Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3017644 A1 2017/09/28

(21) 3 017 644

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2017/03/23
(87) Date publication PCT/PCT Publication Date: 2017/09/28
(85) Entrée phase nationale/National Entry: 2018/09/12
(86) N° demande PCT/PCT Application No.: US 2017/023747
(87) N° publication PCT/PCT Publication No.: 2017/165610
(30) Priorité/Priority: 2016/03/24 (US62/312,709)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01),
E05B 47/00 (2006.01)

(71) Demandeur/Applicant:
SPECTRUM BRANDS, INC., US

(72) Inventeurs/Inventors:
BROWN, TROY M., US;
BUI, TAM, US...

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : ENSEMBLE VERROU SANS FIL A CARACTERISTIQUE ANTI-PIRATAGE
(54) Title: WIRELESS LOCKSET WITH ANTI-HACKING FEATURE

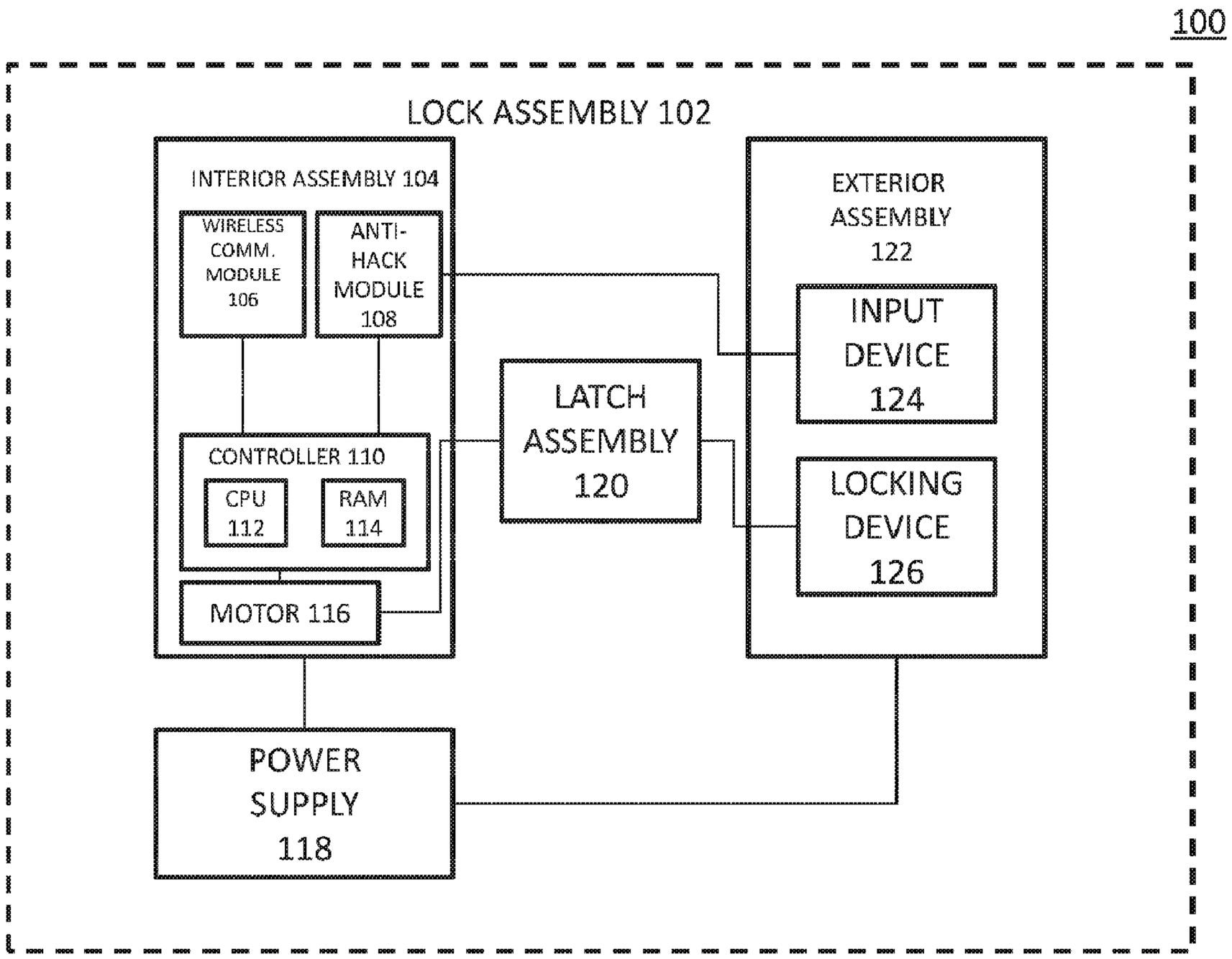

Figure 1

(57) Abrégé/Abstract:
A wireless lockset with integrated anti-hacking methods is described herein. The integrated anti-hacking methods in the wireless lockset allows the detection of unauthorized access by one or more individuals. The integrated anti-hacking methods can detect an

(21) 3 017 644

(13) A1

(57) Abrégé(suite)/Abstract(continued):
anomaly regarding wireless command sequence numbers, timing of received commands or flooding attack, and/or unauthorized access based on the MAC address of a command-issuing device. Upon detection of a hacking attempt, the wireless lockset performs one or more actions.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2017 (28.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/165610 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *E05B 47/00* (2006.01)

(21) International Application Number:
PCT/US2017/023747

(22) International Filing Date:
23 March 2017 (23.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/312,709 24 March 2016 (24.03.2016) US

(71) Applicant: **SPECTRUM BRANDS, INC.** [US/US]; 3001 Deming Way, Middleton, Wisconsin 53562 (US).

(72) Inventors: **BROWN, Troy M.**; 197 Woodcrest Lane, Lake Forest, California 92656 (US). **BUI, Tam**; 18575 Callens Cir, Fountain Valley, California 92708 (US).

(74) Agent: **WEVER, Michael E.**; BARNES & THORNBURG LLP, 888 S. Harrison Street, Suite 600, Fort Wayne, Indiana 46802 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) Title: WIRELESS LOCKSET WITH ANTI-HACKING FEATURE

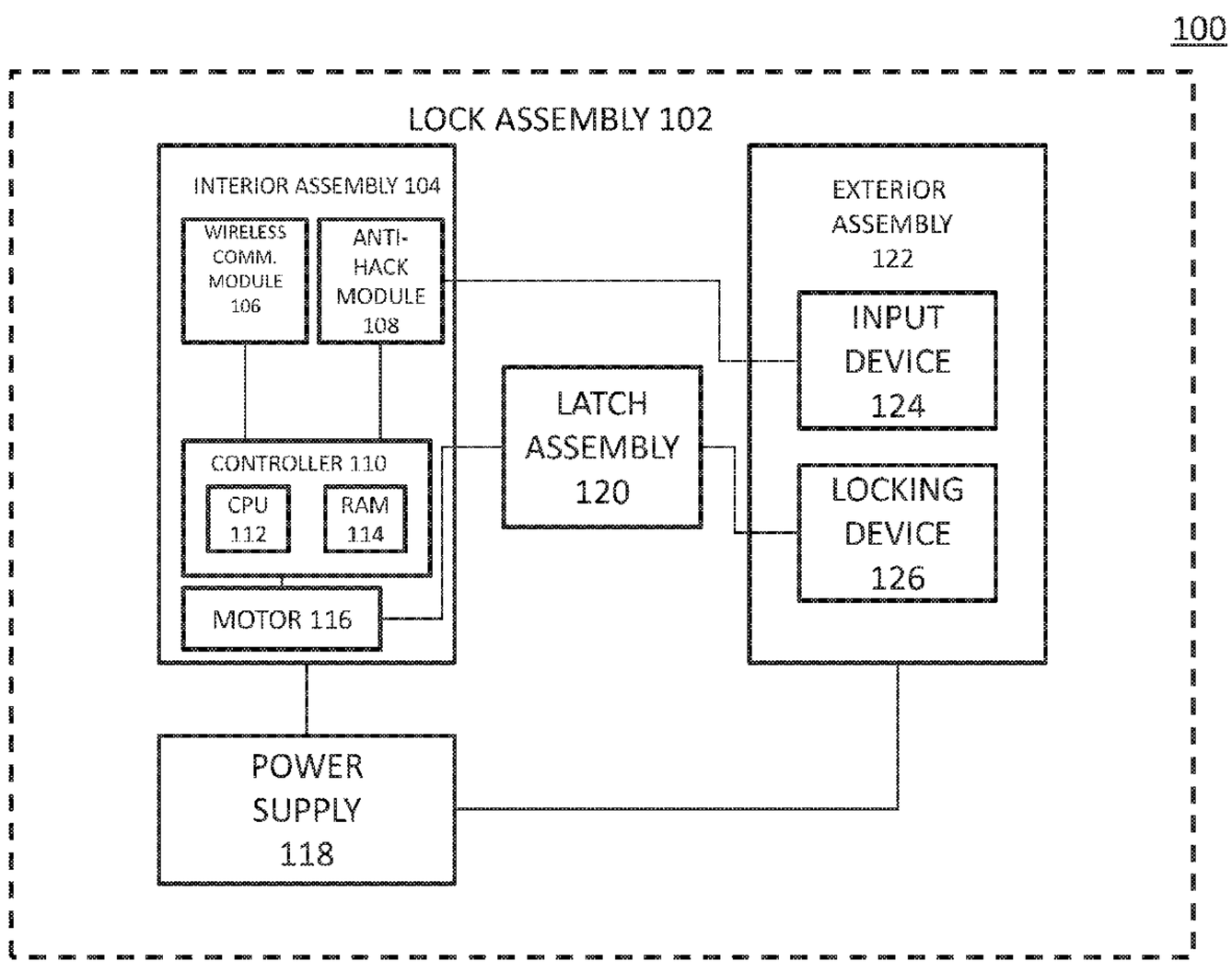

Figure 1

(57) Abstract: A wireless lockset with integrated anti-hacking methods is described herein. The integrated anti-hacking methods in the wireless lockset allows the detection of unauthorized access by one or more individuals. The integrated anti-hacking methods can detect an anomaly regarding wireless command sequence numbers, timing of received commands or flooding attack, and/or unauthorized access based on the MAC address of a command-issuing device. Upon detection of a hacking attempt, the wireless lockset performs one or more actions.

WO 2017/165610 A1

WIRELESS LOCKSET WITH ANTI-HACKING FEATURE

Related Applications

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 62/312,709 filed March 24, 2016, which is hereby incorporated by reference in its entirety.

Technical Field

[0002] This disclosure relates generally to locks; in particular, this disclosure relates to a wireless lock with integrated anti-hacking processes.

Background and Summary

[0003] Security systems are in widespread use in residential and commercial markets. These devices control ingress through doors to secured areas, such as a building or other secured space, by requiring certain authorized credentials. Existing security systems may be subject to different types of hacking which have surfaced during recent years. For example, an unauthorized person may attempt to flood a security system with numerous commands in a short time period. In some cases, an unauthorized person may attempt to confuse the security system by sending commands with high frame numbers to be executed prior to other commands. These, and those attempts are made by unauthorized persons to gain access to the security system. The need for more intelligence in door locksets is necessary to minimize the risk of a hacking attack and certainly to prevent unauthorized access to secured areas.

[0004] According to one aspect, this disclosure provides a wireless lockset with the ability to detect potential hacking attempts. For example, in some embodiments, the lock could detect quantity and timing of specific commands issued to the lock and surrounding wireless access control devices. The lock can detect when an anomaly in the number of

commands that is being sent to it (flooding attack) and also the timing (faster than usual requests) has occurred. In some cases, the lock also is able to identify and track the wireless command sequence numbers and will respond when an anomaly occurs with the sequence number. For example, when a command with an out of order sequence number is received, the lock could detect this anomaly as a potential hacking attempt. Depending on the circumstances, the lock may also be able to track the identity of the access control panel/hub and discern when it is being sent commands from a control panel/hub that is different than that originally assigned. Upon detection of any of these potential hacking anomalies, the lock may take certain actions, including, but not limited to: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and/or automatically lock/unlock.

Brief Description of the Drawings

[0005] The detailed description makes reference to the accompanying figures in which:

[0006] Figure 1 is a simplified block diagram of a lock assembly according to an embodiment of the disclosure;

[0007] Figure 2 is a simplified block diagram of an anti-hacking module according to an embodiment of the disclosure;

[0008] Figure 3 is a side view of an electronic lock in accordance with an embodiment of the present invention, installed on a door and with the door shown in phantom lines;

[0009] Figure 4 is a flow diagram of an exemplary method for detecting an out of sequence command according to an embodiment of the disclosure;

[00010] Figure 5 is a flow diagram of an exemplary method for detecting a flooding attack according to an embodiment of the disclosure; and

[00011] Figure 6 is a flow diagram of an exemplary method for detecting a valid MAC address of a device according to an embodiment of the disclosure.

Detailed Description of the Drawings

[00012] The figures and descriptions provided herein may have been simplified to illustrate aspects that are relevant for a clear understanding of the herein described devices, systems, and methods, while eliminating, for the purpose of clarity, other aspects that may be found in typical devices, systems, and methods. Those of ordinary skill may recognize that other elements and/or operations may be desirable and/or necessary to implement the devices, systems, and methods described herein. Because such elements and operations are well known in the art, and because they do not facilitate a better understanding of the present disclosure, a discussion of such elements and operations may not be provided herein. However, the present disclosure is deemed to inherently include all such elements, variations, and modifications to the described aspects that would be known to those of ordinary skill in the art.

[00013] References in the specification to "one embodiment," "an embodiment," "an illustrative embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may or may not necessarily include that particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly

described. Additionally, it should be appreciated that items included in a list in the form of "at least one A, B, and C" can mean (A); (B); (C); (A and B); (A and C); (B and C); or (A, B, and C). Similarly, items listed in the form of "at least one of A, B, or C" can mean (A); (B); (C); (A and B); (A and C); (B and C); or (A, B, and C).

[00014] In the drawings, some structural or method features may be shown in specific arrangements and/or orderings. However, it should be appreciated that such specific arrangements and/or orderings may not be required. Rather, in some embodiments, such features may be arranged in a different manner and/or order than shown in the illustrative figures. Additionally, the inclusion of a structural or method feature in a particular figure is not meant to imply that such feature is required in all embodiments and, in some embodiments, may not be included or may be combined with other features.

[00015] In some embodiments, this disclosure relates to methods of detecting specific types of hacking attacks that have been developed and integrated into a lockset, such as a wireless lockset. Referring to Figure 1, there is shown an example wireless lock with an anti-hacking feature, which is illustratively shown as an anti-hacking circuit 100. Although the term "circuit" is illustratively used to describe the anti-hacking feature, the disclosed embodiments may be implemented, in some cases, in hardware, firmware, software, or any combination thereof. The disclosed embodiments may also be implemented as instructions carried by or stored on a transitory or non-transitory machine-readable (e.g., computer-readable) storage medium, which may be read and executed by one or more processors. A machine-readable storage medium may be embodied as any storage device, mechanism, or other physical structure for storing or transmitting information in a form readable by a machine (e.g., a volatile or non-volatile memory, a media disc, or other media device).

[00016] In the example shown, the circuit 100 includes a lock assembly 102 that includes an interior assembly 104 and an exterior assembly 122 that are typically mounted on

the inside and outside of a door, respectively. As shown, the circuit 100 includes a power supply 118 for electrically powering the circuit 100, which could be batteries, a solar cell or other power source. In the embodiment shown, the circuit 100 includes a latch assembly 120 that is typically movable between locked and unlocked positions either manually or electronically, such as by a motor 116. The interior assembly 104 may include a wireless communication module 106, an anti-hacking module 108, and a controller. The controller 110 may further include a processing unit ("CPU") 112 and a memory ("RAM") 114. The exterior assembly 122 may include an input device 124, such as a keypad for entering a pin code, and a locking device 126. The controller 110 may include a wireless communication module 106 facilitates wireless communications with a gateway (not shown), a user's mobile device (not shown) or other connected device for alerts, remote commands and/or other messaging with the circuit 100, which could be through any one or more associated wireless communication protocols (e.g., Bluetooth®, Wi-Fi®, WiMAX, Zigbee®, Z-Wave®, etc.).

[00017] The anti-hacking module 108 of the lock assembly 102 may be embodied as hardware, firmware, software, or a combination thereof. As such, in some embodiments, the anti-hacking module may be embodied as circuitry or a collection of electrical devices (e.g., packet inspection circuitry, timing attack detector circuity, flooding attack detector circuitry, etc.). It should be appreciated that, in such embodiments, one or more of the circuitry may form a portion of the processor, memory and/or other electrical components of the locking assembly.

[00018] Referring to Figure 2, there is shown an example block diagram 200 of the anti-hacking module 108 for at least one embodiment of the present disclosure. In the example shown, the anti-hacking module 108 may include a packet inspection engine 204, a flooding attack detector 206, a wireless command counter 208, a timing attack detector 210, and a hacking attack notification engine 212. In some embodiments, the packet inspection

engine 204 inspects packets received by the wireless communication module 106. These packets could be provided to the flooding attack detector 206 to determine whether the packet is part of a flooding attack, which could be based on data regarding a number of commands received by the wireless command counter 208. The packets could also be provided to the timing attack detector 210 to determine whether the packet is part of a timing attack. The timing attack detector 210 may be in further communication with a database 214 to store wireless command time data. If the flooding attack detector 206 and/or the timing attack detector 210 determine that a packet may be part of an attack, a message will be provided to the hacking attack notification engine, which will provide an alert to such attack. Depending on a desired configuration, the series of engines and detectors depicted in the anti-hacking module, which may be realized in a combination of hardware and/or software, may be in communication with one another as illustrated by the appropriate arrows. It is noted that this configuration is merely for exemplary purposes only and may be rearranged as needed.

[00019] Figure 3 shows an exemplary electronic lock 300 in accordance with an embodiment of the present disclosure mounted to a door 302. In the example shown, the electronic lock 300 includes an interior assembly 304 with a battery holder 306, a turnpiece 308, a bolt 310, a strike 312, a user input 314, an exterior assembly 316, a mechanical locking assembly 318, and a key 320. In some cases, the credentials and/or commands may be provided wirelessly to the electronic lock 300, such as disclosed in United States Patent Application Number 2014/0250956 for an "Electronic Deadbolt," filed February 25, 2014, which is hereby incorporated by reference. In another example, the electronic lock may be equipped to receive user credentials via touch activation, such as disclosed in United States Patent Number 9,024,759, which is hereby incorporated by reference.

[00020] Figure 4 is a simplified flowchart showing an example anti-hacking method of a wireless lockset 300 using the anti-hacking module 108 to detect a command with an out of

order frame count. In this example, the method 400 begins with Block 402, in which a counter variable is determined. The counter variable may be a Sequence number. The counter variable may be stored in a typical storage device or a database. With each wireless command received at the lockset, there is a Sequence number associated with each command. This ensures that commands received at a lockset are executed in order. As each command executes, a counter variable may be incremented and prevent commands having a sequence number below the counter variable value from being executed, or, in other words, from being executed out of turn.

[00021] Turning back to Figure 4, after the counter variable is determined, the process moves to step 404 and the wireless lockset receives a command. A decision 406 is then made to detect an anomaly based on the sequence number associated with the received command. If the sequence number is significantly higher than the counter variable by a predetermined amount, the process moves to step 410 and a special action is performed. The special action may include, but is not limited to, timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock action, or the like. In the event that the command sequence number is not deemed to be significantly higher, the process moves to step 408 and normal processing of the command resumes. In this example scenario, the command is executed and the counter variable is incremented. A typical command may be a lock command of the lockset or an unlock command of the lockset. The anomaly detection of Figure 4 is directed towards the detection of out of order frame count. In this example, a hacker may attempt to issue a false command and program the false command to have a very high sequence number.

[00022] Figure 5 is a simplified flowchart showing an example anti-hacking method of a wireless lockset 300 using the anti-hacking module 108 to detect a flooding attack. In this example, the method 500 begins with step 502 to track the time between received commands.

The tracked time variables may be stored in a storage device or a database, for example. In step 504, the average time between commands may be determined and stored as a variable, for example a Delta variable. In decision block 506 an anomaly is determined to be present based on either the quantity of commands received within a certain period of time or the determined average time between commands received, or a combination of both. In one embodiment, recently received commands may include all commands received within the past 30 seconds or 30 minutes, for example. Alternatively, the recently received commands may include a certain amount of commands, such as the last five received commands, for example. If the average time between commands is considered to be a predetermined amount below the regular average time, an anomaly is considered to be detected and the process moves to step 510 and a special action may be performed. The special action may include, but is not limited to, timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock action, or the like. In the event that no anomaly is detected, the process moves to step 508 and the command is executed.

[00023] Figure 6 is a simplified flowchart showing an example anti-hacking method of a wireless lockset 300 using the anti-hacking module 108. In this example, the method 600 begins with receiving a command at the lockset 300 from a user device at step 602. The command includes an identifier of the user device. In one embodiment, the identifier may be a MAC address of the user device. At decision block 604, the lockset 300 determines if the identifier is recognized. For example, the identifier may be compared to a table of trusted or valid identifiers. Continuing with the example above, the table may comprise a list of valid MAC addresses determined to be associated with a trusted user device. In the event that the identifier is recognized and therefore no anomaly is detected, the process moves to step 606 and the command is executed. In the event that the identifier is not recognized and therefore an anomaly is detected, the process moves to step 608 and a special action may be performed.

The special action may include, but is not limited to, timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock action, or the like.

EXAMPLES

[00024] Illustrative examples of the lockset disclosed herein are provided below. An embodiment of the lockset may include any one or more, and any combination of, the examples described below.

[00025] Example 1 is a lockset that includes a latch assembly, a controller, an interior assembly and an exterior assembly. The latch assembly has a bolt movable between an extended position and a retracted position. The controller is configured to electronically control movement of the bolt between the extended position and the retracted position. The interior assembly includes a turn piece for manually actuating the bolt between the extended position and the retracted position. The exterior assembly includes a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position. The controller is configured to determine a command sequence number, receive at least one command, compare the command sequence number with a sequence number associated with the received command to identify an anomaly, execute the command in response to an anomaly not being identified, and perform a special action in response to an anomaly being identified.

[00026] In Example 2, the subject matter of Example 1 is further configured such that the command sequence number is incremented in response to the received command being executed.

[00027] In Example 3, the subject matter of Example 1 is further configured such that the command, when executed, causes the bolt to move into the extended position or the retracted position.

[00028] In Example 4, the subject matter of Example 1 is further configured such that the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

[00029] In Example 5, the subject matter of Example 1 is further configured such that the anomaly is identified when the received command sequence number is significantly greater than the command sequence number.

[00030] In Example 6, the subject matter of Example 1 is further configured such that the anomaly is identified when a difference between the received command sequence number and the command sequence number exceeds a predetermined amount.

[00031] Example 7 is a lockset that includes a latch assembly, a controller, an interior assembly and an exterior assembly. The latch assembly includes a bolt movable between an extended position and a retracted position. The controller is configured to electronically control movement of the bolt between the extended position and the retracted position. The interior assembly includes a turn piece for manually actuating the bolt between the extended position and the retracted position. The exterior assembly includes a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position. The controller is configured to track a series of commands received at the controller, execute at least one of the series of commands in response to determining that an anomaly has not been detected based on a quantity and/or a timing of the series of commands, and perform a special action in response to determining that an anomaly has been detected based on a quantity and/or a timing of the series of commands.

[00032] In Example 8, the subject matter of Example 7 is further configured such that the timing is based on an average time between received commands.

[00033] In Example 9, the subject matter of Example 7 is further configured such that the quantity is based on a certain amount of commands received within a predetermined period of time.

[00034] In Example 10, the subject matter of Example 7 is further configured such that the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

[00035] In Example 11, the subject matter of Example 7 is further configured such that the command, when executed, causes the bolt to move into the extended position or the retracted position.

[00036] Example 12 is a lockset that includes a latch assembly, a controller, an interior assembly and an exterior assembly. The latch assembly includes a bolt movable between an extended position and a retracted position. The controller is configured to electronically control movement of the bolt between the extended position and the retracted position. The interior assembly includes a turn piece for manually actuating the bolt between the extended position and the retracted position. The exterior assembly includes a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position. The controller is further configured to receive at least one command from a device, wherein the at least one command comprises an identifier associated with the device, determine if the identifier is recognized, execute the command in response to the identifier being recognized, and perform a special action in response to the identifier not being recognized.

[00037] In Example 13, the subject matter of Example 12 is further configured such that the identifier is compared to a list of known identifiers to determine if the identifier is recognized.

[00038] In Example 14, the subject matter of Example 12 is further configured such that the identifier is a MAC address.

[00039] In Example 15, the subject matter of Example 12 is further configured such that the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

[00040] In Example 16, the subject matter of Example 12 is further configured such that the command, when executed, causes the bolt to move into the extended position or the retracted position

[00041] Although the present disclosure has been described with reference to particular means, materials and embodiments, from the foregoing description, one skilled in the art can easily ascertain the essential characteristics of the present disclosure and various changes and modifications may be made to adapt the various uses and characteristics without departing from the spirit and scope of the present invention as set forth in the following claims.

WHAT IS CLAIMED IS:

1. A lockset comprising:

a latch assembly including a bolt movable between an extended position and a retracted position;

a controller configured to electronically control movement of the bolt between the extended position and the retracted position;

an interior assembly including a turn piece for manually actuating the bolt between the extended position and the retracted position;

an exterior assembly including a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position;

wherein the controller is further configured to:

determine a command sequence number;

receive at least one command;

compare the command sequence number with a sequence number associated with the received command to identify an anomaly;

execute the command in response to an anomaly not being identified; and

perform a special action in response to an anomaly being identified.

2. The lockset as recited in claim 1, wherein the command sequence number is incremented in response to the received command being executed.

3. The lockset as recited in claim 1, wherein the command, when executed, causes the bolt to move into the extended position or the retracted position.

4. The lockset as recited in claim 1, wherein the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

5. The lockset as recited in claim 1, wherein the anomaly is identified when the received command sequence number is significantly greater than the command sequence number.

6. The lockset as recited in claim 1, wherein the anomaly is identified when a difference between the received command sequence number and the command sequence number exceeds a predetermined amount.

7. A lockset comprising:

a latch assembly including a bolt movable between an extended position and a retracted position;

a controller configured to electronically control movement of the bolt between the extended position and the retracted position;

an interior assembly including a turn piece for manually actuating the bolt between the extended position and the retracted position;

an exterior assembly including a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position;

wherein the controller is further configured to:

track a series of commands received at the controller

execute at least one of the series of commands in response to determining that an anomaly has not been detected based on a quantity and/or a timing of the series of commands; and

perform a special action in response to determining that an anomaly has been detected based on a quantity and/or a timing of the series of commands.

8. The lockset as recited in claim 7, wherein the timing is based on an average time between received commands.

9. The lockset as recited in claim 7, wherein the quantity is based on a certain amount of commands received within a predetermined period of time.

10. The lockset as recited in claim 7, wherein the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

11. The lockset as recited in claim 7, wherein the command, when executed, causes the bolt to move into the extended position or the retracted position.

12. A lockset comprising:

a latch assembly including a bolt movable between an extended position and a retracted position;

a controller configured to electronically control movement of the bolt between the extended position and the retracted position;

an interior assembly including a turn piece for manually actuating the bolt between the extended position and the retracted position;

an exterior assembly including a mechanical lock assembly configured to manually move the bolt between the extended position and the retracted position;

wherein the controller is further configured to:

receive at least one command from a device, wherein the at least one command comprises an identifier associated with the device;

determine if the identifier is recognized;

execute the command in response to the identifier being recognized; and

perform a special action in response to the identifier not being recognized.

13. The lockset as recited in claim 12, wherein the identifier is compared to a list of known identifiers to determine if the identifier is recognized.

14. The lockset as recited in claim 12, wherein the identifier is a MAC address.

15. The lockset as recited in claim 12, wherein the special action includes at least one of: timeouts, keypad disable, wireless disable, notifications, audible alarms, wireless alarms, LED indicators, and an automatic lock/unlock of the lockset.

16. The lockset as recited in claim 12, wherein the command, when executed, causes the bolt to move into the extended position or the retracted position

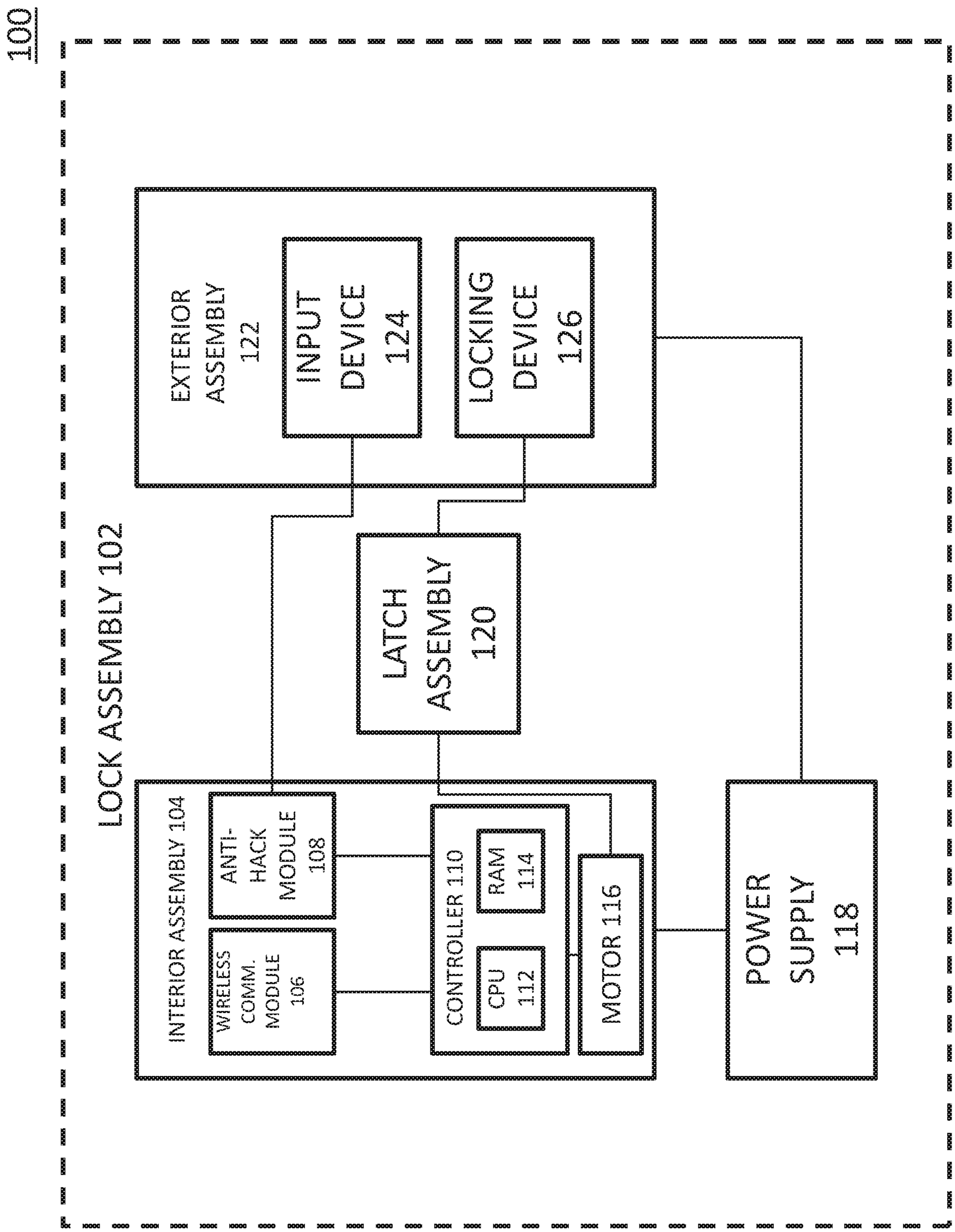
100
LOCK ASSEMBLY 102
EXTERIOR ASSEMBLY 122
INPUT DEVICE 124
LOCKING DEVICE 126
LATCH ASSEMBLY 120
INTERIOR ASSEMBLY 104
WIRELESS COMM. MODULE 106
ANTI-HACK MODULE 108
CONTROLLER 110
CPU 112
RAM 114
MOTOR 116
POWER SUPPLY 118

Figure 1

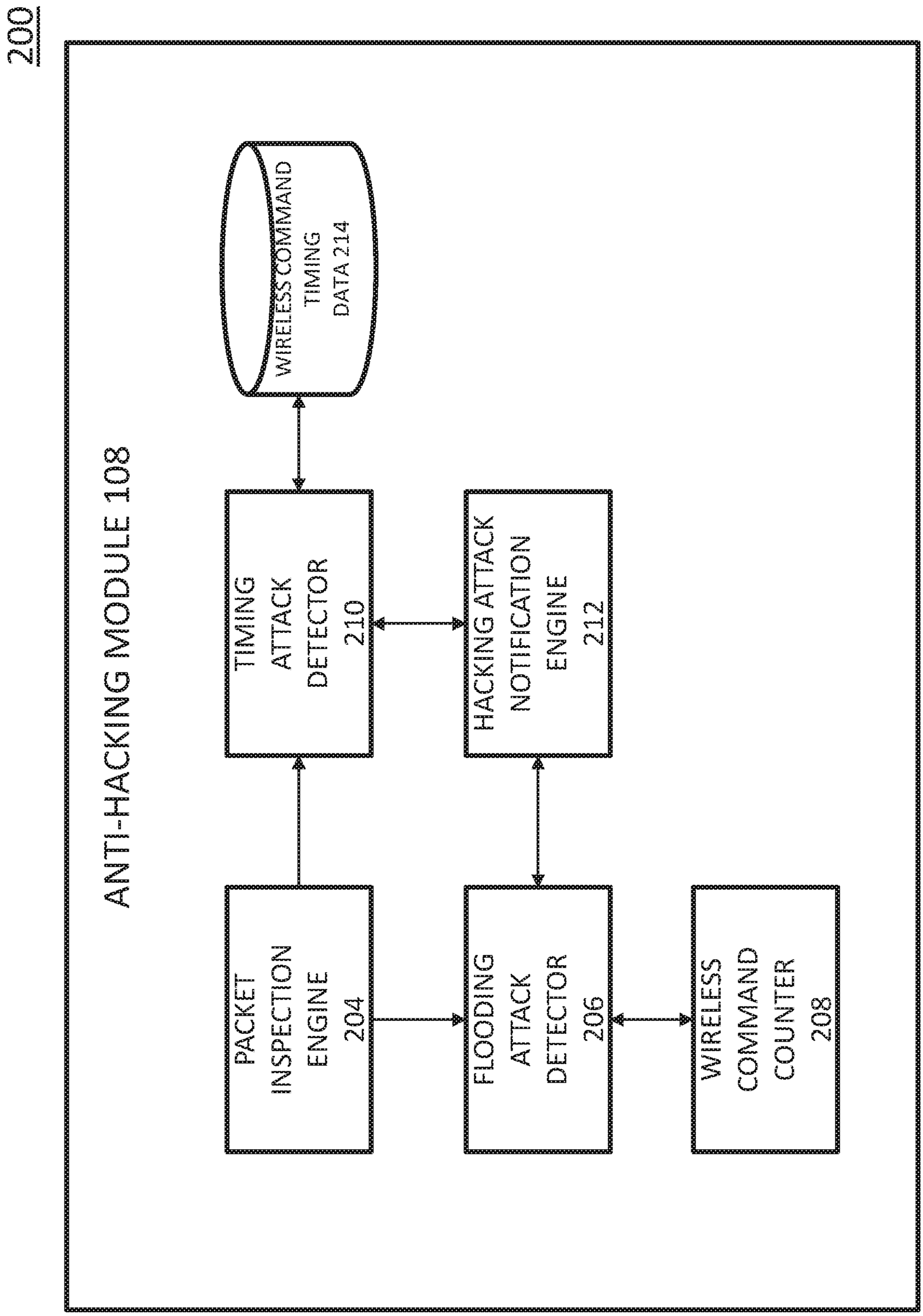
200
ANTI-HACKING MODULE 108
WIRELESS COMMAND TIMING DATA 214
TIMING ATTACK DETECTOR 210
HACKING ATTACK NOTIFICATION ENGINE 212
PACKET INSPECTION ENGINE 204
FLOODING ATTACK DETECTOR 206
WIRELESS COMMAND COUNTER 208

Figure 2

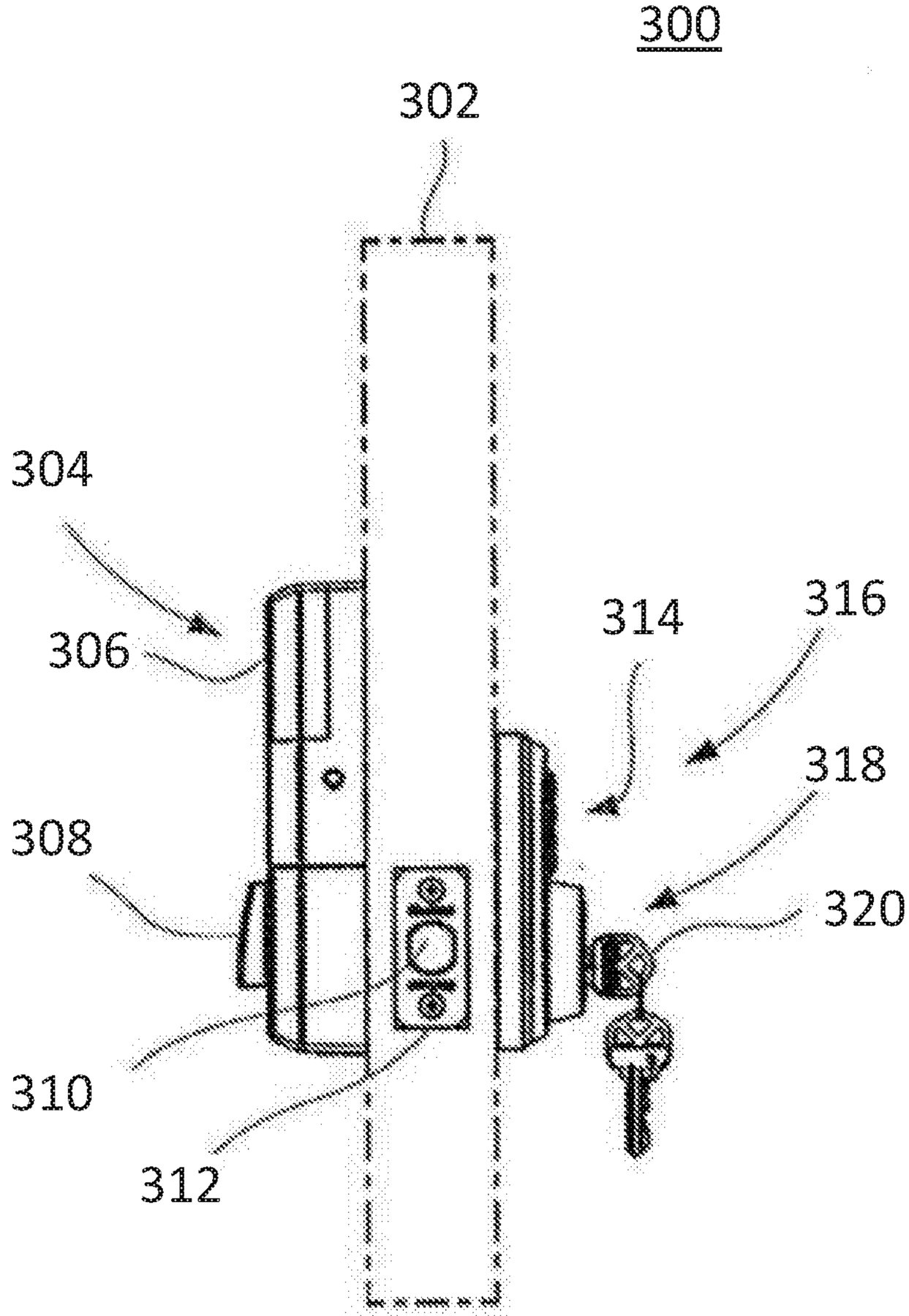

Figure 3

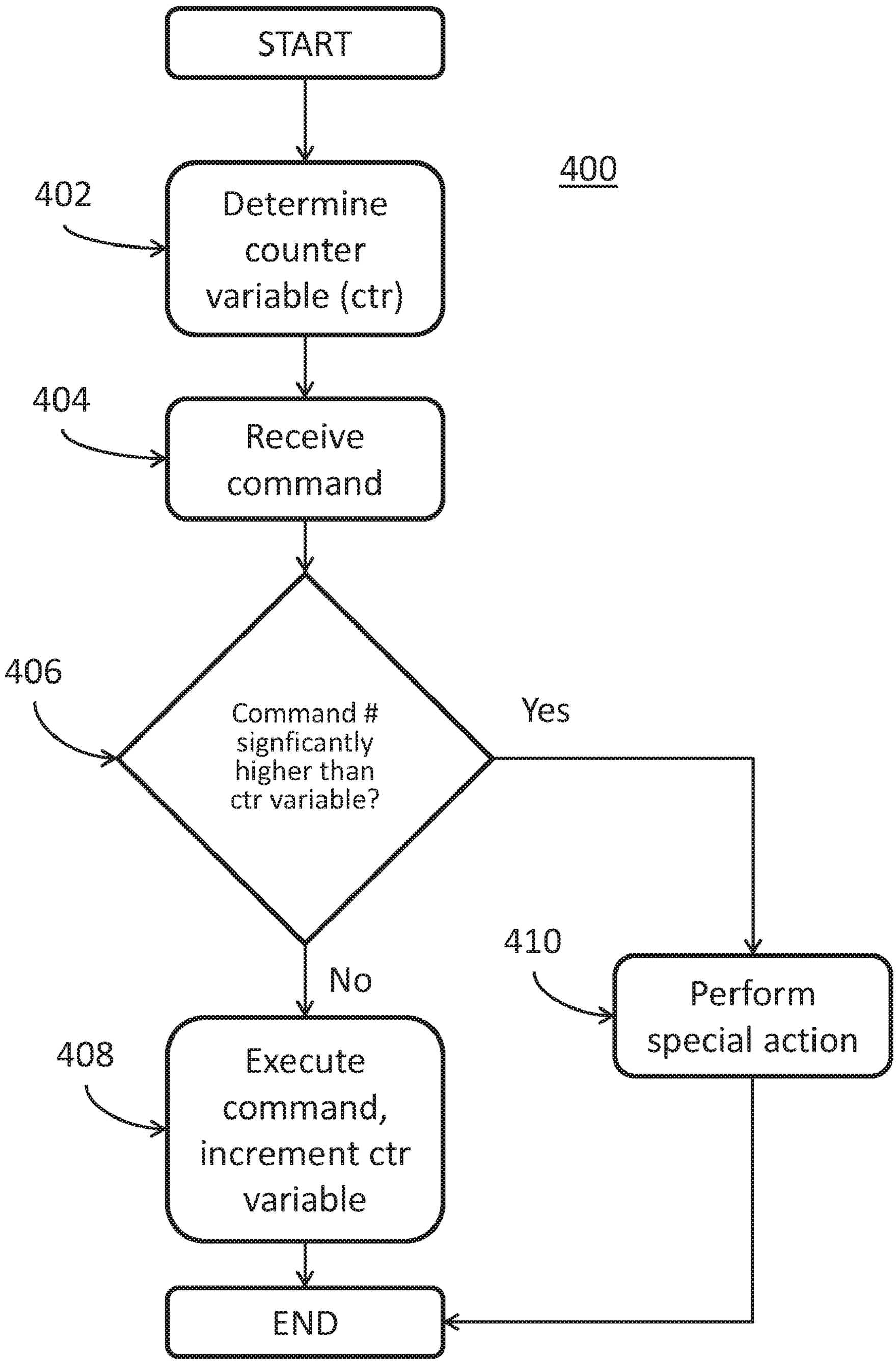
START
400
402
Determine counter variable (ctr)
404
Receive command
406
Command # signficantly higher than ctr variable?
Yes
No
410
Perform special action
408
Execute command, increment ctr variable
END

Figure 4

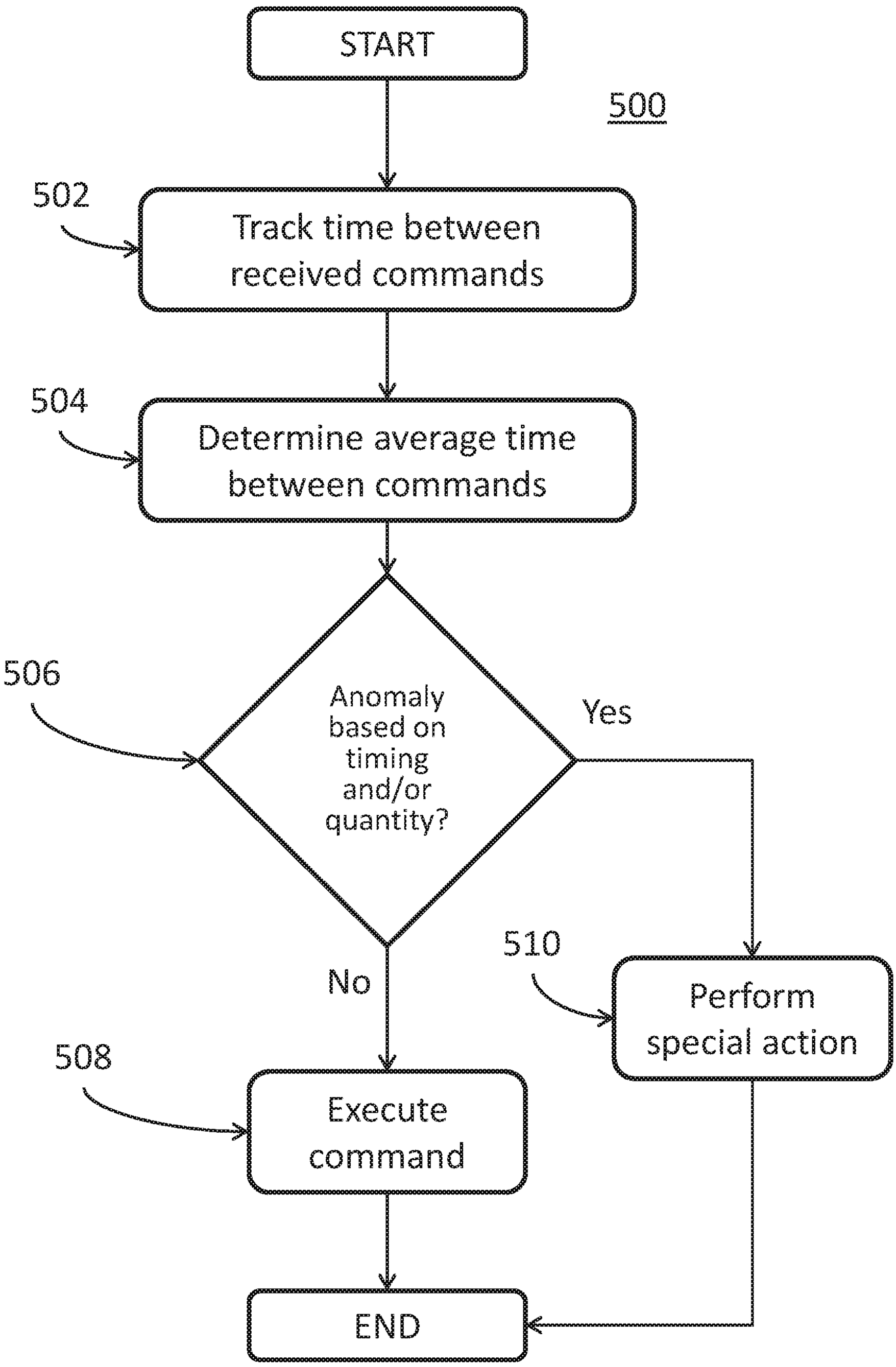
START
500
502
Track time between received commands
504
Determine average time between commands
506
Anomaly based on timing and/or quantity?
Yes
No
510
Perform special action
508
Execute command
END

Figure 5

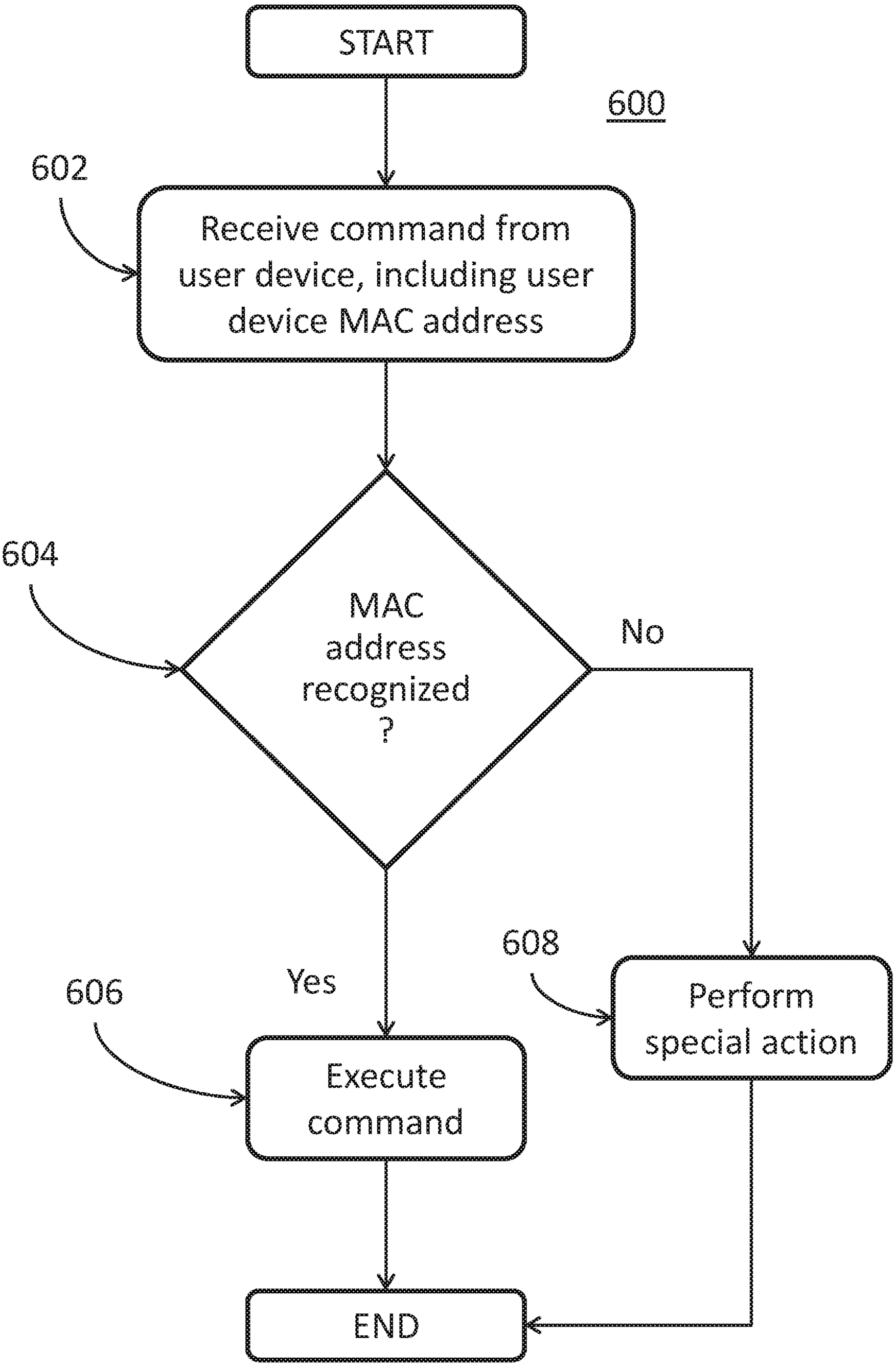
START
600
602
Receive command from user device, including user device MAC address
604
MAC address recognized ?
No
Yes
606
608
Execute command
Perform special action
END

Figure 6

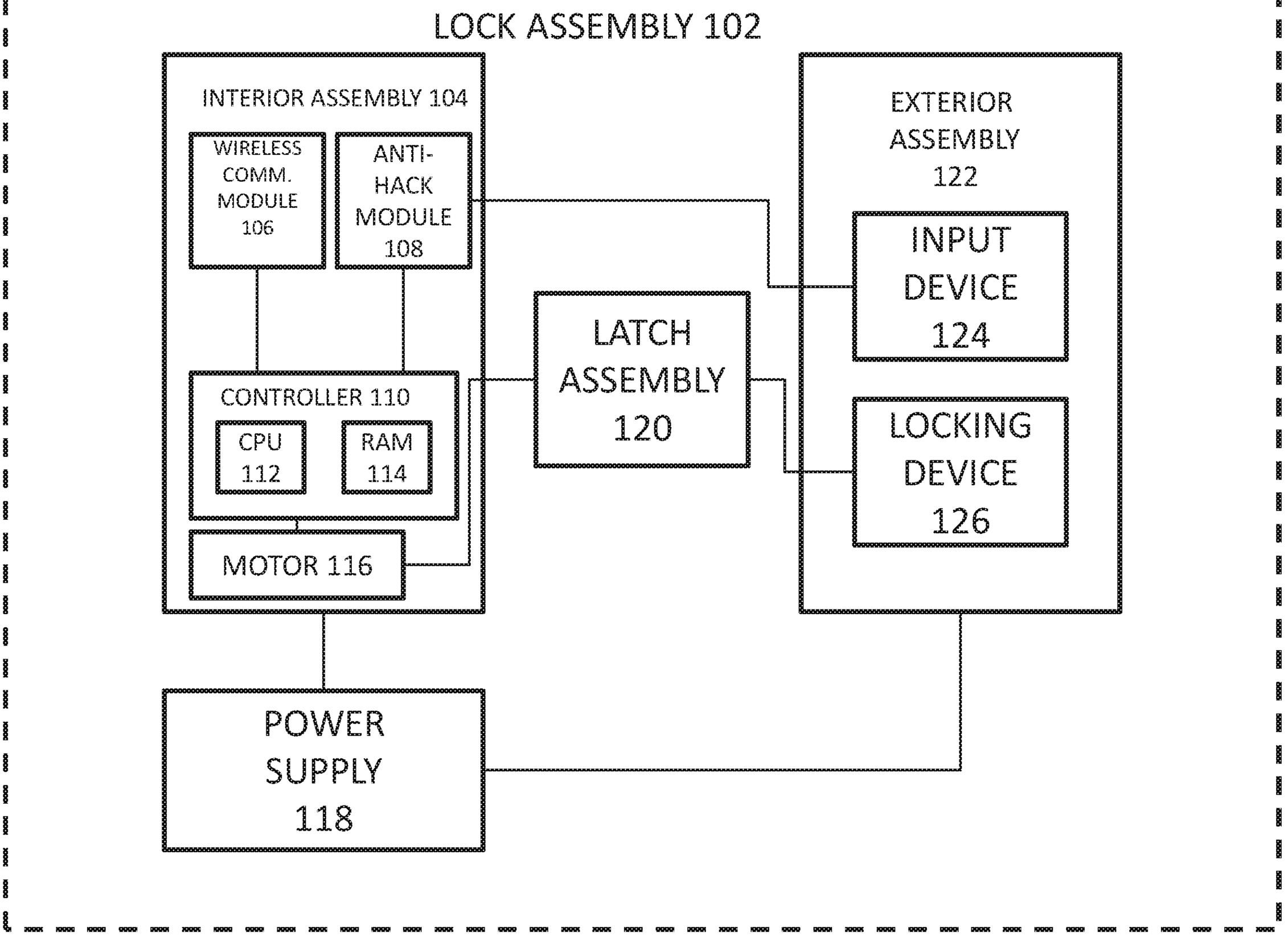
LOCK ASSEMBLY 102
INTERIOR ASSEMBLY 104
WIRELESS COMM. MODULE 106
ANTI-HACK MODULE 108
CONTROLLER 110
CPU 112
RAM 114
MOTOR 116
POWER SUPPLY 118
LATCH ASSEMBLY 120
EXTERIOR ASSEMBLY 122
INPUT DEVICE 124
LOCKING DEVICE 126

Figure 1