may involve ripping the device from the access point. Such a tampering may be referred to as a physical tamper.

[0010] The devices and methods described in the present application may solve one or more of the above problems and/or provide useful market alterative(s).

[0011] Reference to any prior art in this specification is not an acknowledgement or suggestion that this prior art forms part of the common general knowledge in any jurisdiction, or globally, or that this prior art could reasonably be expected to be understood, regarded as relevant/or combined with other pieces of prior art by a person skilled in the art.

Summary

[0012] In a first aspect, there is provided a security device for use at an access point of a premises. The security device comprises a sensor configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration. The security device further comprises a processor configured to identify a potential tamper event; process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and designate the potential tamper event as a tamper event if the values meet the detection condition over the sustained period of time.

[0013] Determining whether the sensor output meets the detection condition over the sustained period of time may allow tamper events to be distinguished from other types of events, for example normal door opening or door closing events. In some circumstances, tamper events may be distinguished from shock events, for example a shock event caused by someone banging on a door. Accuracy of tamper detection may be improved. A number of false tamper detections may be reduced.

[0014] The detection condition may be representative of a characteristic acceleration that is distinguishable from at least one of a typical acceleration caused upon a moving part of the access point when opening, or a typical acceleration caused by a shock event.

[0015] Determining whether values for the parameters of the sensor output meet the detection condition may comprise comparing the values for the parameter of the sensor output to a threshold value. Determining whether values for the parameter of the sensor output meet the detection condition over the sustained period of time may comprise determining whether values for the parameter of the sensor output meet the detection condition for a predetermined number of sample points. Determining whether values for the parameter of the sensor output meet the detection condition may comprise determining whether values for the parameter of the sensor output meet the detection condition for a predetermined proportion of sample points within the sustained period of time.

[0016] The identifying of the potential tamper event may comprise processing the sensor output to determine that a value for a further parameter of the sensor output meets a predefined condition. The determining that the value for the further parameter of the sensor output meets the predefined condition may comprise comparing the value for the further parameter to a further threshold. The identifying of the potential tamper event may comprise determining, by the processor, that a change of state of the access point has occurred.

[0017] The device may further comprise a magnetic sensor for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field. The processor may be configured to process the magnetic sensor output to perform the determining that the change of state of the access point has occurred.

[0018] The security device may be for use at an access point of a premises. The access point may comprise at least a first component and a second component. At least one of the first component and second component may be moveable to move relative to the other of the first component and second component (108), to open and close the access point. At least one of the first and second component may be rotatable around a hinge. The first component and/or the second component may comprise a door. The first component and/or the second component may comprise a window. The first component and/or the second component may comprise a gate. The first component and/or the second component may comprise a door frame, window frame or gate frame.

[0019] The sustained period of time may be longer than a typical time for which values of the parameter meet the predefined condition when a normal opening or closing action of the first and/or second component of the access point is performed. The sustained period of time may be longer than a typical time for which values of the parameter meet the detection condition when a shock event occurs.

[0020] The sustained period of time may be between 50 ms and 500 ms, optionally between 50 ms and 250 ms, further optionally between 75 ms and 125 ms. For example, the sustained period of time may be 100 ms. The sustained period of time may be greater than 20 ms, optionally greater than 30 ms, further optionally greater than 40 ms, further optionally greater than 50 ms, further optionally greater than 75 ms, further optionally greater than 100 ms. The sustained period of time may be less than 500 ms, optionally less than 400 ms, further optionally less than 300 ms, further optionally less than 200 ms, further optionally less than 150 ms, further optionally less than 125 ms, further optionally less than 100 ms.

[0021] Meeting the detection condition may comprise exceeding a threshold value for 10 consecutive sample points. Meeting the detection condition may comprise exceeding a threshold value for at least 5 consecutive sample points, optionally at least 10 sample points, further optionally at least 15 sample points. The sample points may be spread, e.g. evenly spaced, over any of the above sustained periods of time, but in some embodiments, more particularly, a 100 ms period.

[0022] The processor may be further configured to initiate a detection window in response to identifying the potential tamper event. The processor may be further configured to determine that the tamper event has occurred only if the sustained period of time occurs within the detection window.

[0023] The detection window may be at least 200 ms, optionally at least 500 ms, optionally at least 750 ms. Additionally or alternatively, the detection window may be less than 5 s, optionally less than 2 s, further optionally less than 1.5 s. For example, the detection window may be between 0.5 seconds and 1.5 seconds, or more specifically 1 second, in some embodiments.

[0024] The sensor may be configured to switch from a first mode to a second mode in response to the identifying of the potential tamper event. The first mode may be higher power than the second mode. For example, in some embodiments, the first and second modes may operate at different sampling rates, or in other embodiments, the second mode may be a waking mode and the first mode may be a sleep mode in some embodiments or even an off mode in some embodiments.

[0025] The sensor and/or processor may be configured to switch from the first mode to the second mode in response to a determination of an opening of the access point. The sensor and/or processor may be configured to switch from the first mode to the second mode in response to a determination of a non-closed state. The determined non-closed state is a determined open state in some embodiments.

[0026] The sensor and/or processor may be configured to switch from the second mode to the first mode after expiration of the detection window. The sensor and/or processor may be configured to switch from the second mode to the first mode in response to a determination that a non-closed state has ceased. The determined non-closed state is a determined open state in some embodiments.

[0027] The sensor and/or processor may be configured to switch from the second mode to a third, different mode after expiration of the detection window. For example, the second mode and third mode may operate at

different sampling rates. The first mode and third mode may operate at different sampling rates. In the third mode, the accelerometer may be turned off or in a sleep mode. The accelerometer may not sample when in the third mode.

[0028] The processor may be further configured to trigger an alarm in response to determining that a tamper event has occurred. The processor may be further configured to trigger an alarm in response to values for the parameter of the sensor output meeting the detection condition over the sustained period of time. The processor may be further configured to instruct a transmitter to send a message to a further device in response to determining that a tamper event has occurred. The processor may be further configured to instruct a transmitter to send a message to a further device in response to values for the parameter of the sensor output meeting the detection condition over the sustained period of time. The further device may comprise or form part of a control hub. The further device may comprise or form part of a monitoring system. The further device may comprise a remote server.

[0029] The sensor may comprise or form part of an accelerometer. The sensor may be configured to measure acceleration on each of three axes. The axes may be orthogonal.

[0030] The parameter may comprise or be representative of acceleration on a single axis. The further parameter may comprise or be representative of acceleration on a single axis. The single axis may be a preselected one of the three axes. The single axis may be any one of the three axes.

[0031] The parameter may comprise or be representative of acceleration on two axes. The further parameter may comprise or be representative of acceleration on two axes. The two axes may be preselected from the three axes. The two axes may be any two of the three axes.

[0032] The further parameter may be the same as the parameter. The further threshold value may be the same as the threshold value. The threshold value may be lower than the further threshold value.

[0033] The threshold value may be 350 milli-g. The threshold value may be greater than 100 milli-g, optionally greater than 200 milli-g, further optionally greater than 300 milli-g, further optionally greater than 350 milli-g, further optionally greater than 400 milli-g, further optionally greater than 500 milli-g. The threshold value may be less than 1000 milli-g, optionally less than 750 milli-g, further optionally less than 500 milli-g, further optionally less than 500 milli-g, further optionally less than 400 milli-g, further optionally less than 350 milli-g.

[0034] The further threshold value may be 350 milli-g. The further threshold value may be greater than 100 milli-g, optionally greater than 200 milli-g, further optionally greater than 300 milli-g, further optionally greater than 350 milli-g, further optionally greater than 400 milli-g, further optionally greater than 500 milli-g. The further threshold value may be less than 1000 milli-g, optionally less than 750 milli-g, further optionally less than 500 milli-g, further optionally less than 500 milli-g, further optionally less than 400 milli-g, further optionally less than 350 milli-g.

[0035] The processor may be configured to set the threshold value in dependence on a material and/or size and/or construction of the first component of the access point. The processor may be configured to set the threshold value in dependence on a material and/or size and/or construction of the second component of the access point. The processor may be configured to set the further threshold value in dependence on a material and/or size and/or construction of the first component of the access point. The processor may be configured to set the further threshold value in dependence on a material and/or size and/or construction of the second component of the access point.

[0036] The processor may be configured to set the threshold value using an installation vector determined by a calibration process. The processor may be configured to set the further threshold value using an installation vector determined by a calibration process. The installation vector may comprise or represent a respective value of acceleration for each of a plurality of axes of the security device when the security device is not in motion.

[0037] The sensor and the processor may be housed within a common housing of the security device. The security device may further comprise a battery configured to power the sensor and the processor. The battery may be housed within the common housing.

[0038] The security device may further comprise a transmitter configured to send data to a or the further device. The transmitter may be housed within the common housing. The security device may further comprise a receiver configured to receive data from the further device. The receiver may be housed within the common housing.

[0039] In a second aspect, which may be provided independently, there is provided a security method comprising sensing, by a sensor of a security device for a premises, acceleration of the security device; providing, by the sensor, a sensor output in response to the sensing of the acceleration; identifying, by the processor, a potential tamper event; processing, by the processor, the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and designating, by the processor, the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0040] In a third aspect, which may be provided independently, there is provided a computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of: receiving a sensor output of a sensor of a security device for a premises; identifying a potential tamper event;

processing the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and designating the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0041] In a fourth aspect, which may be provided independently, there is provided a method comprising: mounting a security device to a mounting surface at an access point of a premises, the security device comprising a sensor configured to sense acceleration of the security device and produce a sensor output in response to the sensing of the acceleration; processing, by a processor, the sensor output to determine an installation vector for the security device; and storing, by the processor, the determined installation vector. The installation vector may comprise or represent a respective value of acceleration for each of a plurality of axes of the security device when the security device is not in motion.

[0042] The method may further comprise processing, by the processor, the sensor output to: identify a potential tamper event; process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event, wherein the processing of the sensor output is dependent on the installation vector, and designate the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0043] In a fifth aspect, there is provided a security device for use at an access point of a premises, comprising: a sensor configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration; and a processor configured to operate in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; wherein the processor is configured to disable the tamper detection mode in response to a determination that the access point is in a closed state.

[0044] The processor may be further configured to provide the determination that the access point is in the closed state. The providing of the determination that the access point is in the closed state may comprise processing output of a further sensor to obtain values for a separation parameter that is representative of a separation between the security device and a further device. Additionally, or alternatively, the determination that the access point is in the closed state may be based on the sensor output.

[0045] The processor may be further configured to enable the tamper detection mode in response to a determination that the access point is not in the closed state. The determination that the access point is not in the closed state may comprise a determination that the access point is in an open state. The determination that the access point is not in the closed state may comprise a determination that the access point is in a magnetic tamper state. The processor may be further configured to provide the determination that the access point is not in the closed state. The providing of the determination that the access point is not in the closed state may comprise processing output of a or the further sensor to obtain values for a or the separation parameter that is representative of a separation between the security device and a or the further device. Additionally, or alternatively, the determination that the access point is not in the closed state may be based on the sensor output.

[0046] The processor may be configured to disable the tamper detection mode in response to a determination that a change of state of the access point from the open state to the closed state has occurred. The processor may be configured to enable the tamper detection mode in response to a determination that a change of state of the access point from the closed state to the open state has occurred.

[0047] The processor may be further configured to trigger an alarm in response to the detecting of the tamper event. The processor may be further configured to trigger an alarm in response to determining that the at least one tamper event has occurred. The processor may be further configured to instruct a transmitter to send a message to a further device in response to determining that the at least one tamper event has occurred. The processor may be further configured to instruct a transmitter to send a message to a further device in response to the detecting of the tamper event. The further device may comprise or form part of a control hub. The further device may comprise or form part of a monitoring system.

[0048] The processor may be further configured to operate in a shock detection mode. The operating in the shock detection mode may comprise processing the sensor output to detect at least one shock event.

[0049] The processor may be further configured to switch from the tamper detection mode to the shock detection mode in response to a determination that a state of the access point has changed from a non-closed state to a closed state. The processor may be further configured to switch from the shock detection mode to the tamper detection mode in response to a determination that a state of the access point has changed from a closed state to a non-closed state.

[0050] The sensor may comprise or form part of an accelerometer. The sensor may be configured to measure acceleration on each of three axes. The axes may be orthogonal.

[0051] The device may further comprise a magnetic sensor for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field. The processor may be configured to process the magnetic sensor output to provide the determination that the access point is in the closed state. The processor may be configured to process the magnetic sensor output to provide the determination that the access point is in a

non-closed state. The non-closed state may comprise an open state. The non-closed state may comprise a magnetic tamper state.

[0052] The processor may be configured to process the magnetic output to provide a determination that a state of the access point has changed from a closed state to a non-closed state. The processor may be configured to process the magnetic output to provide a determination that a state of the access point has changed from a non-closed state to a closed state.

[0053] The access point may comprise at least a first component and a second component. At least one of the first component and second component may be moveable to move relative to the other of the first component and second component to open and close the access point. At least one of the first and second component may be rotatable around a hinge. The first component and/or the second component may comprise a door. The first component and/or the second component may comprise a window. The first component and/or the second component may comprise a gate. The first component and/or the second component may comprise a door frame, window frame or gate frame.

[0054] The magnetic sensor may be mounted on one of the first and second components. The magnetic sensor may be configured to sense a magnetic field of a magnet mounted on the other of the first and second components.

[0055] The detecting of the at least one tamper event may comprise: identifying a potential tamper event; processing the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and designating the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0056] Determining whether the values for the parameter meet the detection condition may comprise comparing the values to a threshold value. The sensor may be configured to switch from a first mode to a second mode in response to the determining of the potential tamper event.

[0057] In a sixth aspect, which may be provided independently, there is provided a security method comprising: sensing, by a sensor of a security device for use at an access point of a premises, an acceleration of the security device; providing, by the sensor, a sensor output in response to sensing the acceleration; operating a processor of the security device in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and disabling, by the processor, the tamper detection mode in response to a determination that the access point is in a closed state.

[0058] In a seventh aspect, which may be provided independently, there is provided a computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of: receiving a sensor output from a sensor of a security device for use at an access point of a premises; operating in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and disabling the tamper detection mode in response to a determination that the access point is in a closed state.

[0059] In an eighth aspect, which may be provided independently, there is provided a security device for use at an access point of a premises, comprising: a sensor configured to sense acceleration of the security device and produce a sensor output in response to sensing the acceleration; and a processor configured to operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event; wherein the processor is further configured to disable the shock detection mode in response to a determination that the access point is not in a closed state.

[0060] The processor may be further configured to provide the determination that the access point is not in the closed state. The providing of the determination that the access point is not in the closed state may comprise processing output of a further sensor to obtain values for a separation parameter that is representative of a separation between the security device and a further device. Additionally, or alternatively, the determination that the access point is not in the closed state may be based on the sensor output.

[0061] The processor may be further configured to enable the shock detection mode in response to a determination that the access point is in the closed state. The processor may be further configured to provide the determination that the access point is in the closed state. The providing of the determination that the access point is in the closed state may comprise processing output of a or the further sensor to obtain values for a or the separation parameter that is representative of a separation between the security device and a or the further device. Additionally, or alternatively, the determination that the access point is in the closed state may be based on the sensor output.

[0062] The processor may be configured to disable the shock detection mode in response to a determination of a change of state of the access point from the closed state to the open state. The processor may be configured to enable the shock detection mode in response to a determination of a change of state of the access point from the open state to the closed state.

[0063] The processor may be configured such that the detecting of the at least one shock event disregards features of the sensor output occurring within a delay period after a determination that the access point has ceased to be in the closed state. The delay period may be at least 50 ms, optionally at least 100 ms, further optionally at least 200 ms.

[0064] The processor may initiate the delay period in response to the determination that the access point has

ceased to be in the closed state. The processor may initiate the delay period in response to a determination that a state of the access point has changed from a closed state to a non-closed state. The non-closed state may comprise an open state. The non-closed state may comprise a magnetic tamper state.

[0065] The processor may be further configured to trigger an alarm in response to the detecting of the at least one shock event. The processor may be further configured to trigger an alarm in response to determining that the at least one shock event has occurred. The processor may additionally or alternatively be configured to instruct a transmitter to send a message to a further device in response to the detecting of the at least one shock event. The processor may be further configured to instruct a transmitter to send a message to a further device in response to determining that the at least one shock event has occurred.

[0066] The sensor may comprise or form part of an accelerometer. The sensor may be configured to measure acceleration on each of three axes. The axes may be orthogonal.

[0067] The detecting of the at least one shock event may comprise determining that a value for a third parameter of the sensor output exceeds at least one shock threshold value.

[0068] The third parameter of the sensor output may be representative of an energy of motion of the security device. The third parameter of the sensor output may be integrated over a predetermined integration time.

[0069] The at least one shock threshold value may comprise a first shock threshold representative of gross shock. The first shock threshold may correspond to a first integration time. The at least one shock threshold value may comprise a second shock threshold representative of repetitive shock. The second shock threshold may correspond to a second, different integration time.

[0070] The device may further comprising a magnetic sensor for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field. The processor may be configured to process the magnetic sensor output to provide the determination that the access point is not in the closed state. The processor may be configured to process the magnetic sensor output to provide the determination that the access point is in a non-closed state. The non-closed state may comprise an open state. The non-closed state may comprise a magnetic tamper state.

[0071] The access point may comprise at least a first component and a second component. At least one of the first component and the second component may be moveable to move relative to the other of the first component and the second component to open and close the access point. At least one of the first and second component may be rotatable around a hinge. The first component and/or the second component may comprise a door. The first component and/or the second component may comprise a window. The first component and/or the second component may comprise a gate. The first component and/or the second component may comprise a door frame, window frame or gate frame.

[0072] The magnetic sensor may be mounted on one of the first and second components. The magnetic sensor may be configured to sense a magnetic field of a magnet mounted on the other of the first and second components.

[0073] The processor may be further configured to operate in a tamper detection mode. The operating in the tamper detection mode may comprise processing the sensor output to detect at least one tamper event.

[0074] The processor may be further configured to switch from the tamper detection mode to the shock detection mode in response to a determination that a state of the access point has changed from a non-closed state to a closed state. The processor may be further configured to switch from the shock detection mode to the tamper detection mode in response to a determination that a state of the access point has changed from a closed state to a non-closed state. The non-closed state may comprise an open state. The non-closed state may comprise a magnetic tamper state.

[0075] In a ninth aspect, which may be provided independently, there is provided a security method comprising sensing, by a sensor of a security device for use at an access point of a premises, acceleration of the security device; producing, by the sensor, a sensor output in response to the sensing of the acceleration; operating a processor of the security device in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event; and disabling, by the processor, the shock detection mode in response to a determination that the access point is not in a closed state.

[0076] In a tenth aspect, which may be provided independently, there is provided a computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of: receiving a sensor output from a sensor of a security device for use at an access point of a premises; operating in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event; and disabling the shock detection mode in response to a determination that the access point is not in a closed state.

[0077] Features in one aspect may be applied as features in any other aspect, in any appropriate combination. For example, method features may be provided as device features or vice versa. Features of an apparatus of one aspect may be provided as features of an apparatus of another aspect. Features of a method of one aspect may be provided as features of a method of another aspect.

Brief description of the drawings

[0078] Embodiments will now be described by way of example only, and with reference to the accompanying drawings, of which:

Figure 1 is a schematic illustration of a security device mounted at an access point of a premises in accordance with an embodiment;

Figure 2 is a schematic illustration of a security device in accordance with an embodiment;

Figure 3 is a flow chart illustrating in overview a method of determining occurrence of a tamper event in accordance with an embodiment;

Figure 4 is a flow chart illustrating in overview a tamper detection method in accordance with an embodiment;

Figure 5 is a flow chart illustrating in overview a shock detection method in accordance with an embodiment;

Figure 6 is a flow chart illustrating in overview a tamper detection method in accordance with an embodiment;

Figure 7a is a flow chart illustrating in overview a method of detecting a tamper event in accordance with an embodiment;

Figure 7b is a flow chart illustrating in overview a method of detecting a tamper event in accordance with a further embodiment;

Figure 8 is a flow chart illustrating in overview a method of switching a security device between a tamper detection mode and a shock detection mode in accordance with an embodiment;

Figure 9 is a plot of acceleration against time, showing an example of acceleration for a tamper event;

Figure 10 is a plot of acceleration against time, showing an example of acceleration for a door opening event; and

Figure 11 is a plot of acceleration against time, showing an example of acceleration for a door closing event.

Detailed description

[0079] As used herein, except where the context requires otherwise, the terms "comprises", "includes", "has", and grammatical variants of these terms, are not intended to be exhaustive. They are intended to allow for the possibility of further additives, components, integers or steps.

[0080] Figure 1 is a schematic illustration of a system in accordance with an embodiment. The system is mounted at an access point. In the illustrated embodiment, the access point comprises a door 108 and its corresponding door frame or surround 106. The door provides a moveable barrier whose movement allows the opening and closing of the access point. For example, the door 108 may slide relative to the door frame 106. The door 106 may rotate around a hinge (not shown).

[0081] In other embodiments, the access point may comprise any openable or breakable structure, for example a window or gate. The access point may further comprise any corresponding frame or surround.

[0082] Coordinate axes are shown, with x being horizontal along a plane of the door 108 when closed, y being vertical, and z being horizontal perpendicular to the plane of the door 108 when closed. In other embodiments, any suitable coordinate system may be used. Cartesian axes and/or rotational axes may be defined.

[0083] The system comprises a security device 102 and a second device 104. The second device 104 comprises a magnet 110.

[0084] The security device 102 has a surface (not shown) for mounting the sensor device against a first component of the access point, which in the embodiment of Figure 1 is the door frame 106. The second device 104 has a surface (not shown) for mounting the second device 104 against a second component of the access point. In the embodiment of Figure 1, the second component of the access point is the door frame 106.

[0085] In other embodiments, the security device 102 may be mounted on the door 108 and the second device 104 may be mounted on the door frame 106. In further embodiments, the security device 102 may be mounted on any first component of the access point, and the second device 104 may be mounted on any second component of the access point, wherein the first component and second component are relatively moveable. Any suitable method of mounting the security device 102 and second device 104 may be used. For example, the security device 102 and second device 104 may each be adhesively mounted.

[0086] The security device 102 and second device 104 are shown in exaggerated size in Figure 1 to increase the clarity of the figure. The figure is not to scale.

[0087] Figure 2 is a schematic illustration of components of the security device 102. The security device 102 comprises an accelerometer 212 and a magnetic sensor 214. The security device 102 further comprises a processor 204, a memory 206 and a transceiver 208. The security device 102 further comprises a battery 210 configured to power the security device 210. In the present embodiment, the security device 102 does not require a connection to mains power.

[0088] In the present embodiment, the accelerometer 212, magnetic sensor 214, processor 204, memory 206, transceiver 208 and battery 210 are housed within a common housing. In further embodiments, the accelerometer 212, magnetic sensor 214, processor 204, memory 206, transceiver 208 and battery 210 may be housed within any suitable housing or housings. In further embodiments, the security device 102 may not include one or more of the accelerometer 212, magnetic sensor 214, processor 204, memory 206, transceiver 208 and battery 210.

[0089] In the present embodiment, the accelerometer 212 is configured to sense acceleration of the security device on each of three orthogonal axes. In other embodiments, the accelerometer 212 may be replaced or supplemented by any sensor configured to sense acceleration of the security device. The sensor may sense acceleration in any one or more axes.

[0090] The magnetic sensor 214 is configured to sense magnetic field. In use, the magnetic sensor 214 senses a magnetic field of the magnet 110. The magnetic field sensed by the magnetic sensor 214 is dependent on the separation between the magnetic sensor 214 and the magnet 110. A change in the position of the door 108, for example from closed to open, causes a change in the magnetic field that is sensed by the magnetic sensor 214.

[0091] In other embodiments, the magnetic sensor 214 may be replaced or supplemented by a different sensor that may be used in sensing an open or closed state of the access point, for example an electrical or optical sensor. The magnet 110 may be replaced or supplemented by a corresponding component, for example a light source.

[0092] In some embodiments, at least one sensor component of the security device is configured for use in detecting an open state or closed state of the access point without the use of a corresponding component in the second device 104, for example without the presence of a magnet 110 or light source. In some such embodiments, the second device 104 may be omitted. In some embodiments, the security device 102 is mounted on a moveable component of the access point. Optionally in such embodiments, the accelerometer 212 may be used to detect an open state or closed state of the access point, for example by detecting movement from an open state to a closed state or from a closed state to an open state.

[0093] The processor 204 comprises processing circuitry which is configured to receive and process output from the accelerometer 212 and magnetic sensor 214. The processor 204 may store data in and/or retrieve data from the memory 206.

[0094] The transceiver 208 is a wireless transceiver configured to transmit signals to, and receive signals from, a control hub 114. In other embodiments, the security device 102 may comprise any suitable transmitter and/or receiver for transmitting signals to and/or receiving signals from the control hub 114. The processor 204 is configured to instruct the transceiver 208 to wirelessly transmit data to the control hub 114.

[0095] The control hub 114 comprises a processor (not shown) and a wireless transceiver (not shown) configured to transmit signals to, and receive signals from, the security device 102. In some embodiments, the wireless transceiver of the control hub 114 is also configured to transmit signals to and/or receive signals from further security devices, or other devices.

[0096] The processor of the control hub 114 and the processor 204 may each comprise one or more processing chips and/or components. For example, each processor may comprise: control circuitry; and/or processor circuitry; and/or at least one application specific integrated circuit (ASIC); and/or at least one field programmable gate array (FPGA); and/or single or multi-processor architectures; and/or sequential/parallel architectures; and/or at least one programmable logic controllers (PLCs); and/or at least one microprocessor; and/or at least one microcontroller; and/or a central processing unit (CPU); and/or a graphics processing unit (GPU).

[0097] In the illustrated examples, transceiver 208 is shown as being distinct from corresponding processor 204 but in some embodiments at least part of the processing aspects of the transceiver 208 may have hardware in common with at least one processor component of the corresponding processing circuitry 204.

[0098] A memory may be separate from each processor and/or partly or wholly integrated onto a common chip(s) with the processor. The memory may store code that, when read by the processing circuitry, causes performance of any of the methods described herein, and/or as illustrated in in the drawings. For example, the memory may comprise: volatile memory, for example, one or more dynamic random access (DRAM) modules and/or static random access memory (SRAM) modules; and/or non-volatile memory, for example, one or more read only memory (ROM) modules, which for example may comprise a Flash memory and/or other electrically erasable programmable read-only memory (EEPROM) device. The code may for example be software, firmware, or hardware description language (HDL) or may be any combination of these or any other form of code for one or more processors that is known by a person skilled in the art.

[0099] Further, in other embodiments, the memory 206 of the security device 102 may instead, or at least in part be provided by a memory device(s) that may in some embodiments be separate or removable from the device. Such devices may comprise magnetic storage devices (e.g., hard disk, floppy disk, magnetic strips), optical disks (e.g., compact disk (CD), digital versatile disk (DVD)), smart cards, and removable flash memory devices (e.g., card, stick, key drive). Further, the memory components may be distributed. For example a distributed server may store code, which may be downloaded to the device for execution by processing circuitry described herein, to perform any method described herein that is executable by the processing circuitry. In some embodiments, the downloaded code may be stored on local memory of the device before execution by the processing circuitry.

[0100] In further embodiments, the system of Figure 1 may further comprise a server (not shown) and/or a monitoring system (not shown) that are remote from the control hub 114. The control hub 114 may be configured to communicate wirelessly with the server and/or monitoring system. For example, the monitoring system may comprise a monitoring system that is used to monitor multiple premises. The monitoring system may, additionally or alternatively comprise a smartphone or other personal portable device, such as may be in the possession of an owner of the premises.

[0101] Figure 3 is a flow chart 300 illustrating in overview a method of an embodiment. A sensor, for example accelerometer 212 of Figure 2, is configured to sense acceleration of a security device 102. A processor 204 is configured to process output of the sensor to determine

that a tamper event has occurred. For example, the tamper event may comprise physical removal of the security device 102 from an access point by an intruder.

[0102] At stage 302, the sensor senses acceleration of the security device 102.

[0103] At stage 304, the sensor produces a sensor output in response to sensing the acceleration.

[0104] At stage 306, a processor 204 identifies a potential tamper event.

[0105] At stage 308, the processor 204 processes the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event. At stage 310, the processor 204 designates the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0106] Figure 4 is a flow chart 400 illustrating in overview a method of an embodiment in which a processor 204 operates in, and disables, a tamper detection mode for detecting tamper events. A sensor, for example accelerometer 212 of Figure 2, is configured to sense acceleration of a security device 102. A processor 204 is configured to process output of the sensor in a tamper detection mode to determine that a tamper event has occurred.

[0107] At stage 402, the sensor senses acceleration of the security device.

[0108] At stage 404, the sensor produces a sensor output in response to sensing the acceleration.

[0109] At stage 406, a processor 204 operates in a tamper detection mode. The operating in a tamper detection mode comprises processing the sensor output to detect at least one tamper event.

[0110] At stage 408, the processor 204 disables the tamper detection mode in response to a determination that the access point is in a closed state. The tamper detection mode is not used when the access point is determined to be in the closed state. The tamper detection mode is used when the access point is determined not to be in the closed state.

[0111] Figure 5 is a flow chart 500 illustrating in overview a method of an embodiment in which a processor 204 operates in, and disables, a shock detection mode for detecting shock events. A sensor, for example accelerometer 212 of Figure 2, is configured to sense acceleration of a security device 102. A processor 204 is configured to process output of the sensor in a shock detection mode to determine that a shock event has occurred.

[0112] At stage 502, the sensor senses acceleration of the security device.

[0113] At stage 504, the sensor produces a sensor output in response to sensing the acceleration.

[0114] At stage 506, a processor 204 operates in a shock detection mode. The operating in the shock detection mode comprises processing the sensor output to detect at least one shock event.

[0115] At stage 508, the processor 204 disables the shock detection mode in response to a determination that the access point is not in a closed state. The shock detection mode is used when the access point is determined to be in the closed state. The shock detection mode is not used when the access point is determined not to be in the closed state.

[0116] Figure 6 is a flow chart 600 illustrating in overview a calibration method in accordance with an embodiment. At stage 602, a security device 102 is mounted to a mounting surface at an access point of a premises. For example, the security device 102 may be mounted to a door frame 106 or door 108. Any suitable method of mounting may be used, for example adhesive mounting.

[0117] The security device 102 comprises a sensor configured to sense acceleration of the security device 102 and produce a sensor output in response to the sensing of the acceleration. For example, the sensor may be an accelerometer 212 and the sensor output may be representative of acceleration in three orthogonal axes. In steady state, which may also be described as resting state, the output of the accelerometer 212 is indicative of the gravitational force vector.

[0118] At stage 604, a processor 204 processes the sensor output to determine an installation vector for the security device 102. The installation vector may comprise or represent a respective value of acceleration for each of a plurality of axes of the security device when the security device is not in motion. For example, the installation vector may comprise steady state acceleration values for x, y and z axes.

[0119] At stage 606, the processor 204 stores the determined installation vector of the security device 102. The stored steady state acceleration values may be used as offsets when calculating subsequent changes in acceleration. For example, the processor 204 may store the determined installation vector in a memory 206.

[0120] The processor 204 may use the installation vector to determine an orientation of a coordinate system of the accelerometer 212 and thus of the security device 102 relative to an environment in which it is installed. For example, it may be determined that x, y and z coordinates of the accelerometer 212 are aligned with two perpendicular horizontal axes and a vertical axis, respectively. In some embodiments, a mathematical manipulation, for example a rotation matrix, may be used to adjust for any misalignment in axes.

[0121] The processor 204 may determine one or more axes of interest based on the determined installation vector and/or further information about the access point. For example, if a component of the access point is known to move within a horizontal plane only, the processor may determine that movement along the vertical axis is particularly relevant to tampering. The processor 204 determines the orientation of the vertical axis based on the stored installation vector.

[0122] At stage 608, the processor 204 identifies a potential tamper event. The identifying of a potential tamper event means that there is a determination that tampering

may have occurred, but that further processing, which may be based on further measurement, is required to determine whether or not such tampering occurred. At stage 610, the processor 204 processes the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event. The determining whether values for the parameter meet the detection period over the sustained period of time may be in dependence on the stored installation vector. For example, the processor 204 may use acceleration values of the installation vector as offset values when determining changes in acceleration.

[0123] At stage 612, the processor 204 designates the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

[0124] In other embodiments, a determined installation vector may be used by the processor in any suitable manner, for example to inform any suitable action or decision. The use of a calibration process may enable the security device 102 to be installed in any orientation, rather than a prescribed orientation. In some embodiments, a calibration process may be repeated while the security device 102 is installed. For example, the calibration process may be repeated at a predetermined calibration interval.

[0125] The security device 102 of Figures 1 and 2 is configured to perform the methods of Figures 3, 4, 5 and 6. In other embodiments, a security device 102 may be configured to perform any one, two or three of the methods of Figures 3, 4, 5 and 6, or to perform all of the methods of Figures 3, 4, 5 and 6.

[0126] Figure 7a is a flow chart 700 illustrating in overview a tamper detection method in accordance with an embodiment. In the method of Figure 7a, the security device 102 is operated in a tamper detection mode. A tamper condition is identified based on an output of an accelerometer being greater than a threshold magnitude for more than a threshold amount of time. In other embodiments, any suitable method of determining a tamper event may be used.

[0127] The stages of Figure 7a as described below may be preceded by a calibration method as described above with reference to stages 602 to 606 of Figure 6, or by any other suitable calibration method.

[0128] At stage 702, a sensor of the security device 102 is active. The sensor is configured to sense acceleration of the security device 102. The sensor may also be referred to as a tamper detection sensor.

[0129] In the present embodiment, the sensor is the accelerometer 212 of Figure 2. The accelerometer 212 is configured to sense acceleration in each of the orthogonal axes. For example, the three orthogonal axes on which acceleration is sensed may be the x, y and z axes as illustrated in Figure 1. In other embodiments, any sensor configured to sense acceleration may be used.

[0130] At stage 704, the sensor produces a sensor output that is representative of acceleration. In the present embodiment, the sensor samples acceleration on each of the three axes at a sampling rate of 100 Hz. The sensor outputs values for acceleration on each axis every 10 ms. In other embodiments, a different sampling rate may be used.

[0131] At stage 706, the processor 204 processes the sensor output. At stage 706, the processor 204 is operating in a lower-power mode of operation, which may be referred to as a sleep mode. In some embodiments, the processor is configured to operate in more than one sleep mode, for example, a sleep mode and a deep sleep mode.

[0132] The processor 204 compares acceleration on each of the three axes to a first threshold value for acceleration. A different respective first threshold value may be used for each of the axes. The acceleration values may represent a difference between a measured acceleration and an acceleration sensed by the sensor due to gravity. In other words, a determined acceleration due to gravity may be used as an offset to the measured accelerations to determine the acceleration values. For example, the first threshold value for the y axis may take into account acceleration due to gravity. Further, the acceleration value compared to the first threshold value may be an absolute value for acceleration, such that the acceleration value that is compared to the first threshold value is always a positive number.

[0133] At stage 708, the processor 204 determines whether any of the accelerations exceeds its respective first threshold value. If none of the accelerations exceeds its respective first threshold value, the method of Figure 7a returns to stage 702 and the sensor continues to sense acceleration and produce sensor output that is representative of the acceleration.

[0134] If an acceleration on any axis exceeds its respective first threshold value, the method of Figure 7a proceeds to stage 710. At stage 710, the processor 204 determines that a potential tamper event is occurring based on the determination that the first threshold value has been exceeded. The processor 204 determines a potential tamper event has occurred if any of the accelerations exceeds its first threshold value at any one sample time.

[0135] At stage 712, the processor 204 transitions from the lower-power mode of operation, which may be referred to as a sleep mode, to a higher-power mode of operation, which may be referred to as a waking mode. The transition from sleep mode to waking mode is in response to the determining that a potential tamper event has occurred. In the present embodiment, the processor 204 wakes up for a period of one second, starting at the time at which the potential tamper event is identified.

[0136] The processor 204 initiates a detection window in which to determine whether a tamper event has occurred. In the present embodiment, the detection window is 1 second. In other embodiments, the detection window may be of any appropriate length.

[0137] At stage 714, the processor 204 processes the

sensor output. The processor 204 stores acceleration values for the three axes in memory 206. The processor 204 compares the acceleration values to a respective second threshold value for acceleration for each axis. In the present embodiment, the second threshold value for each axis is the same as the first threshold value for that axis. In other embodiments, the second threshold value may be different from the first threshold value. For example, the second threshold value may be lower than the first threshold value.

[0138] At stage 716, the processor 204 determines whether the values for acceleration have exceeded the second threshold value for a sustained period of time. In the present embodiment, the sustained period of time has a predetermined duration of 100 ms. The processor 204 determines that values for acceleration have exceeded the second threshold value for the sustained period of time if values for acceleration for a given axis have exceeded the second threshold value for that axis in 10 consecutive samples. In other embodiments, a different number of samples and/or a different sampling rate may be used. A shorter sustained period of time, for example 50 ms, may be used in some embodiments, and likewise the sampling rate may differ. However, regardless, the processor 204 determines whether at least a predetermined number of consecutive samples exceed the second threshold, and therefore whether the values for acceleration exceed the second threshold for at least a sustained period of time having a predetermined duration (since the sample rate is known). The predetermined number is generally selected to be more than 2, which also may have an effect of countering a noise sample.

[0139] If a threshold acceleration and/or predetermined duration of the sustained period of time is too low, there may be too many false tamper detections.

[0140] For example, if the predetermined duration of the sustained period of time is too short, there may be an increase in false tamper detections due to transient accelerations caused by a door opening action being confused for tamper events.

[0141] If the predetermined duration of the sustained period of time is too long, there is an increased chance that any changes in acceleration due to changes in orientation that result from a tamper may not be detected in cases where the orientation change is temporary.

[0142] Different sizes or materials of doors may impact a time required. For example, different sizes of doors may take different times to open and close.

[0143] In some embodiments, suitable values for the first threshold value, second threshold value and/or predetermined duration may be determined empirically. The empirical determination may be performed prior to installation, based on data collected from prior installations of devices that are the same as device 102.

[0144] If the values for acceleration have not exceeded the second threshold value over the predetermined duration of the sustained period of time, the method proceeds to stage 718. At stage 718, the processor 204 determines whether the detection window has expired. In the present embodiment, the detection window expires 1 second after the identifying of the potential tamper event.

[0145] If the detection window has not yet expired, the method returns to stage 714 and the processor continues to process the sensor output in the waking mode.

[0146] If the detection window has expired, the method proceeds to stage 720. At stage 720, the processor 204 determines that no tamper event has occurred within the detection window. The processor 204 reverts to sleep mode. After stage 720, the method returns to stage 702, in which the accelerometer 212 is active and sensing acceleration. In the embodiment of Figure 7a, the accelerometer 212 may always have a sampling rate of 100 Hz. In other embodiments, the accelerometer 212 may switch to a different sampling rate during the detection window.

[0147] If at stage 716 it is determined that acceleration has exceeded the second threshold value for a sustained period of time, which in this embodiment is 100 ms or 10 samples, the method proceeds to stage 722. At stage 722, the processor 204 determines that a tamper event has occurred. The processor 204 designates the potential tamper event that was identified at stage 710 as a tamper event. The method proceeds to stage 724 and 726, which may occur simultaneously or in either order.

[0148] At stage 724, the processor 204 activates an alarm (not shown in Figures 1 and 2) which is configured to operate acoustic and/or visual transducers to issue an audible or visible alarm signal. The alarm may form part of the security device 102. In some embodiments, the alarm and/or activation thereof by the processor 204 may be omitted.

[0149] At stage 726, the processor 204 instructs the transceiver 208 to send a message to the control hub 114 in response to the determining that a tamper event has occurred. The message may comprise data that is representative of the tamper event. The message may comprise data that is representative of the sensor output. In some embodiments, the control hub 114 may activate an alarm in response to the message.

[0150] In some embodiments, the processor 204 or control hub 114 may instruct a transmitter to send an alert notification to a remote monitoring system and/or server. For example, the control hub 114 may send a notification to an offsite server. In response to the notification, a service person may be sent to the premises at which the security device 102 is installed. The service person may check the security device 102. The service person may reinstall or replace the security device 102 if needed. Additionally, security personnel may be dispatched to the premises in response to the notification.

[0151] Once the message has been transmitted and/or the alarm has been triggered, the processor 204 remains in a waking mode until a notification is received from the control hub 114 indicating that the processor 204 can return to a sleep mode. For example, the processor 204

may receive a notification from the control hub 114 indicating that the tamper event has been recorded. The processor 204 may receive a notification from the control hub 114 that the tamper event is a false alarm. In other embodiments, the processor 204 may return to a sleep mode as soon as it has transmitted the message and/or triggered the alarm. In some embodiments, the processor 204 may wake up again, or continue in a waking mode, if accelerations continue to be above the first threshold value and/or the second threshold value.

[0152] In the method of Figure 7a, a potential tamper event is determined when the first threshold value is crossed. In other embodiments, for example the embodiment of Figure 7b as described below, a potential tamper event may be determined in dependence on a determined change of state of the access point, for example from a closed state to an open state.

[0153] In the present embodiment, both the potential tamper event and the occurrence of the tamper event are determined based on values for acceleration. The acceleration may be on any axis. If the acceleration on any axis exceeds the respective first threshold value for that axis, the processor 204 determines the potential start of a tamper event. Then, if the acceleration on any axis exceeds its respective second threshold value for at least 10 consecutive samples (100 ms) within the detection window of 1 second following the potential start of the tamper event, the processor 204 determines that a tamper event has occurred.

[0154] In other embodiments, the processor 204 may use any change in the output of the accelerometer 212 that is beyond a threshold amount for more than a threshold amount of time to detect a physical tamper event. A change in any one or more dimensions may be considered alone, or as a difference in a 3D vector.

[0155] In some embodiments, the processor 204 may determine the potential tamper event based on the comparison of any suitable first parameter to a first threshold value for that first parameter. For example, the first parameter may be a combination of values from multiple axes.

[0156] In the present embodiment, the tamper event is determined if acceleration on any given axis exceeds the respective second threshold value for that axis for 10 consecutive samples. The determination considers the axes separately. In other embodiments, the processor 204 determines that a tamper event has occurred if there are 10 consecutive samples in which any axis exceeds its second threshold value. For example, the processor 204 may determine that a tamper event has occurred if the x axis acceleration exceeds its second threshold value for 4 samples, then the y axis acceleration exceeds its second threshold value for the next 6 samples, even if neither the x axis acceleration nor the y axis acceleration exceeds its respective second threshold value for 10 consecutive samples.

[0157] In other embodiments, the processor 204 may determine that a tamper event has occurred based on whether any suitable second parameter has met a suitable detection condition for a sustained period of time. In the present embodiment, the second parameter is acceleration, and the detection condition is exceeding the second threshold value for 10 samples at the 10 Hz sampling rate or, equivalently, for 100 ms.

[0158] In other embodiments, the second parameter may be any suitable parameter. Values for the second parameter may be obtained by combining values for acceleration. For example, a value for the second parameter may be a sum or average of values obtained on one or more axes. The detection condition may be met if a given number or proportion of samples exceed the second threshold value within the predetermined duration, for example if 8 samples or 9 samples out of a set of 10 consecutive samples exceed the second threshold value. The detection condition may be based on an integrated acceleration value over a plurality of samples.

[0159] Any one or more of the stages of Figure 7a may be performed in dependence on an installation vector as determined using a calibration method.

[0160] In the embodiment described above with reference to Figure 7a, acceleration on all of the axes is considered. In other embodiments, one or more axes may be selected. Values from two or more axes may be combined, and the combined values compared to a first threshold value and/or a second threshold value for the combination. A selection or combination of axes may be based on a known configuration or pattern of movement of the access point.

[0161] In the embodiment of Figure 7a, a tamper condition is identified based on an output of an accelerometer 212 being greater than a threshold value for more than a threshold amount of time, wherein the threshold amount of time is greater than a maximum amount of the time that the acceleration is able to be greater than, or is typically greater than, the threshold by way of opening or closing a door or window on which the accelerometer may be mounted. The threshold amount of time may also be greater than a maximum amount of time for which the acceleration is greater than the threshold by way of a shock event. When an appropriate threshold amount of time is used, physical tamper detection may involve fewer false tamper detections, especially but not only in the case of opening and closing doors, and especially when the security device 102 is mounted on a moveable barrier.

[0162] If a physical tamper were to be detected by determining if an acceleration greater than a threshold value is sensed at a single point in time, without also applying a threshold amount of time, it may be the case that false tamper events would occur. For example, in a case in which the security device is mounted on a moveable barrier, the acceleration may rise above the threshold value when the moveable barrier is opened or closed. The acceleration due to opening or closing the moveable barrier may result in a false tamper detection.

[0163] Shock events are typically represented by short duration acceleration oscillations that decay to zero. An

example of a shock event may be someone banging on a door. Shock events may not be sustained in time.

[0164] Consider an embodiment in which the security device 102 is mounted on the moveable barrier. Opening and closing motions comprise accelerations that decay to zero because the motion of the moveable barrier eventually is stopped. Thus, any increases in acceleration due to opening or closing are followed by a decrease in acceleration.

[0165] In contrast, a physical tamper event is typically accompanied by a prolonged or permanent change in orientation of the device that has been moved. This results in a change in the direction of gravitational force vector, which is sensed by the accelerometer.

[0166] In the embodiment of Figure 1, the security device 102 is mounted on a door frame 106. In other embodiments, the security device 102 is mounted on a moveable barrier, for example door 108.

[0167] A normal opening or closing movement of the moveable barrier may cause a predictable change of acceleration. For example, moving the door 108 of Figure 1 may result in a change in acceleration in the x axis if the door 108 is a sliding door. Moving the door 108 of Figure 1 may result in a change of acceleration in the x and z axes if the door 108 is a hinged door. There will be a change of acceleration in two Cartesian axes or one rotational axis. In some embodiments, the processor 204 is configured to determine a tamper event based on detection of an acceleration that differs from an expected change of acceleration resulting from door opening or closing. For example, a threshold value for acceleration may be set to distinguish a tamper event from normal opening or closing. A duration for the sustained period of time for which a threshold is to be met may differ from a duration of acceleration due to normal opening or closing.

[0168] The door 108 may rotate around a vertically orientated hinge. Some access point components, for example windows, may have a horizontally oriented hinge. In the case of a horizontal hinge, movement of the moveable barrier results in a change in steady stage acceleration, when considered from the point of view of a security device 102 mounted on the moveable barrier. For example, when a window is closed, the measured gravity vector points in a first direction relative to the security device. When the window is opened by rotation around a horizontal hinge, the measured gravity vector points in a second direction relative to the security device 102, since the orientation of the security device 102 in space has changed.

[0169] It may often be the case that an access point component that rotates around a vertical hinge has a greater range of possible rotation than an access point that rotates round a horizontal hinge. For example, a door that rotates around a vertical hinge may have a range of rotation of 90 degrees or more. A window that rotates around a horizontal hinge may have a range of rotation of, for example, 20 degrees. The second threshold in the horizontal hinge case may be selected to be greater than that caused by, say, a 20 degree or rotation of the gravity vector (9.8ms^-2). Otherwise, a 20 degree opening of a window on the horizontal hinge with the sensor on the window, would result in more than 10 consecutive samples above the threshold (since in in the steady state it will be above the threshold), thus being mischaracterised as a physical tamper.

[0170] Figure 7b is a flow chart 730 illustrating in overview a tamper detection method in accordance with an embodiment. A security device 102 comprises an accelerometer 212, a magnetic sensor 214 and a processor 204 which may be mounted on a static part (e.g. a door frame 106) or a moving part (e.g. a door 108) of an access point. A second device 104 comprising a magnet 110 is mounted on the other of the parts of the access point.

[0171] At stage 732, the accelerometer 212 of the security device is active to sense acceleration of the security device 102. At stage 734, the accelerometer 212 produces a sensor output that is representative of acceleration. In the present embodiment, the sensor may sample acceleration on each of the three axes at a sampling rate of 100 Hz.

[0172] At stage 736, which may occur at the same time as stages 732 and 734, the magnetic sensor 214 is operable to sense magnetic field. The magnetic sensor 214 samples magnetic field at regular intervals, for example every second or every 0.1 second or every 0.5 seconds.

[0173] At stage 738, an output of the magnetic sensor 214 indicates that the door 108 has been opened. For example, the output of the magnetic sensor 214 may indicate a decrease in magnetic field.

[0174] At stage 740, a potential tamper event is determined in response to the change in magnetic field, since physical removal of the security device 102 is expected to result in a reduction in the sensed magnetic field. At this point in time it is unknown whether the change in magnetic field is due to such a physical tamper event, a magnetic event, or an access point opening event, and for this reason the event is treated as only a "potential" tamper event, which may more specifically be treated as a potential physical tamper event. At stage 742, the processor 204 transitions from sleep mode to a waking mode. In the embodiment of Figure 7b, the processor 204 wakes up for a period of one second, starting at the time at which the potential tamper event is identified. The processor 204 initiates a detection window in which to determine whether a tamper event has occurred. In the present embodiment, the detection window is 1 second. In other embodiments, the detection window may be of any appropriate length.

[0175] The flow chart of Figure 7b then proceeds to stages 714 to 726, which are the same as stages 712 to 726 of Figure 7a as described above. However, the embodiment of Figure 7b differs from the embodiment of Figure 7a in that potential tamper event is determined, and the detection window is started, in response to the output of the magnetic sensor 214 rather than in response

to the output of the accelerometer 212. Once the detection window is started, the determining of whether or not the potential tamper event is a tamper event is based on the output of the accelerometer 212 in both the embodiment of Figure 7a and the embodiment of Figure 7b.

[0176] In the embodiment of Figure 7b, a change of state of the access point is detected using a magnetic sensor of the security device in combination with a magnet of the second device 104. In other embodiments, the security device may be configured to detect a change of the state of the access point without use of any such second device. For example, the change of state may be identified based on sensed kinematics and/or orientation of a moveable barrier of the access point, for example using a multi-axis accelerometer. Any suitable method of sensing a change of state may be used to determine a potential tamper event and to start a detection window.

[0177] In the embodiment of Figure 7b, the accelerometer 212 may operate using the same sampling rate throughout. In other implementations, a sampling rate of the accelerometer 212 may change. The accelerometer 212 may switch between different modes, or may be switched off. For example, the accelerometer 212 may be switched on, or its sampling rate may be increased, when the potential tamper event is triggered by the determining of the door opening. The accelerometer 212 may be switched off, or its sampling rate may be decreased, when the detection window ends.

[0178] Figure 8 is a flow chart 800 illustrating in overview a method comprising operation of the processor 204 of the security device 102 in two different detection modes. A first detection mode is a tamper detection mode in which the processor 204 operates as described above with reference to Figure 7a. A second detection mode is a shock detection mode in which the processor 204 operates to detect shock.

[0179] In the embodiment of Figure 8, a single three-dimensional accelerometer is used for both shock sensing and physical tamper detection. Shock sensing and physical tamper detection are not performed at the same time. Instead, the processor 204 alternates between a shock detection mode and a tamper detection mode.

[0180] In the embodiment of Figure 8, the security device 102 is mounted on a static part (e.g. frame 106 of Figure 1) surrounding a moveable barrier or the moveable barrier (e.g. door 108 of Figure 1), and the second device 104 is mounted on the other of the parts.

[0181] At stage 802, the magnetic sensor 214 is operable to sense magnetic field. The magnetic sensor 214 samples magnetic field at regular intervals, for example every second or every 0.1 second or every 0.5 seconds. The processor 204 processes the output of the magnetic sensor.

[0182] At stage 804, which may occur at the same time as stage 802, the accelerometer 212 is operable to sense acceleration. The accelerometer 212 samples acceleration at regular intervals. For example, the accelerometer 212 may sample at a rate of 100 Hz.

[0183] At stage 806, the processor 204 determines that the barrier of the access point is closed based on the output of the magnetic sensor 214. For example, the processor 204 may compare a sensed magnetic field to a magnetic field that is expected when the magnetic sensor 214 is in proximity to the magnet 110 of the second device 104.

[0184] At stage 808, the processor 204 operates in a shock detection mode in response to the determination that the barrier is closed. In the shock detection mode, the processor 204 does not perform tamper detection. The processor 204 processes the output of the accelerometer 212 to determine whether a shock event has occurred. In the embodiment of Figure 8, the processor 204 is configured to recognise two different forms of shock. The processor 204 determines that a gross shock event has occurred if a first shock threshold value is exceeded. A gross shock may be a single shock event having energy above the first shock threshold value. An example of a gross shock event could be a window breaking. The first shock threshold value may be several g (several times the acceleration due to gravity).

[0185] The processor 204 determined that a repetitive shock has occurred if an integrated output of the accelerometer 212 over a given time exceeds a second shock threshold value. The time over which the output is integrated may be, for example, 20 seconds or 30 seconds. A repetitive shock event may comprise repeated small shocks. An example of a repetitive shock event could be a person drilling through a door.

[0186] If the processor 204 determines that a shock event has occurred, the processor 204 may instruct the transceiver 208 to transmit a message to the control hub 114 notifying the control hub 114 that a shock event has occurred. The processor 204 may trigger an alarm in dependence on determining that a shock event has occurred.

[0187] The processor 204 may continue in shock detection mode for as long as it determines, based on the output of the magnetic sensor 214, that the barrier is closed.

[0188] At stage 810, the processor 204 determines that the barrier has been opened. The processor 204 may determine that the barrier has been opened based on a change in the sensed magnetic field. For example, the determining may be based on a comparison of values of the sensed magnetic field to a magnetic threshold value. For example, the processor 204 may determine that the barrier has been opened if a value for the sensed magnetic field falls below an expected value for magnetic field when the barrier is closed. In other embodiments, any suitable method of determining that the barrier has been opened may be used.

[0189] At stage 812, the processor 204 switches from a shock detection mode to a tamper detection mode in response to the determining that the barrier has been opened.

[0190] In the tamper detection mode, the processor

204 processes the output of the accelerometer 212 to determine whether a tamper event has occurred. For example, the processor 204 may compare the output of the accelerometer 212 to a first threshold value and second threshold value as described above. While in tamper detection mode, the processor 204 does not process the output of the accelerometer 212 to determine whether a shock event has occurred.

[0191] If the processor 204 determines that a tamper event has occurred, the processor 204 may instruct the transceiver 208 to transmit a message to the control hub 114 and/or trigger an alarm.

[0192] The processor 204 continues in shock detection mode while the processor 204 determines, based on the magnetic sensor output, that the barrier is open.

[0193] At stage 814, the processor 204 determines, based on the magnetic sensor output, that the barrier has been closed. For example, the processor 204 may determine that a value for the magnetic sensor output meets an expected value for magnetic sensor output when the barrier is closed.

[0194] At stage 816, the processor 204 switches from tamper detection mode to shock detection mode. The processor 204 initiates a delay period starting from a time at which it is determined that the barrier has been closed. The processor 204 does not consider output received within the delay period when determining whether a shock event has occurred. The closing of a barrier, for example a door, may cause some continued movement of the barrier for a short period (e.g. 1 second) after the barrier is closed. By disregarding output received within the delay period, a risk of false shock event detections due to the barrier closing may be reduced.

[0195] At stage 818, after the delay period has finished, the processor 204 processes output of the accelerometer 212 to determine whether a shock event has occurred.

[0196] The steps of Figure 8 may be repeated many times. The processor 204 may switch from a tamper detection mode to a shock detection mode whenever the barrier is closed, and may switch from a shock detection mode to a tamper detection mode whenever the barrier is open. The processor 204 processes the output of the accelerometer 212 in shock detection mode and in tamper detection mode. However, the processor 204 applies different thresholds and detection criteria in each of shock detection mode and tamper detection mode.

[0197] In the present embodiment, a single accelerometer is used for shock sensing and physical tamper detection, but not at the same time. When the door is closed, the physical tamper mode is disabled. When a door open event is detected, for example due to a change in sensed magnetic field, the output of the accelerometer 212 is analysed to determine whether there is a physical tamper event. The analysis switches back to shock sensing mode when a door close event is detected, for example based on sensed magnetic field. In other embodiments, the shock sensing may be based on a first accelerometer and the physical tamper detecting may be based on a second accelerometer.

[0198] In the embodiment of Figure 8, the processor 204 determines an open state of the access point and a closed state of the access point based on output of the magnetic sensor 214. An open state is a state in which the processor 204 determines that the barrier of the access point is open, which may include configurations in which the access point is not fully closed. However, it is noted the determining of an open state or closed state is based on the information available to the processor 204, but there may be some circumstances in which the determining of the open state does not reflect the real state of the barrier. For example, if the security device is removed from its mounting by physical tampering, the processor 204 initially determines an open state because of a change in the magnetic field as detected by the magnetic sensor. Thus, in such a scenario, the security device may determine an open state even if the barrier is actually closed, at least until a tamper state is detected.

[0199] In other embodiments, the processor 204 is also configured to process the output of the magnetic sensor 214 to determine a magnetic tamper state. It is known that an intruder may attempt to circumvent detection of a door opening action by tampering with the magnetic sensor 214. For example, the intruder may position an external magnet next to the magnetic sensor 214 with the intention of causing the processor 204 to determine a door closed state even when the door has been opened. However, the magnetic sensor output caused by a magnetic tamper event may differ from the magnetic sensor output in a closed state. For example, introducing an external magnet near the magnetic sensor 214 may cause magnetic field to rise unexpectedly. The processor 204 may determine that a magnetic tamper has occurred if an output of the magnetic sensor increases beyond a normal output in the closed state. In other embodiments, any suitable criterion or criterion may be used to determine that the access point is in a magnetic tamper state. The processor 204 may set one or more magnetic sensor thresholds to which to compare the output of the magnetic sensor 214.

[0200] It is noted that the tamper detection mode described above is configured to detect physical tamper, for example the removal of the security device 102 from the access point. Magnetic tamper may be detected in the (physical) tamper detection mode and/or in the shock detection mode.

[0201] The processor 204 may switch to the tamper detection mode in response to a determination of any state that is not the closed state. For example, the processor 204 may switch to the tamper detection mode if it determines that the state of the access point has changed from closed to open. The processor 204 may switch to the tamper detection mode if it determines that the state of the access point has changed from closed to magnetic tamper.

[0202] In some embodiments, the processor 204 transmits different tamper notification types, e.g. for a physical

tamper and a magnetic tamper, respectively. In other embodiments, the processor 204 transmits a tamper notification that does not define whether the tamper event was caused by a physical or magnetic tamper.

[0203] A summary of actions resulting from a physical tamper may be as follows. Firstly, a case is considered in which the door is closed when a physical tamper action is performed. For example, the physical tamper action may comprise physical removal of the security device from an access point surface to which it is affixed. The physical removal of the security device 102 causes increased acceleration along one or more axes.

[0204] The magnetic sensor 214 detects a change in magnetic field, which is due to a change in position of the security device 102 relative to the magnet 110. The processor 204 processes an output of the magnetic sensor 214 and determines that the access point is in a non-closed state. The determining that the access point is in a non-closed state may comprise determining that the access point is in an open state. The determining that the access point is in a non-closed state may comprise determining that the access point is in a magnetic tamper state.

[0205] In some embodiments, the processor 204 only determines the state of the access point as being a closed state or a non-closed state, or between a closed state and an open state, and does not determine a magnetic tamper state. As discussed above, in some circumstances, the state of the access point determined by the processor 204 may not correctly reflect a non-closed state of the access point. For example, the processor 204 may determine an open state when a physical tamper has occurred, at least until the physical tamper is detected. In another example, the processor 204 may determine a magnetic tamper state, but a magnetic tamper state may occur when the access point is open, or when the access point is closed.

[0206] In response to the determining that the access point is in a non-closed state, the processor 204 switches from shock detection mode to tamper detection mode. The processor 204 sets at least one physical tamper threshold. In the present embodiment, the physical tamper thresholds comprise the first threshold value and the second threshold value. The processor 204 determines that the first threshold value has been crossed. The processor 204 is woken up. The processor 204 determines that the second threshold value has been crossed for the predetermined duration of 100 ms. In this example, the second threshold value and the first threshold value are the same. The processor 204 detects that the physical tamper has occurred.

[0207] The physical tamper triggers the processor 204 to detect a change in state from a closed state to a non-closed state based on the output of the magnetic sensor. The processor 204 switches from the shock detection mode to the tamper detection mode based on the detected change of state from the closed state to the non-closed state. The processor 204 then determines that a physical tamper has occurred by processing the output of the accelerometer 212 in the physical tamper mode.

[0208] A case is now considered in which a physical tamper occurs while the door is open. Since the door is open, the processor 204 is operating in the physical tamper mode. The processor 204 applies the first threshold value and second threshold value to the accelerator output. The processor 204 determines that the first threshold value has been crossed. The processor 204 is woken up. The processor 204 determines that the second threshold value has been crossed for the predetermined duration of 100 ms. The processor 204 detects that the physical tamper has occurred.

[0209] If a physical tamper occurs while the access point is determined to be in a magnetic tamper state, the detection of physical tamper is performed in the same manner to the case in which a physical tamper occurs while the access point is determined to be in an open state.

[0210] In the present embodiment, the detection of physical tamper can be positive only when the access point is determined to be in an open state or in a magnetic tamper state.

[0211] When the device 102 is removed from its mounted position it results in a determination by the processor that the access point is in the open state because the removal of the security device 102 will result in the separation of the magnetic sensor 214 from the magnet 110. When the magnetic field changes due to the separation, the processor 202 thinks the access point is open. Since the processor 102 doesn't know whether the access point is actually open or there has been a tamper event, it checks to see if there was a tamper event, or more in specifically, at least a physical tamper event.

[0212] A minimum number of samples for tamper event detection may be denoted as MIN_COUNT=10.

[0213] The processor 204 wakes up when a last determined state of the access point is a closed state, and a change in state is then detected based on an output of the magnetic sensor. The processor 204 wakes up when a last state is a magnetic tamper state, and the magnetic tamper state is exited. The processor 204 wakes up when a last determined state of the access point was open, and any of the low or high thresholds of any of the three axes for physical tamper are crossed.

[0214] The accelerometer 212 samples for 1 second at a sample rate of 100 Hz for a total of 100 samples per axis. The processor 204 counts a number of consecutive samples that are out of the thresholds per each axis. If this count is above MIN_COUNT, a physical tamper event is declared.

[0215] Figure 9 shows a plot 900 of acceleration in milli-g (i.e. 9.8 mm/s/s; also denoted herein as mg) against sample number for an example of a tamper event.

[0216] Figure 9 plots acceleration against sample number for acceleration on an x axis, shown as line 910, acceleration on a y axis, shown as line 920, and acceleration on a z axis, shown as line 930. The axes are as

shown in Figure 1. The x and z axes are in a horizontal plane, and the y axis is vertical.

[0217] Each axis has respective high and low thresholds. The x axis has a low threshold value 912 and a high threshold value 914. The low threshold value 912 is zero minus a first threshold value for the x axis, representing an acceleration of the first threshold value in a negative x direction. The high threshold value 914 is zero plus the first threshold value for the x axis, representing an acceleration of the first threshold value in a positive x direction. In the example of Figure 9, the first threshold value for the x axis is around 750 milli-g. An absolute value for acceleration on the x axis exceeds the first threshold value if the acceleration on the x axis falls below the low threshold value 912 or rises above the high threshold value 914. In the example of Figure 9, acceleration on the x axis does not cross its threshold. Acceleration on the x axis does not exceed its first threshold value.

[0218] The y axis has a low threshold value 922 and a high threshold value 924. In this example, y is vertical. Therefore, a baseline level for acceleration in the y axis may be taken to be acceleration due to gravity, which is 1 g, or 1000 mg, in a downwards direction. The low threshold value 922 for the y axis is -1000 mg minus a first threshold value for the y axis. The high threshold value is -1000 mg plus the first threshold value for the y axis. In the example of Figure 9, the first threshold value for the y axis is around 200 milli-g.

[0219] An absolute value for a difference in acceleration between the measured acceleration on the y axis and an offset value of -1000 mg is determined. The absolute value for the difference exceeds the first threshold value if the acceleration on the y axis falls below the low threshold value 922 for the y axis, or rises above the high threshold value 924 for the y axis.

[0220] In the example shown in Figure 9, the acceleration 920 for the y axis crosses the low threshold value 922 in a first instance highlighted by a circle 950. The crossing highlighted by circle 950 only crosses the low threshold value at a single sample.

[0221] The acceleration 920 for the y axis crosses the high threshold value 924 in a second instance highlighted by a circle 952. The crossing highlighted by circle 952 only crosses the high threshold value at a single sample.

[0222] The acceleration 920 for the y axis also crosses its high threshold value at sample 48. The crossing point is illustrated by a dashed line 940. The acceleration 920 for the y axis continues to be higher than its high threshold value until the end of the plot 900 at sample 100. The y axis has 52 consecutive samples above the high threshold.

[0223] The z axis of Figure 9 has a low threshold value 932 and a high threshold value 934. The low threshold value 932 is zero minus a first threshold value for the z axis. The high threshold value 934 is zero plus the first threshold value for the z axis. In the example of Figure 9, the first threshold value for the z axis is around 450 milli-g. An absolute value for acceleration on the z axis exceeds the first threshold value if the acceleration on the z axis falls below low threshold value 932 or rises above high threshold value 934.

[0224] In the example of Figure 9, the z axis acceleration 930 crosses its high threshold value 934 at sample number 30, which is indicated by a dashed line 942 at a crossing point. The z axis acceleration 930 continues to be above the high threshold value 934 until the end of the plot 900 at sample number 100. The z axis therefore exceeds its first threshold value for 70 consecutive samples.

[0225] The example of Figure 9 is now considered in view of the method described above in relation to Figure 7a. At the first crossing of a threshold at sample 30, the processor 204 determines a potential start of a tamper event. The processor 204 wakes up in response to the determining of the potential start. The processor 204 initiates a detection window of 1 second. Within the detection window, the processor 204 determines whether 10 consecutive samples exceed a threshold value. In the example of Figure 7a, it is the case that the first 10 consecutive samples in the detection window exceed the threshold value. The processor 204 determines that a tamper event has occurred. The processor 204 sends a message to the control hub 116 and triggers an alarm.

[0226] Figure 10 shows a plot 1000 of acceleration in milli-g (denoted mg) against sample number for an example of a real door open event. In Figure 10, the low and high threshold values 912, 914, 922, 924, 932, 934 are the same as those described above with reference to Figure 9.

[0227] Figure 10 plots acceleration against sample number for acceleration on an x axis, shown as line 1010, acceleration on a y axis, shown as line 1020, and acceleration on a z axis, shown as line 1030. In the example shown in Figure 10, the x axis acceleration 1010 does not cross its low threshold value 912 or its high threshold value 914.

[0228] The y axis acceleration 1020 crosses its low threshold value for a single sample value indicated by circle 1040. The y axis acceleration 1020 crosses its high threshold value for two sample values indicated by circle 1042, but they are not consecutive.

[0229] The z axis acceleration 1030 crosses its high threshold value for a two consecutive sample values indicated by circle 1044. The z axis acceleration 1030 crosses its high threshold value for a single sample value indicated by circle 1046.

[0230] In the example of Figure 10, all the crossings of the thresholds are brief.

[0231] The example of Figure 10 is now considered in view of the method described above in relation to Figure 7a. At the first crossing of a threshold, the processor 204 determines a potential start of a tamper event. The processor wakes up in response to the determining of the potential start. The processor 204 initiates a detection period of 1 second. Within the detection period, the processor 204 determines whether 10 consecutive samples

exceed a threshold value. In the example of Figure 10, the crossings are very short and it is not the case that 10 consecutive samples exceed a threshold value. No tamper event is detected and the processor returns to a sleep mode.

[0232] Figure 11 shows a plot 1100 of acceleration in milli-g (denoted mg) against sample number for an example of a door closing event. In Figure 11, the low and high threshold values 912, 914, 922, 924, 932, 934 are the same as those described above with reference to Figure 9.

[0233] Figure 11 plots acceleration against sample number for acceleration on an x axis, shown as line 1110, acceleration on a y axis, shown as line 1120, and acceleration on a z axis, shown as line 1130. It is noted that the range of acceleration shown in the vertical axis of plot 1100 is larger than that shown in plot 900 of Figure 9 and plot 1000 of Figure 10.

[0234] Circle 1140 highlights a sample at which the z axis acceleration crosses its high threshold value 934 for a single sample. Circle 1142 highlights a subsequent sample at which acceleration on each of the x, y and z axes crosses its respective low threshold value 914, 924, 934 for a single sample. Acceleration on the y axis also crosses its low threshold value 924 for a further sample. Circle 1144 highlights a subsequent collection of 3 consecutive samples at which acceleration on the z axis is beyond its high threshold value 934. Each of the crossings respectively indicated by the circles 1142 and 1140 is brief in duration.

[0235] The example of Figure 11 is now considered in view of the method described above in relation to Figure 7a. At the first crossing of a threshold, the processor 204 determines a potential start of a tamper event. The processor wakes up in response to the determining of the potential start. The processor 204 initiates a detection period of 1 second. Within the detection period, the processor 204 determines whether 10 consecutive samples exceed a threshold value. In the example of Figure 11, the crossings are very short and it is not the case that 10 consecutive samples exceed a threshold value. No tamper event is detected and the processor returns to a sleep mode.

[0236] It may be seen in Figure 10 and Figure 11 that high accelerations caused by door opening and door closing are short in duration. By evaluating changes in acceleration over a predetermined duration, for example 100 ms or 10 samples, a tamper event may be distinguished from normal door opening and door closing events.

[0237] In the embodiment for which data is illustrated in Figures 9 to 11, high and low threshold values are symmetric around a central value (0 or 1000 milli-g, depending on the axis), which may also be referred to as an offset value. The offset values are representative of steady state acceleration on each axis. In other embodiments, any appropriate values for high and low thresholds may be used. The high and low threshold values may not be symmetrical. For example, a high threshold value and low threshold value for the x axis may not be symmetrical around 0.

[0238] Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made within the scope of the present invention as defined by the claims. Moreover, features of one or more embodiments may be mixed and matched with features of one or more other embodiments.

[0239] Consistent with the present disclosure, each of the following clauses represent respective exemplary embodiments of the present invention.

1. A security device (102) for use at an access point of a premises, comprising:

    a sensor (212) configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration; and

    a processor (204) configured to operate in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event;

    wherein the processor (204) is configured to disable the tamper detection mode in response to a determination that the access point is in a closed state.

2. The device according to clause 1, wherein the processor (204) is further configured to provide the determination that the access point is in the closed state.

3. The device according to clause 2, wherein the providing of the determination that the access point is in the closed state comprises processing output of a further sensor to obtain values for a separation parameter that is representative of a separation between the security device (102) and a further device.

4. The device according to clause 2, wherein the determination that the access point is in the closed state is based on the sensor output.

5. The device according to any of clauses 1 to 4, wherein the processor is further configured to enable the tamper detection mode in response to a determination that the access point is not in the closed state.

6. The device according to clause 5, wherein the processor (204) is further configured to provide the determination that the access point is not in the closed state.

7. The device according to clause 5 or 6, wherein the providing of the determination that the access point is not in the closed state comprises processing output of a or the further sensor to obtain values for a or the separation parameter that is representative of a separation between the security device (102) and a or the further device.

8. The device according to clause 6, wherein the determination that the access point is not in the closed state is based on the sensor output.

9. The device according to any of clauses 1 to 8, wherein the processor is further configured to trigger an alarm in response to the detecting of the tamper event.

10. The device according to any of clauses 1 to 9, wherein the processor is further configured to instruct a transmitter to send a message to a further device (114) in response to the detecting of the tamper event.

11. The device according to any of clauses 1 to 10, wherein the processor is further configured to operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event.

12. The device according to clause 11, wherein:

the processor is further configured to switch from the tamper detection mode to the shock detection mode in response to a determination that a state of the access point has changed from a non-closed state to a closed state; and
the processor is further configured to switch from the shock detection mode to the tamper detection mode in response to a determination that a state of the access point has changed from a closed state to a non-closed state.

13. The device according to any of clauses 1 to 12, wherein the sensor comprises or forms part of an accelerometer that is configured to measure acceleration on each of three axes.

14. The device according to any of clauses 1 to 13, further comprising a magnetic sensor (214) for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field,
wherein the processor is configured to process the magnetic sensor output to provide the determination that the access point is in the closed state.

15. The device according to any of clauses 1 to 14, wherein the access point comprises at least a first component (106) and a second component (108), wherein at least one of the first component (106) and second component (108) is moveable to move relative to the other of the first component (106) and second component (108) to open and close the access point.

16. The device according to clause 15 as dependent on clause 14, wherein the magnetic sensor is mounted on one of the first and second components and is configured to sense a magnetic field of a magnet mounted on the other of the first and second components.

17. The device according to any preceding clause, wherein the detecting of the at least one tamper event comprises:

identifying a potential tamper event;
processing the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and
designating the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

18. A security method comprising:

sensing, by a sensor (212) of a security device (102) for use at an access point of a premises, an acceleration of the security device (102);
providing, by the sensor (212), a sensor output in response to sensing the acceleration;
operating a processor (204) of the security device (102) in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and
disabling, by the processor (204), the tamper detection mode in response to a determination that the access point is in a closed state.

19. A computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of:

receiving a sensor output from a sensor of a security device for use at an access point of a premises;
operating in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and
disabling the tamper detection mode in response to a determination that the access point is in a closed state.

20. A security device (102) for use at an access point of a premises, comprising:

a sensor configured to sense acceleration of the security device and produce a sensor output in response to sensing the acceleration; and
a processor (204) configured to operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event;
wherein the processor (204) is further configured to disable the shock detection mode in response to a determination that the access point is not in a closed state.

21. The device according to clause 20, wherein the processor (204) is further configured to provide the determination that the access point is not in the closed state.

22. The device according to clause 20 or 21, wherein the providing of the determination that the access point is not in the closed state comprises processing output of a further sensor to obtain values for a separation parameter that is representative of a separation between the security device (102) and a further device.

23. The device according to clause 21, wherein the determination that the access point is not in the closed state is based on the sensor output.

24. The device according to any of clauses 20 to 23, wherein the processor (204) is further configured to enable the shock detection mode in response to a determination that the access point is in the closed state.

25. The device according to clause 24, wherein the processor (204) is further configured to provide the determination that the access point is in the closed state.

26. The device according to clause 24 or 25, wherein the providing of the determination that the access point is in the closed state comprises processing output of a further sensor to obtain values for a or the separation parameter that is representative of a separation between the security device (102) and a or the further device.

27. The device according to clause 25, wherein the determination that the access point is in the closed state is based on the sensor output.

28. The device according to any of clauses 20 to 27, wherein the processor is configured such that the detecting of the at least one shock event disregards features of the sensor output occurring within a delay period after a determination that the access point has ceased to be in the closed state.

29. The device according to any of clauses 20 to 28, wherein the processor is further configured to trigger an alarm in response to the detecting of the at least one shock event.

30. The device according to any of clauses 20 to 29, wherein the processor is further configured to instruct a transmitter to send a message to a further device in response to the detecting of the at least one shock event.

31. The device according to any of clauses 20 to 30, wherein the sensor comprises or forms part of an accelerometer that is configured to measure acceleration on each of three axes.

32. The device according to any of clauses 20 to 31, wherein the detecting of the at least one shock event comprises determining that a value for a third parameter of the sensor output exceeds a shock threshold value.

33. The device according to clause 32, wherein the third parameter of the sensor output is representative of an energy of motion of the security device integrated over a predetermined integration time.

34. The device according to any of clauses 20 to 33, further comprising a magnetic sensor (214) for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field,
wherein the processor is configured to process the magnetic sensor output to provide the determination that the access point is not in the closed state.

35. The device according to any of clauses 20 to 34, wherein the access point comprises at least a first component (106) and a second component (108), wherein at least one of the first component (106) and second component (108) is moveable to move relative to the other of the first component (106) and second component (108) to open and close the access point.

36. The device according to clause 35 as dependent on clause 34, wherein the magnetic sensor is mounted on one of the first and second components and is configured to sense a magnetic field of a magnet mounted on the other of the first and second components.

37. The device according to any of clauses 20 to 36, wherein the processor is further configured to oper-

ate in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event.

38. The device according to clause 37, wherein:

the processor is further configured to switch from the tamper detection mode to the shock detection mode in response to a determination that a state of the access point has changed from a non-closed state to a closed state; and
the processor is further configured to switch from the shock detection mode to the tamper detection mode in response to a determination that a state of the access point has changed from a closed state to a non-closed state.

39. A security method comprising:

sensing, by a sensor of a security device for use at an access point of a premises, acceleration of the security device;
producing, by the sensor, a sensor output in response to the sensing of the acceleration;
operating a processor of the security device in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event; and
disabling, by the processor, the shock detection mode in response to a determination that the access point is not in a closed state.

40. A computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of:

receiving a sensor output from a sensor of a security device for use at an access point of a premises;
operating in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event; and
disabling the shock detection mode in response to a determination that the access point is not in a closed state.

41. A security device (102) for use at an access point of a premises, comprising:

a sensor (212) configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration; and
a processor (204) configured to:

identify a potential tamper event;
process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and
designate the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

42. The device according to clause 41, wherein determining whether values for the parameter of the sensor output meet the detection condition comprises comparing the values for the parameter of the sensor output to a threshold value.

43. The device according to clause 41 or clause 42, wherein the identifying of the potential tamper event comprises processing the sensor output to determine that a value for a further parameter of the sensor output meets a predefined condition.

44. The device according to clause 43, wherein the determining that the value for the further parameter of the sensor output meets the predefined condition comprises comparing the value for the further parameter to a further threshold.

45. The device according to any of clauses 41 to 44, wherein the identifying of the potential tamper event comprises determining, by the processor, that a change of state of the access point has occurred.

46. The device according to any of clauses 41 to 45 , further comprising a magnetic sensor (214) for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field.

47. The device according to clause 46 as dependent on clause 45, wherein the processor is configured to process the magnetic sensor output to perform the determining that the change of state of the access point has occurred.

48. The device according to any of clauses 41 to 47, wherein the security device is for use at an access point of a premises, the access point comprising at least a first component (106) and a second component (108), wherein at least one of the first component (106) and second component (108) is moveable to move relative to the other of the first component (106) and second component (108) to open and close the access point.

49. The device according to clause 48, wherein the sustained period of time is longer than a typical time for which values of the parameter meet the detection

condition when a normal opening or closing action of the first and/or second component of the access point is performed.

50. The device according to any of clauses 41 to 49, wherein the sustained period of time is between 50 ms and 500 ms, optionally between 50 ms and 250 ms, further optionally between 75 ms and 125 ms.

51. The device according to any of clauses 41 to 50, wherein the processor is further configured to initiate a detection window in response to identifying the potential tamper event, and to determine that the tamper event has occurred only if the sustained period of time occurs within the detection window.

52. The device according to any of clauses 41 to 51, wherein at least one of the sensor and the processor is configured to switch from a first mode to a second mode in response to the identifying of the potential tamper event.

53. The device according to any of clauses 41 to 52, wherein the processor is further configured to trigger an alarm in response to values for the parameter of the sensor output meeting the detection condition over the sustained period of time.

54. The device according to any of clauses 41 to 53, wherein the processor is further configured to instruct a transmitter to send a message to a further device in response to values for the parameter of the sensor output meeting the detection condition over the sustained period of time.

55. The device according to any of clauses 41 to 54, wherein the sensor comprises or forms part of an accelerometer that is configured to measure acceleration on each of three axes.

56. The device according to any of clauses 41 to 55, wherein at least one of the parameter and the further parameter comprises or is representative of acceleration on a single axis.

57. The device according to any of clauses 41 to 55, wherein at least one of the parameter and the further parameter comprises or is representative of acceleration on two axes.

58. The device according to any of clauses 41 to 57, wherein at least one of a) and b):-

a) the further parameter is the same as the parameter;
b) the further threshold value is the same as the threshold value.

59. The device according to any of clauses 41 to 58, wherein the sensor and the processor are housed within a common housing of the security device.

60. The device according to any of clauses 41 to 59, wherein the security device further comprises a battery configured to power the sensor and the processor.

61. A security method comprising:

sensing, by a sensor of a security device for a premises, acceleration of the security device;
providing, by the sensor, a sensor output in response to the sensing of the acceleration;
identifying, by the processor, a potential tamper event;
processing, by the processor, the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and
designating, by the processor, the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

62. A computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of:

receiving a sensor output of a sensor of a security device for a premises;
identifying a potential tamper event;
processing the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and
designating the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

63. A method comprising:

mounting a security device to a mounting surface at an access point of a premises, the security device comprising a sensor configured to sense acceleration of the security device and produce a sensor output in response to the sensing of the acceleration;
processing, by a processor, the sensor output to determine an installation vector for the security device, the installation vector comprising or representing a respective value of acceleration for each of a plurality of axes of the security de-

vice when the security device is not in motion; and
storing, by the processor, the determined installation vector.

64. The method of clause 63, further comprising processing, by the processor, the sensor output to:

identify a potential tamper event;
process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event, wherein the processing of the sensor output is dependent on the installation vector; and
designate the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

65. A security device (102) for use at an access point of a premises, comprising:

a sensor (212) configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration; and
a processor (204) configured to operate in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event;
wherein the processor (204) is configured to disable the tamper detection mode in response to a determination that the access point is in a closed state

66. A security device (102) for use at an access point of a premises, comprising:

a sensor configured to sense acceleration of the security device and produce a sensor output in response to sensing the acceleration; and
a processor (204) configured to operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event;
wherein the processor (204) is further configured to disable the shock detection mode in response to a determination that the access point is not in a closed state.

Claims

1. A security device (102) for use at an access point of a premises, comprising:

a sensor (212) configured to sense acceleration of the security device and to produce a sensor output in response to sensing the acceleration; and
a processor (204) configured to operate in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event;
wherein the processor (204) is configured to disable the tamper detection mode in response to a determination that the access point is in a closed state.

2. The device according to claim 1, wherein the processor (204) is further configured to provide the determination that the access point is in the closed state, wherein the providing of the determination that the access point is in the closed state comprises processing output of a further sensor to obtain values for a separation parameter that is representative of a separation between the security device (102) and a further device.

3. The device according to claim 2, wherein the determination that the access point is in the closed state is based on the sensor output.

4. The device according to any of claims 1 to 3, wherein the processor is further configured to enable the tamper detection mode in response to a determination that the access point is not in the closed state.

5. The device according to claim 4, wherein the processor (204) is further configured to provide the determination that the access point is not in the closed state.

6. The device according to claim 4 or 5, wherein the providing of the determination that the access point is not in the closed state comprises processing output of a or the further sensor to obtain values for a or the separation parameter that is representative of a separation between the security device (102) and a or the further device.

7. The device according to claim 5, wherein the determination that the access point is not in the closed state is based on the sensor output.

8. The device according to any of claims 1 to 7, wherein the processor is further configured to operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event.

9. The device according to claim 8, wherein:

the processor is further configured to switch from the tamper detection mode to the shock detection mode in response to a determination that a state of the access point has changed from a non-closed state to a closed state; and
the processor is further configured to switch from the shock detection mode to the tamper detection mode in response to a determination that a state of the access point has changed from a closed state to a non-closed state.

10. The device according to any of claims 1 to 9, wherein the sensor comprises or forms part of an accelerometer that is configured to measure acceleration on each of three axes.

11. The device according to any of claims 1 to 10, further comprising a magnetic sensor (214) for sensing a magnetic field and producing magnetic sensor output in response to sensing the magnetic field,
wherein the processor is configured to process the magnetic sensor output to provide the determination that the access point is in the closed state.

12. The device according to any of claims 1 to 11, wherein the access point comprises at least a first component (106) and a second component (108), wherein at least one of the first component (106) and second component (108) is moveable to move relative to the other of the first component (106) and second component (108) to open and close the access point, wherein the magnetic sensor is mounted on one of the first and second components and is configured to sense a magnetic field of a magnet mounted on the other of the first and second components.

13. The device according to any preceding claim, wherein the detecting of the at least one tamper event comprises:

identifying a potential tamper event;
processing the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event; and
designating the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time.

14. A security method comprising:

sensing, by a sensor (212) of a security device (102) for use at an access point of a premises, an acceleration of the security device (102);
providing, by the sensor (212), a sensor output in response to sensing the acceleration;
operating a processor (204) of the security device (102) in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and
disabling, by the processor (204), the tamper detection mode in response to a determination that the access point is in a closed state.

15. A computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the steps of:

receiving a sensor output from a sensor of a security device for use at an access point of a premises;
operating in a tamper detection mode, the operating in the tamper detection mode comprising processing the sensor output to detect at least one tamper event; and
disabling the tamper detection mode in response to a determination that the access point is in a closed state.

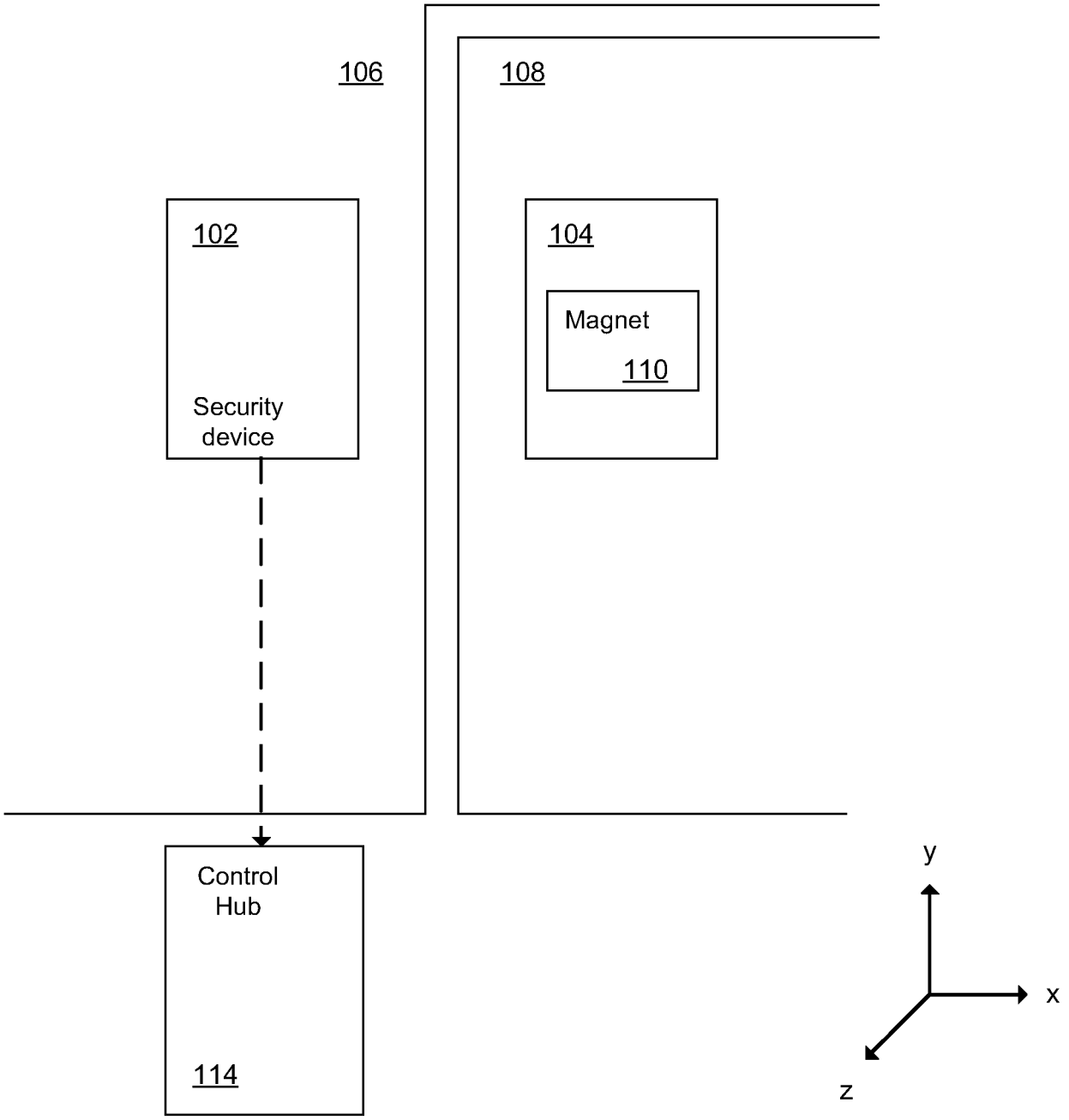
106
108
102
Security device
104
Magnet
110
Control Hub
114
y
x
z

FIG. 1

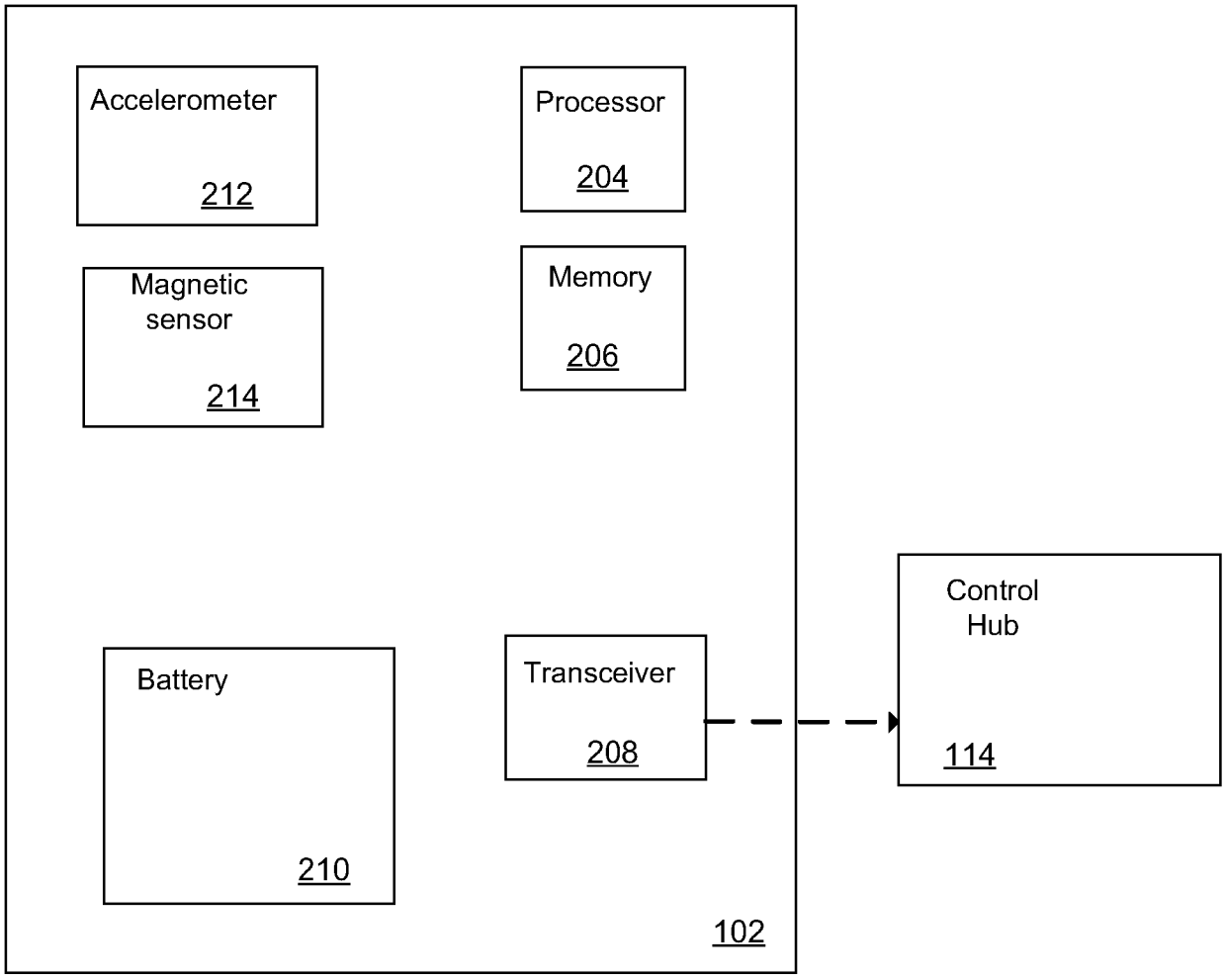
Accelerometer
212
Processor
204
Magnetic sensor
214
Memory
206
Control Hub
114
Battery
210
Transceiver
208
102

FIG. 2

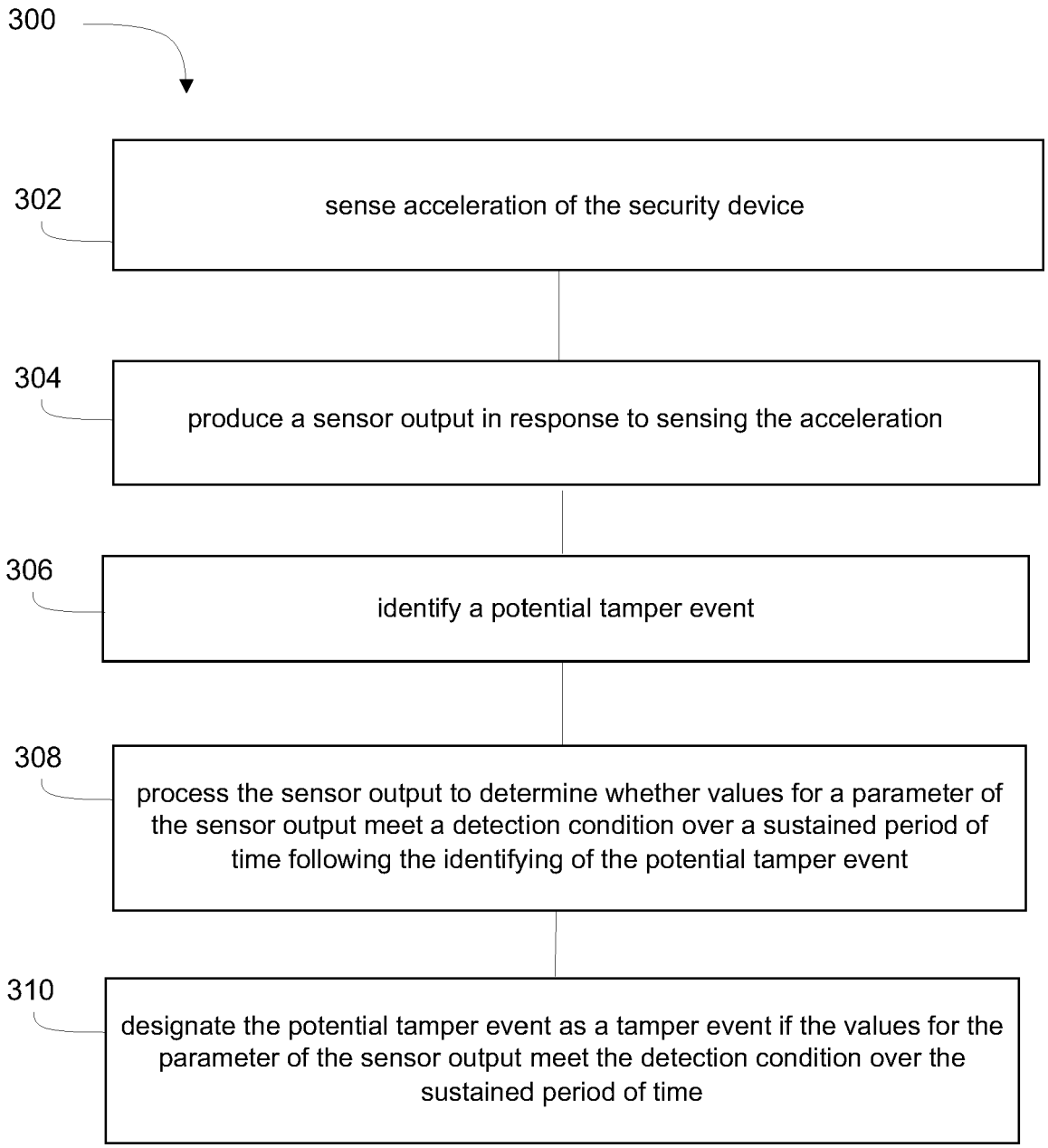
300
302
sense acceleration of the security device
304
produce a sensor output in response to sensing the acceleration
306
identify a potential tamper event
308
process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event
310
designate the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time

FIG. 3

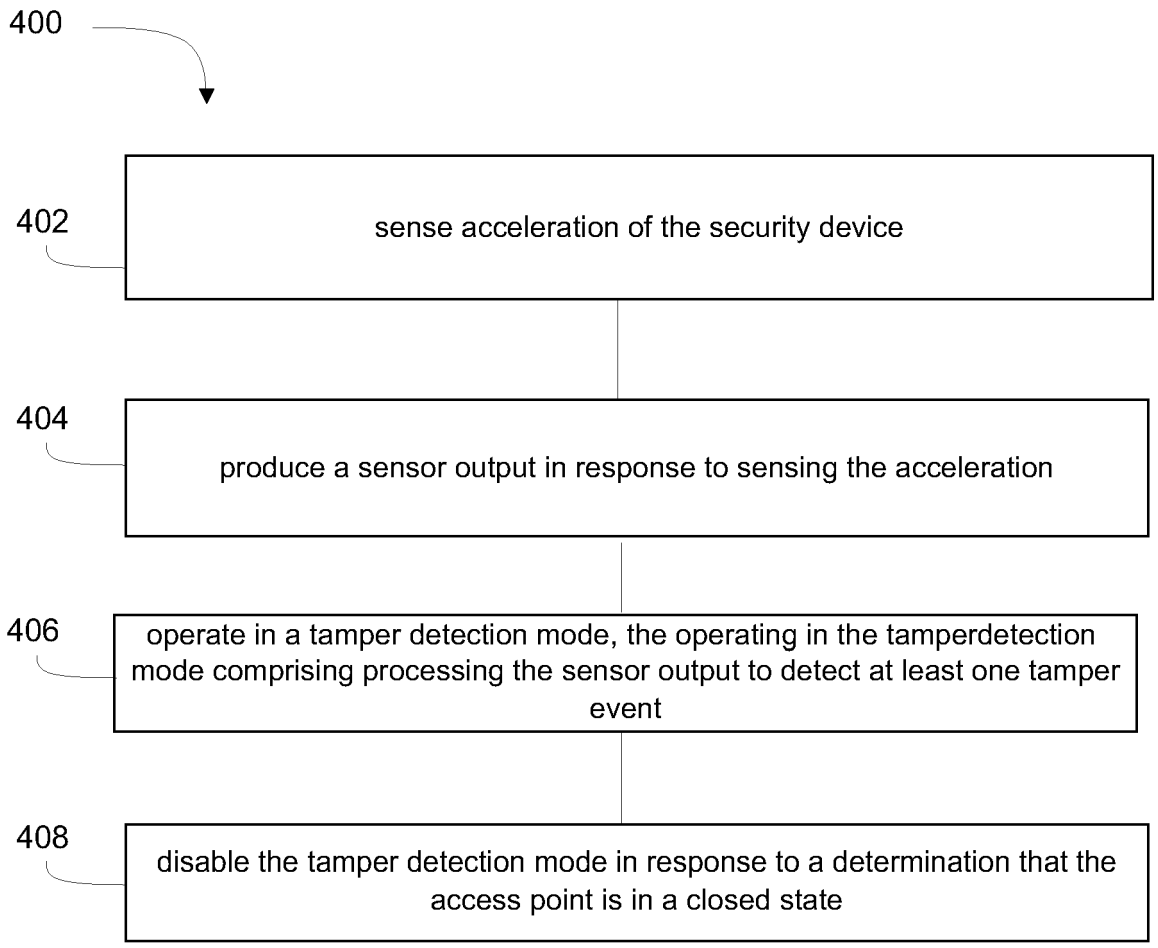
400
402
sense acceleration of the security device
404
produce a sensor output in response to sensing the acceleration
406
operate in a tamper detection mode, the operating in the tamperdetection mode comprising processing the sensor output to detect at least one tamper event
408
disable the tamper detection mode in response to a determination that the access point is in a closed state

FIG. 4

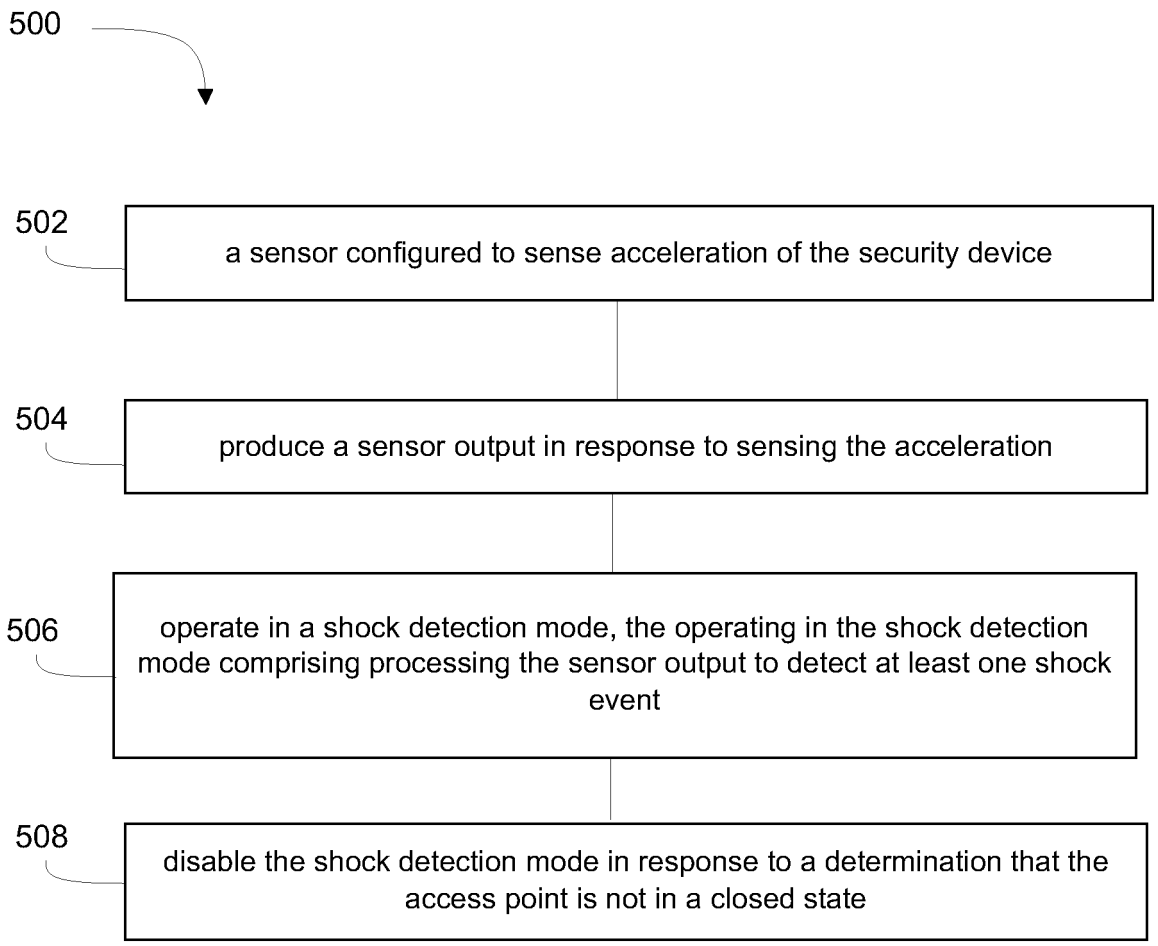
500
502
a sensor configured to sense acceleration of the security device
504
produce a sensor output in response to sensing the acceleration
506
operate in a shock detection mode, the operating in the shock detection mode comprising processing the sensor output to detect at least one shock event
508
disable the shock detection mode in response to a determination that the access point is not in a closed state

FIG. 5

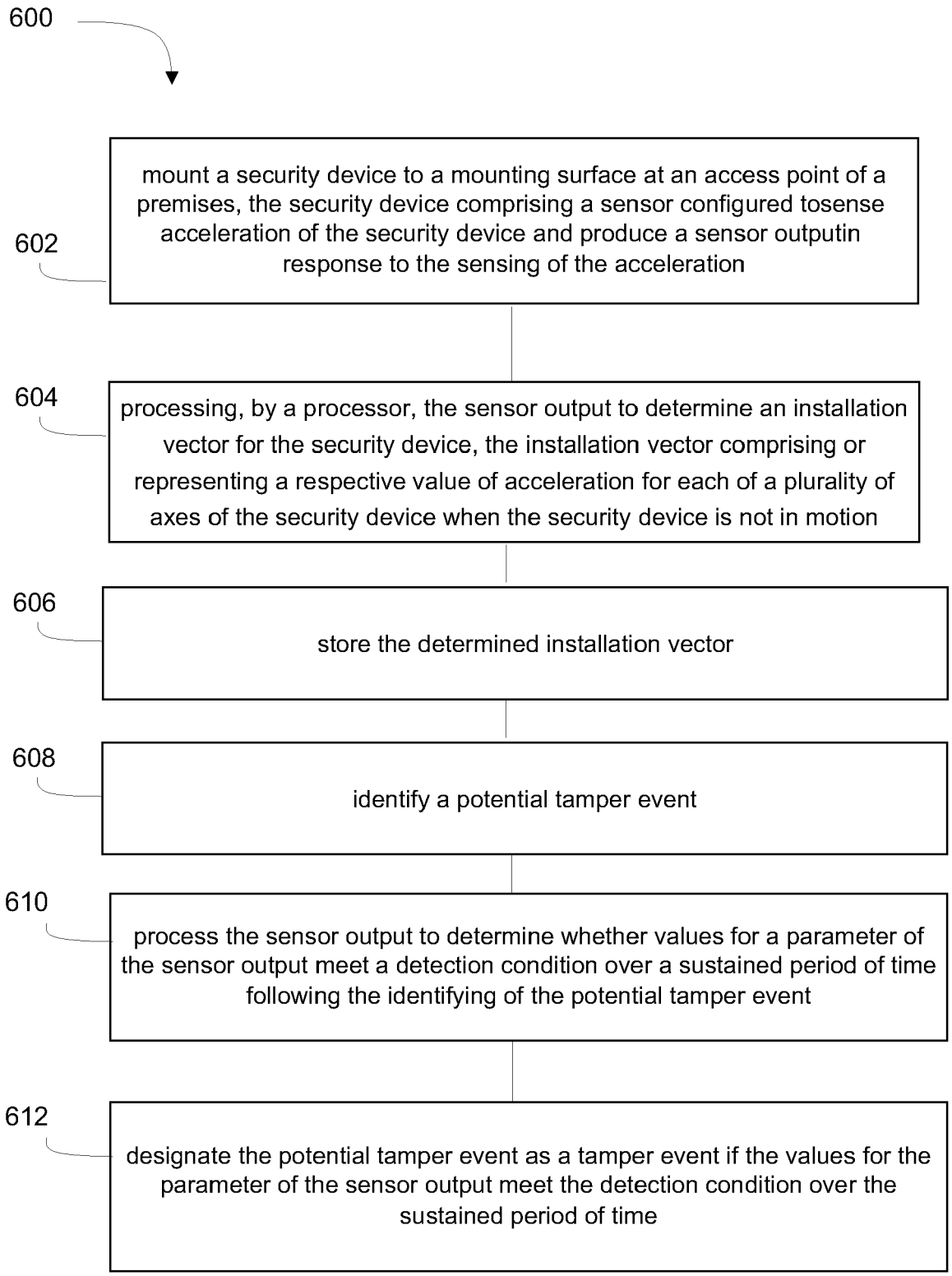
600
602
mount a security device to a mounting surface at an access point of a premises, the security device comprising a sensor configured tosense acceleration of the security device and produce a sensor outputin response to the sensing of the acceleration
604
processing, by a processor, the sensor output to determine an installation vector for the security device, the installation vector comprising or representing a respective value of acceleration for each of a plurality of axes of the security device when the security device is not in motion
606
store the determined installation vector
608
identify a potential tamper event
610
process the sensor output to determine whether values for a parameter of the sensor output meet a detection condition over a sustained period of time following the identifying of the potential tamper event
612
designate the potential tamper event as a tamper event if the values for the parameter of the sensor output meet the detection condition over the sustained period of time

FIG. 6

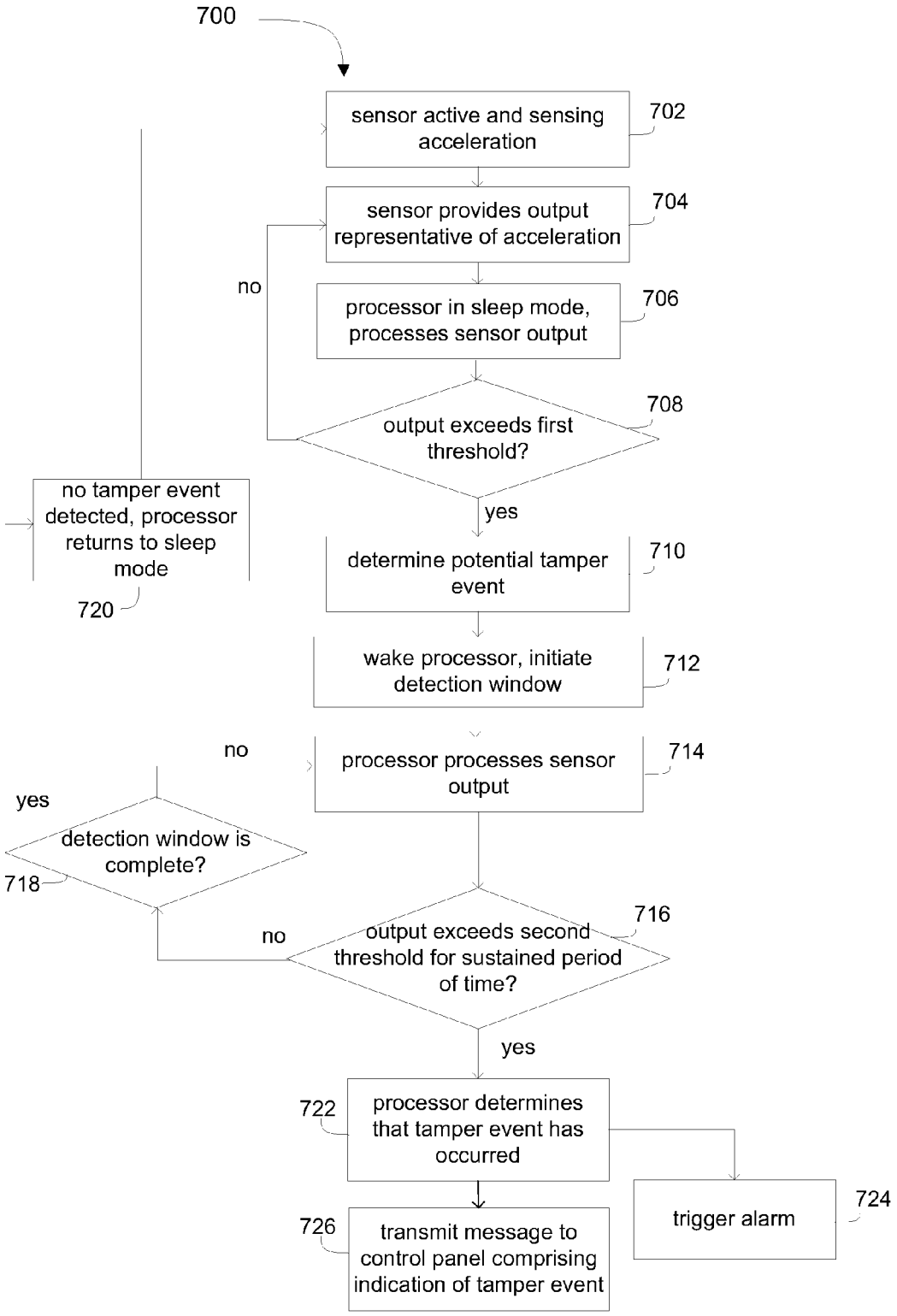
700
sensor active and sensing acceleration
702
sensor provides output representative of acceleration
704
no
processor in sleep mode, processes sensor output
706
output exceeds first threshold?
708
yes
no tamper event detected, processor returns to sleep mode
720
determine potential tamper event
710
wake processor, initiate detection window
712
no
processor processes sensor output
714
yes
detection window is complete?
718
no
output exceeds second threshold for sustained period of time?
716
yes
processor determines that tamper event has occurred
722
trigger alarm
724
transmit message to control panel comprising indication of tamper event
726

FIG. 7A

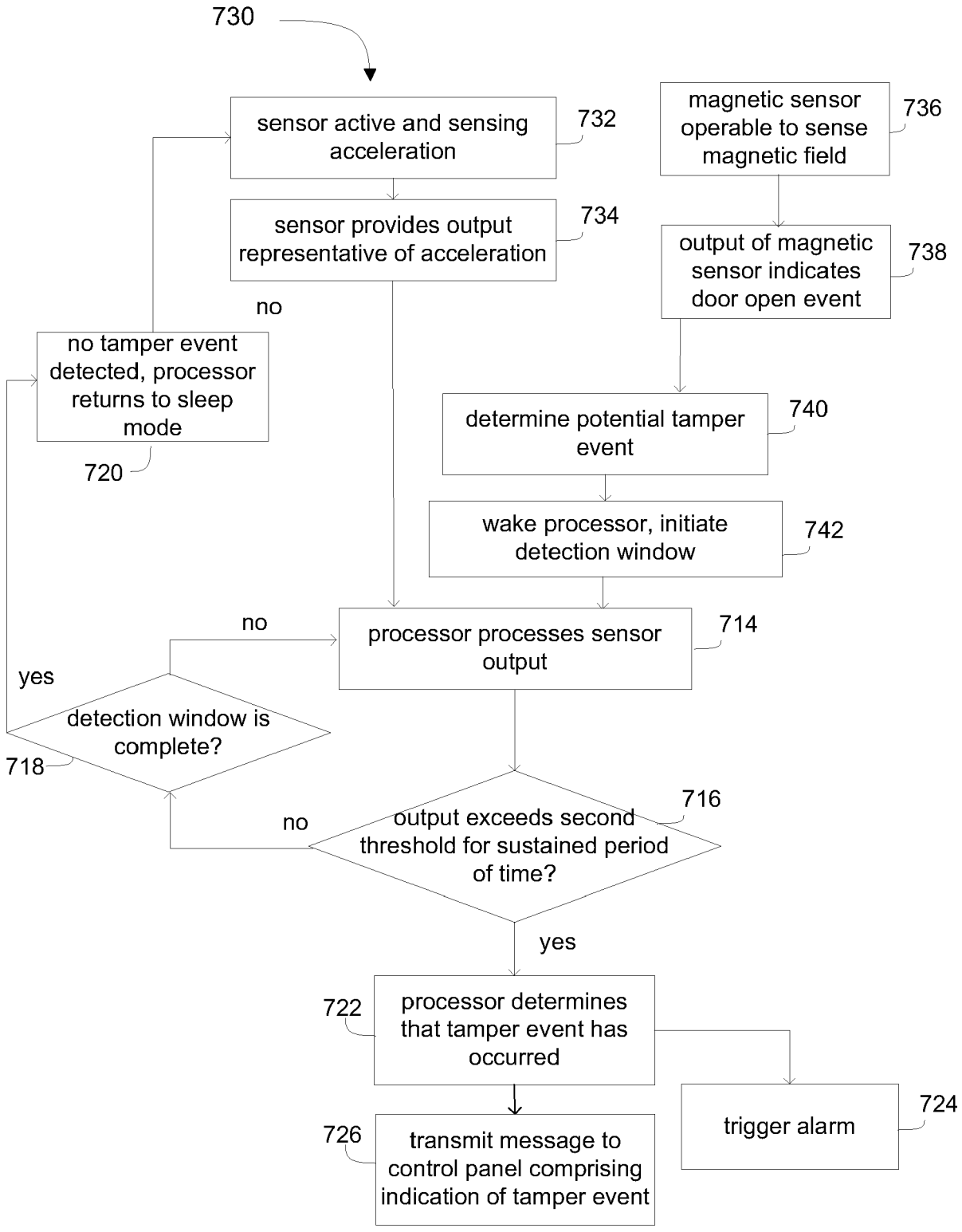
730
sensor active and sensing acceleration
732
magnetic sensor operable to sense magnetic field
736
sensor provides output representative of acceleration
734
output of magnetic sensor indicates door open event
738
no
no tamper event detected, processor returns to sleep mode
720
determine potential tamper event
740
wake processor, initiate detection window
742
no
processor processes sensor output
714
yes
detection window is complete?
718
no
output exceeds second threshold for sustained period of time?
716
yes
processor determines that tamper event has occurred
722
trigger alarm
724
transmit message to control panel comprising indication of tamper event
726

FIG. 7B

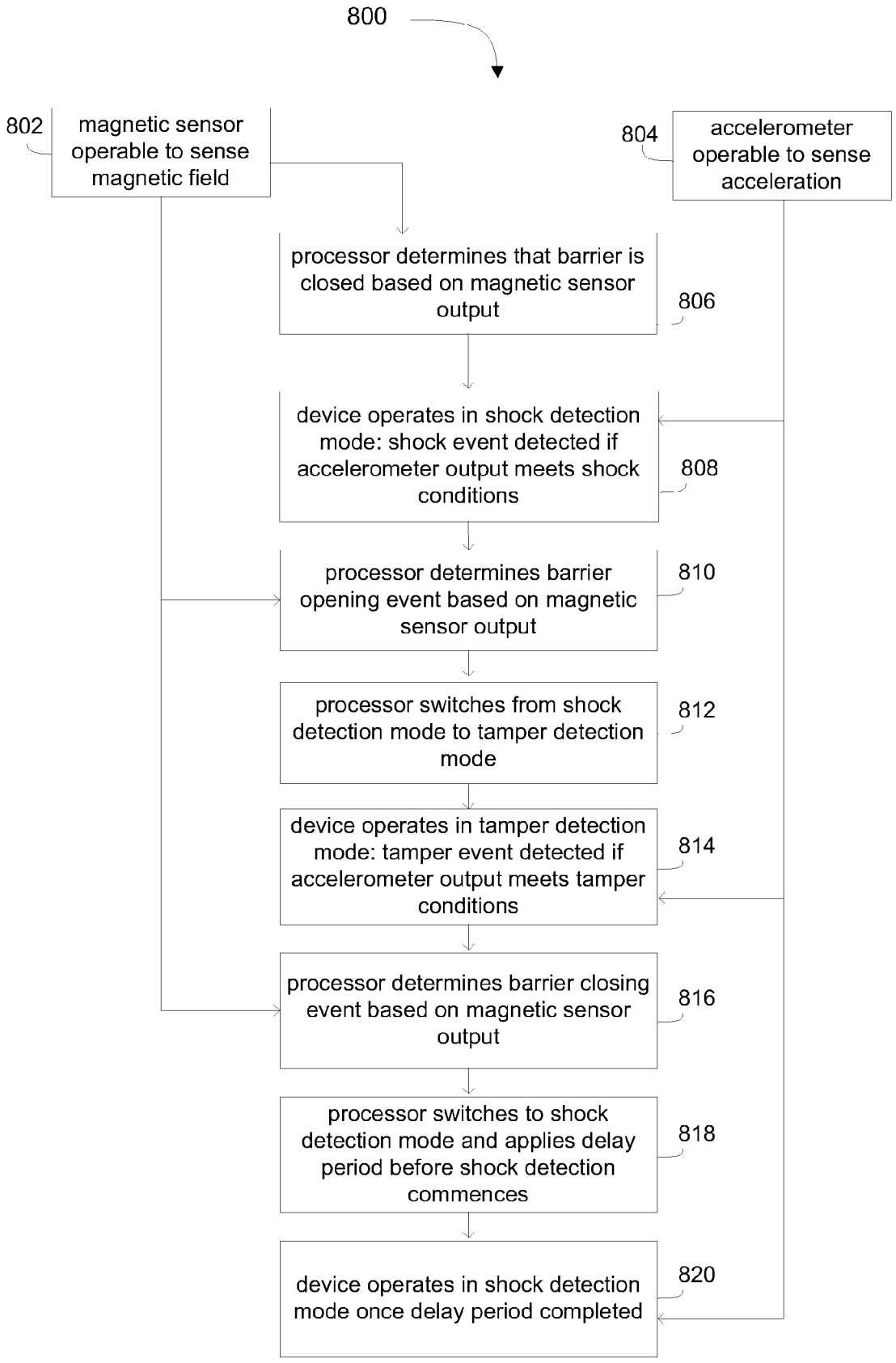
800
802
magnetic sensor operable to sense magnetic field
804
accelerometer operable to sense acceleration
processor determines that barrier is closed based on magnetic sensor output
806
device operates in shock detection mode: shock event detected if accelerometer output meets shock conditions
808
processor determines barrier opening event based on magnetic sensor output
810
processor switches from shock detection mode to tamper detection mode
812
device operates in tamper detection mode: tamper event detected if accelerometer output meets tamper conditions
814
processor determines barrier closing event based on magnetic sensor output
816
processor switches to shock detection mode and applies delay period before shock detection commences
818
device operates in shock detection mode once delay period completed
820

FIG. 8

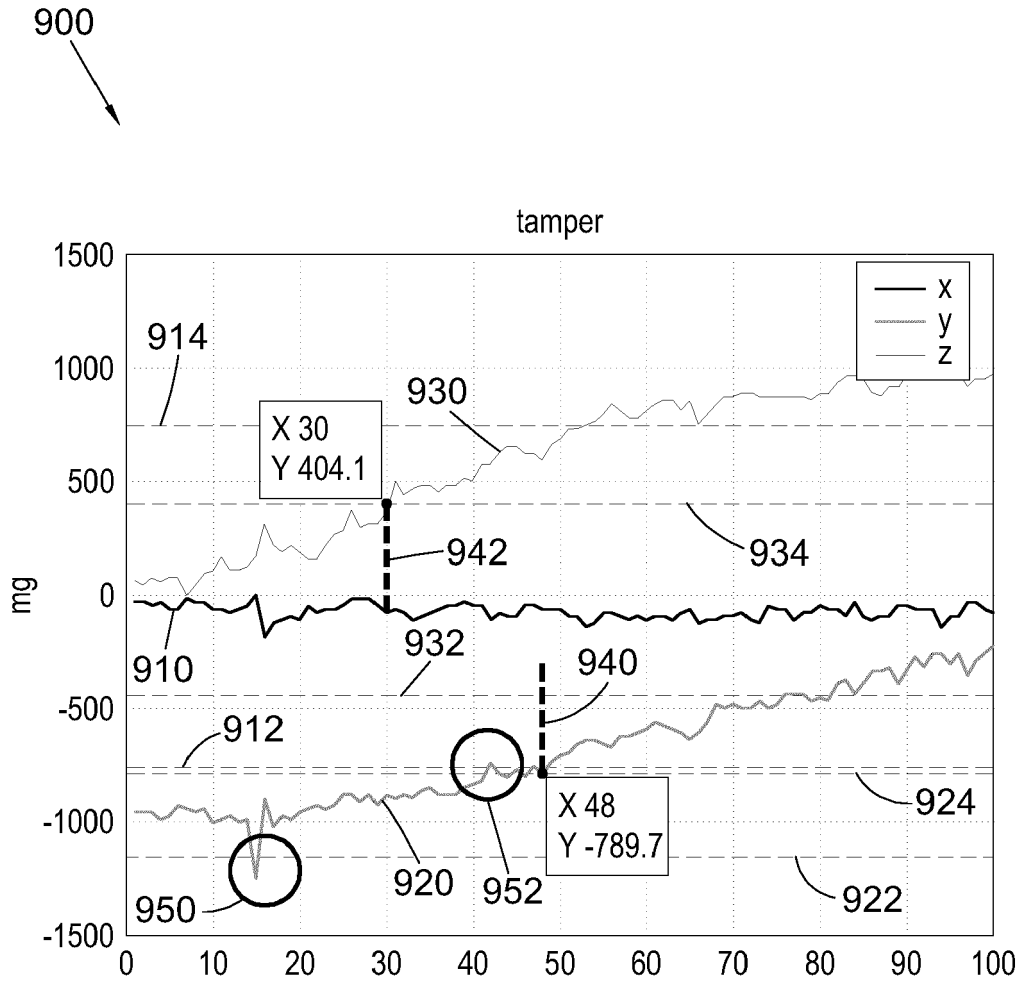
900
tamper
1500
1000
500
0
-500
-1000
-1500
mg
0
10
20
30
40
50
60
70
80
90
100
x
y
z
914
930
X 30
Y 404.1
942
934
910
932
940
912
924
X 48
Y -789.7
920
952
950
922

FIG. 9

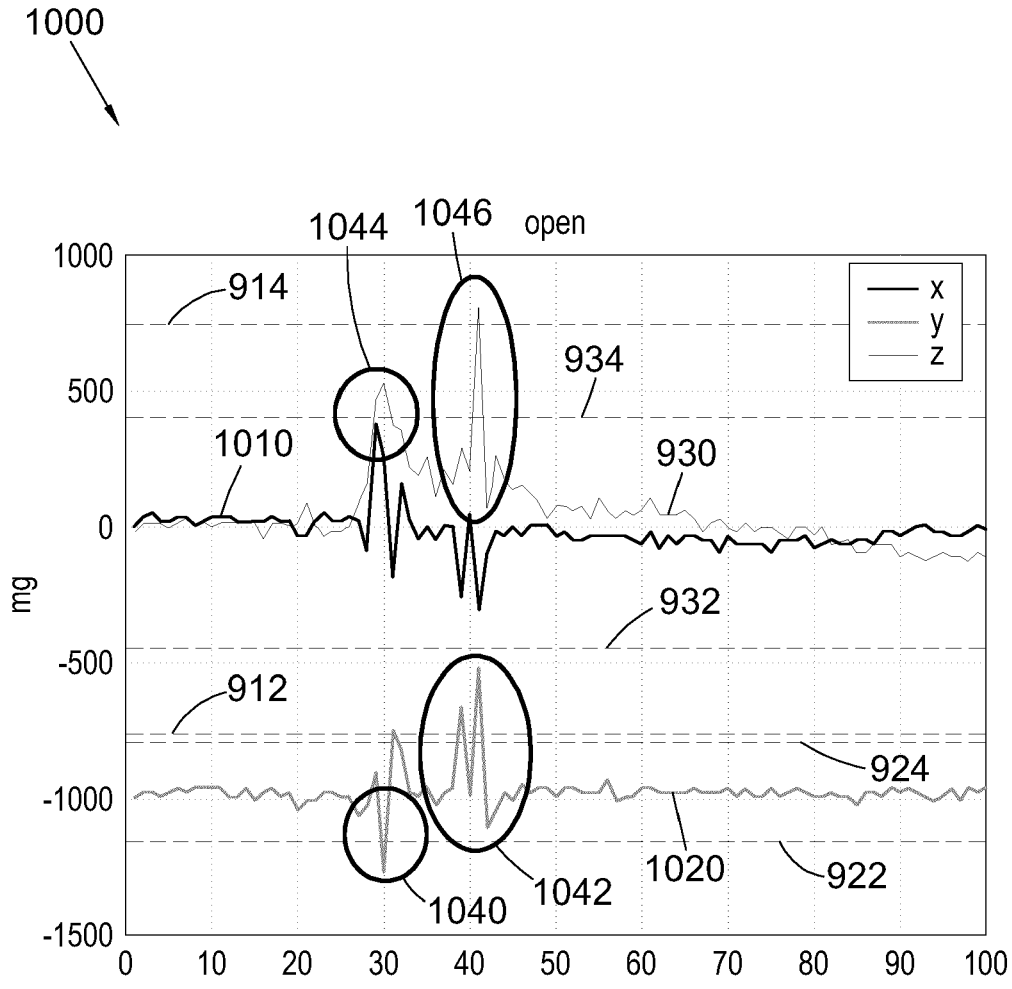
1000
1044
1046
open
914
934
1010
930
932
912
924
1020
922
1042
1040
x
y
z
mg
1000
500
0
-500
-1000
-1500
0
10
20
30
40
50
60
70
80
90
100

FIG. 10

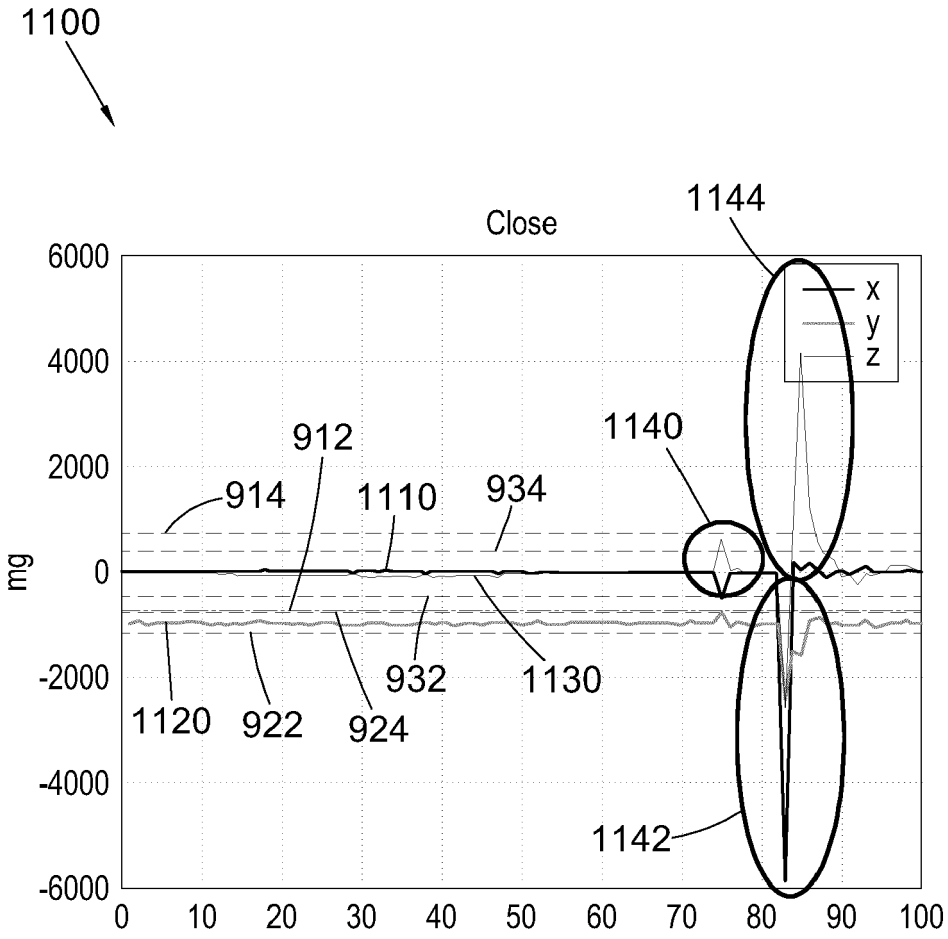
1100
Close
1144
6000
4000
2000
0
-2000
-4000
-6000
mg
x
y
z
912
914
1110
934
1140
1120
922
924
932
1130
1142
0
10
20
30
40
50
60
70
80
90
100

FIG. 11

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 17 8718

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y A	US 10 062 249 B1 (MODI YASH [US] ET AL) 28 August 2018 (2018-08-28) * figures 1,3a-3c * * column 4 - lines 27-54 * * column 5 - lines 4-26 *	1,4,14, 15 2,3,5-8, 10-13 9	INV. G08B13/08 G08B29/18
X Y	AU 2014 216 043 A1 (MCM ELECTRONICS PTY LTD) 10 March 2016 (2016-03-10) * paragraphs [0007], [0030], [0031]; figure 2 *	1,14,15 8	
Y	US 2013/057405 A1 (SEELMAN GEORGE [US] ET AL) 7 March 2013 (2013-03-07) * paragraph [0004]; figure 1a *	2,3,5-7	
Y	WO 2015/175697 A1 (SCHLAGE LOCK CO LLC [US]) 19 November 2015 (2015-11-19) * paragraph [0019] *	10-13	

TECHNICAL FIELDS SEARCHED (IPC)

G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	22 October 2021	Coffa, Andrew

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 21 17 8718

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.

22-10-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 10062249 B1	28-08-2018	NONE	
AU 2014216043 A1	10-03-2016	NONE	
US 2013057405 A1	07-03-2013	US 2013057405 A1	07-03-2013
		US 2016027268 A1	28-01-2016
		US 2017372569 A1	28-12-2017
		US 2019188978 A1	20-06-2019
		US 2020134993 A1	30-04-2020
		US 2021097824 A1	01-04-2021
WO 2015175697 A1	19-11-2015	CA 2949071 A1	19-11-2015
		MX 360490 B	24-10-2018
		US 2015330140 A1	19-11-2015
		US 2018038159 A1	08-02-2018
		US 2019211619 A1	11-07-2019
		US 2021172245 A1	10-06-2021
		WO 2015175697 A1	19-11-2015

EPO FORM P0459

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