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

(11) **EP 3 207 536 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
07.11.2018 Bulletin 2018/45

(21) Application number: **15794605.4**

(22) Date of filing: **05.10.2015**

(51) Int Cl.:
G08B 13/22 *(2006.01)*

(86) International application number:
PCT/GB2015/000281

(87) International publication number:
WO 2016/059359 (21.04.2016 Gazette 2016/16)

(54) **CO-OPERATIVE LOCK SYSTEM**

KOOPERATIVES SCHLOSSSYSTEM

SYSTÈME DE VERROUILLAGE COOPÉRATIF

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

(30) Priority: **14.10.2014 GB 201418139**

(43) Date of publication of application:
23.08.2017 Bulletin 2017/34

(73) Proprietor: **McQuillan, James**
Poole, Dorset BH14 8AB (GB)

(72) Inventor: **McQuillan, James**
Poole, Dorset BH14 8AB (GB)

(74) Representative: **Bailey, Richard Alan**
Bailey IP Consulting Limited
142 Leckhampton Road
Cheltenham, Glos. GL53 0DH (GB)

(56) References cited:
US-A1- 2011 193 678
US-A1- 2014 002 239
US-A1- 2014 109 631

EP 3 207 536 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This invention relates to a lock system.

[0002] US2011/193678 and US2014/002239 both describe lock systems in which individual locks of the system are able to transmit status information to other parts of the lock system.

[0003] According to the present invention there is provided a lock system as defined by appended Claim 1.

[0004] This invention relates, therefore, to a lock fitted with single or multiple tamper and/or shock sensors, transmitters and receivers (Figure 1). It is able to detect an attempt to tamper with the lock, said sensors causing the lock to transmit an alarm which is then received, repeated and sounded by adjacent equivalent locks and located in the same or adjacent groups or clusters.

[0005] The system therefore does not require additional infrastructure to repeat the alarm over a given area, making it more difficult to silence the alarm and creating a stronger deterrent.

[0006] A criminal will usually remove and discard a lock and will silence it if it contains an alarm capability. In many circumstances this provides little deterrent and the lock may be thrown overboard if on a yacht or dropped into a bucket of water or completely smashed to silence the lock alarm.

[0007] The cluster lock is an intelligent lock system that consists of a cluster of alarmed locks of the same type that are able to communicate such an attack event to each other and to provide a wider deterrent than a single physical lock or a simple alarmed lock can offer. This overcomes the issue of a single lock acting alone.

[0008] As each lock transmits an alarm it transmits its own alarm information. The alarm signal or tone in the next lock that is triggered by either an attack or receiving an alarm signal from another lock may be varied according to the proximity of the lock to the originating alarm. The communications techniques may be wireless (shock, vibration, acoustic, radio waves or optical) or wired (using electric or optical conductors), according to the application.

[0009] The system may also employ additional systems to gather alarm and location data and a) to retain that data in a secure repository and/or b) to relay suitable information to a third party for possible action using standard communications channels, web-based systems or modem Android^{RTM}, Apple^{RTM} or other applications ("Apps"). In certain cases it may be desirable for the cluster not to transmit an audible alarm immediately, in order to allow responders sufficient time to apprehend an attacker.

[0010] The device may be any type of lock used to secure one of a group of assets. It contains a sensor to detect an attack, either physical or otherwise, and a transmitter and receiver. When it recognises an attack the lock transmits a signal that other locks can detect. When the lock has completed its transmission to other locks it then transmits a loud acoustic signal that is intended to act as a deterrent to the attacker. The next layer of locks in the community that are within range and can detect the transmission now transmit their own information that may be received by other locks further out in the community. These then also sound an alarm. In this way the alarm works its way out from the core event to provide a wide area alert of the original attack (Figure 2). If the locks in the cluster are set for 'deterrent' and sound the alarm then the resulting noise provides a greater deterrent than a single lock. If they are set to 'catch' then they offer a wider area over which a potential attacker may be detected and apprehended.

[0011] The invention further relates to the detection of this information by another receiver that is able to process the data and to relay this to another system for onwards communication to a nearby office, security station or other facility to support the provision of a response to the event (Figure 3). This invention further relates to the onward
transmission of data using other communications techniques to enable an alarm to be raised remotely from the site of the community. This may be delivered directly to a phone line or through a web-based system or modern Android^{RTM}, Apple^{RTM} or other applications ("Apps").

[0012] The lock architecture is shown in Figure 1. The lock sensor and sensing circuit are permanently listening for abnormally high levels of activity on the mechanism. The sensing circuit is disarmed when the key is used. The key may contain an RFID tag, bar-code or other identifier that can be read by the lock when in close proximity to the key. The sensing circuit may be intelligent, and can be programmed in complex variants to detect attack type for onward transmission. In the simple lock it will merely detect higher amplitude attacks where the key is not used. When an attack is detected this information is passed to the transmitter which uses the techniques for onward transmission built into this particular device. The receiver detects this transmission and, when it is completed, it sounds an alarm or not according to the system settings selected.

[0013] Where an attack on this lock is not detected, the receiver may receive notification from an adjacent lock that it has been attacked. In this case the receiver determines whether the attack was on the immediately adjacent lock, or if this is number two or three or more in the chain from the attacked lock. This determines the transmission type and, if selected, the audio tone is sounded by this alarm using its built-in speaker.

[0014] Users may select the pattern and frequency of the alarm audible output to allow them to work together over wider areas to create groups or clusters of alarms. In this way the users can ensure that there is no confusion over which alarm is the initiating alarm and which are the supporting alarms.

[0015] The lock can include a Global Navigation Satellite System (GNSS) receiver to enable the transmitter to report its position. The GNSS receiver may be embedded in one or all of the locks, or the lock system may

employ another available location source to feed into the lock system (e.g. the National Marine Electronics Association (NMEA) standard output on a yacht Global Positioning System (GPS) or other GNSS solution-based chart plotter).

[0016] An outline of how the cluster system works is shown in Figure 2. A lock is attacked (the initiating alarm) and emits Tone 1, as set by the user group. This is detected by the next layer within range, the receiver determines that this is Tone 1 and selects the next tone in the range, Tone 2. This continues out to the limit of tone options in the product pack chosen by the users. In this way, even if the first lock that is attacked is thrown into deep water, the other locks will have detected it and begin sounding their own alarms. Therefore it becomes increasingly difficult to silence or to ignore the alarm set as a waterfall alarm effect is triggered.

[0017] Figure 2 illustrates the Cluster Lock System.

[0018] The use of Tones offers a method of determining where the alarm originates. For example, if the tones chosen are ascending through the Tone options (e.g. Tone 1 may be 500Hz, Tone 2 may be 1kHz and so on) then moving to the lowest audible tone will guide security staff to the source of the alarm.

[0019] Where an alarm has joined the alarming session triggered by the initiating alarm, and then is itself attacked, it will revert to sounding Tone 1. Adjacent alarms that are higher in the order than Tone 2 will carry on transmitting their tone, but those nearest to the new Tone 1 will begin sounding Tone 2 and so on, until the alarm set levels across the two clusters now alarming. This will be the same for any number of clusters within the overall community.

[0020] In more sophisticated systems the alarm may be propagated by wireless, optical or other means in addition to or instead of the acoustic option in the standard community.

[0021] The next claim connects the community to the remote user via a local or wide area network (Figure 3). A monitor listens for alarm activity and, when this is detected, packages that information and relays it to the user group, either over a dedicated local network or across the public wide area network. This includes the use of web servers and modern communications devices such as 'tablets' and 'smart-phones' to deliver applications to the User. Examples include Android^{RTM} and Apple^{RTM} formats and applications.

[0022] A Lock Identity feature may be provided in some locks to facilitate identification of the initiating lock. If the initiating identification feature is used in each alarm this allows specific users to be targeted with personal messages to inform them that their lock is under attack.

[0023] In order to achieve this functionality the lock may contain some or all of the following functions although other functions may be added for more complex systems:

1. Lock mechanism
2. Lock Housing
3. Lock Sensor set
4. Sensing Circuit
5. Transmitter
6. Receiver
7. Processing Block
8. Power
9. Identity Block
10. Acoustic sounder

[0024] The lock is intended to be deployed singly, as part of a community or as a networked locking system. This community might be, for example, on a single yacht or across a row of yachts on moorings.

[0025] Finally, the community concept may be applied to other requirements. For example, personal attack alarms, vehicle alarms, building intruder alarms and so on may be connected in the same way. In this case the system may be joined to the end user or lock owner in a number of ways. This includes the network interface to port data into the network for a single or multiple locks and alarms. It also includes the application that is required at the user or lock owner site to receive and display relevant information and this will be in the form of an application (on a smart-phone or tablet) or a web service or a bespoke display.

Claims

1. A lock system comprising a first lock having a sensor (3, 4) to detect a tamper attempt on the first lock, said sensor (3, 4) triggering a sounder (10) to output a first audible alarm, a transmitter (5) for transmitting an alarm signal from the first lock to a second, nearby equivalent lock, and a receiver (6) for receiving an alarm signal from a nearby, equivalent lock, the second lock having a transmitter (5) for transmitting an alarm signal to a nearby, equivalent lock and a receiver (6) for receiving the alarm signal from the first lock, **characterised in that** the second lock is operable such that a sounder (10) thereof is triggered to output a second audible alarm upon the reception of the alarm signal from the first lock, the sounder (10) being triggered to output a different alarm signal according to whether the alarm is triggered from the sensor (3, 4) on the lock or due to reception of an alarm signal from another lock.

2. A lock system according to claim 1 wherein the first lock provides an output signal to relay the alarm status across a network to the lock owner and/or security or other staff.

3. A lock system as defined in claim 2 and further comprising a tablet or smart phone application to notify specific lock owners and/or security or other staff.

Patentansprüche

1. Schlosssystem umfassend ein erstes Schloss mit einem Sensor (3, 4) zum Detektieren eines Manipulationsversuchs an dem ersten Schloss, wobei der Sensor (3, 4) einen Schallgeber (10) auslöst zum Ausgeben eines ersten hörbaren Alarms, einem Sender (5) zum Übertragen eines Alarmsignals von dem ersten Schloss zu einem zweiten, nahegelegenen äquivalenten Schloss, und einem Empfänger (6) zum Empfangen eines Alarmsignals von einem nahegelegenen äquivalenten Schloss, wobei das zweite Schloss einen Sender (5) besitzt zum Übertragen eines Alarmsignals zu einem nahegelegenen, äquivalenten Schloss und einen Empfänger (6) zum Empfangen des Alarmsignals von dem ersten Schloss, **dadurch gekennzeichnet, dass** das zweite Schloss derart betätigt werden kann, dass ein Schallgeber (10) davon ausgelöst wird zum Ausgeben eines zweiten hörbaren Alarms bei Empfang des Alarmsignals von dem ersten Schloss, wobei der Schallgeber (10) ausgelöst wird zum Ausgeben eines anderen Alarmsignals gemäß dem, ob der Alarm von dem Sensor (3, 4) an dem Schloss oder aufgrund eines Empfangs eines Alarmsignals von einem anderen Schloss ausgelöst wird.

2. Schlosssystem nach Anspruch 1, wobei das erste Schloss ein Ausgangssignal zum Übertragen des Alarmstatus über ein Netzwerk zu dem Schlossbesitzer und/oder Sicherheitsdienst oder anderem Personal liefert.

3. Schlosssystem nach Anspruch 2 und weiterhin umfassend eine Tablet- oder eine Smartphone-Applikation, um spezifische Schlossbesitzer und/oder Sicherheitsdienst oder anderes Personal zu benachrichtigen.

Revendications

1. Système de verrouillage comportant un premier verrou doté d'un capteur (3, 4) pour détecter une tentative d'effraction sur le premier verrou, ledit capteur (3, 4) déclenchant un bruiteur (10) pour délivrer une première alarme audible, un émetteur (5) servant à envoyer un signal d'alarme du premier verrou à un deuxième verrou équivalent voisin, et un récepteur (6) servant à recevoir un signal d'alarme provenant d'un verrou équivalent voisin, le deuxième verrou étant doté d'un émetteur (5) servant à envoyer un signal d'alarme à un verrou équivalent voisin et d'un récepteur (6) servant à recevoir le signal d'alarme provenant du premier verrou, **caractérisé en ce que** le deuxième verrou peut être utilisé de telle façon qu'un bruiteur (10) de celui-ci soit déclenché pour délivrer une deuxième alarme audible suite à la réception du signal d'alarme provenant du premier verrou, le bruiteur (10) étant déclenché pour délivrer un signal d'alarme différent suivant que l'alarme est déclenchée à partir du capteur (3, 4) sur le verrou ou du fait de la réception d'un signal d'alarme provenant d'un autre verrou.

2. Système de verrouillage selon la revendication 1, le premier verrou fournissant un signal de sortie pour relayer l'état d'alarme à travers un réseau au propriétaire du verrou et/ou à des agents de sécurité ou un autre personnel.

3. Système de verrouillage selon la revendication 2 et comportant en outre une application de tablette ou d'ordiphone pour une notification à des propriétaires de verrous spécifiques et/ou à des agents de sécurité ou un autre personnel.

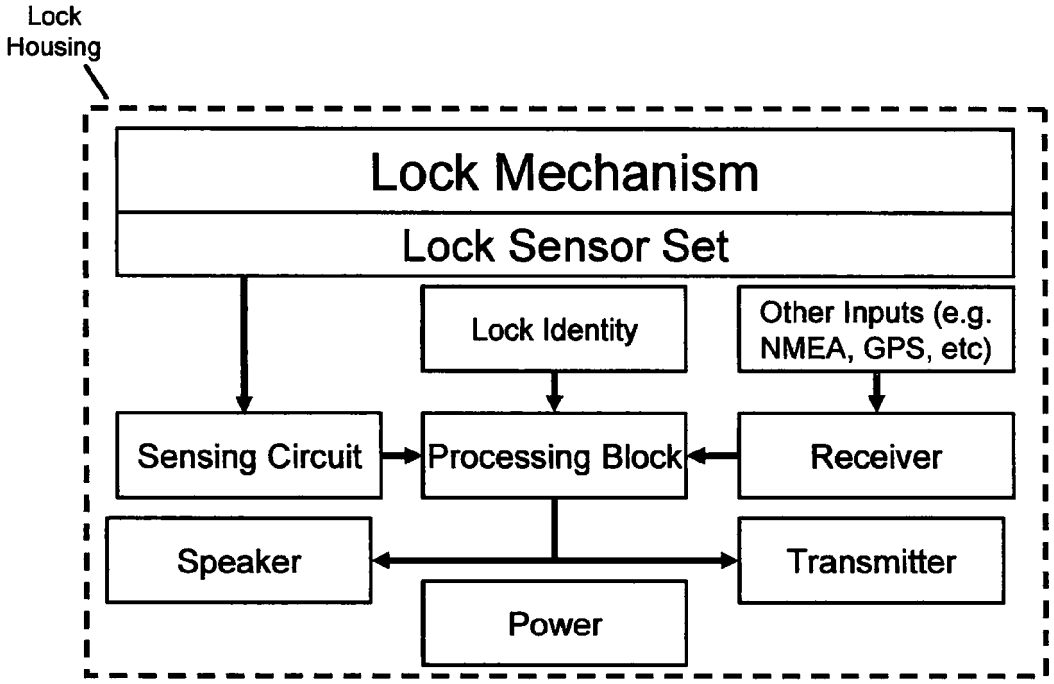

Figure 1: Lock Architecture

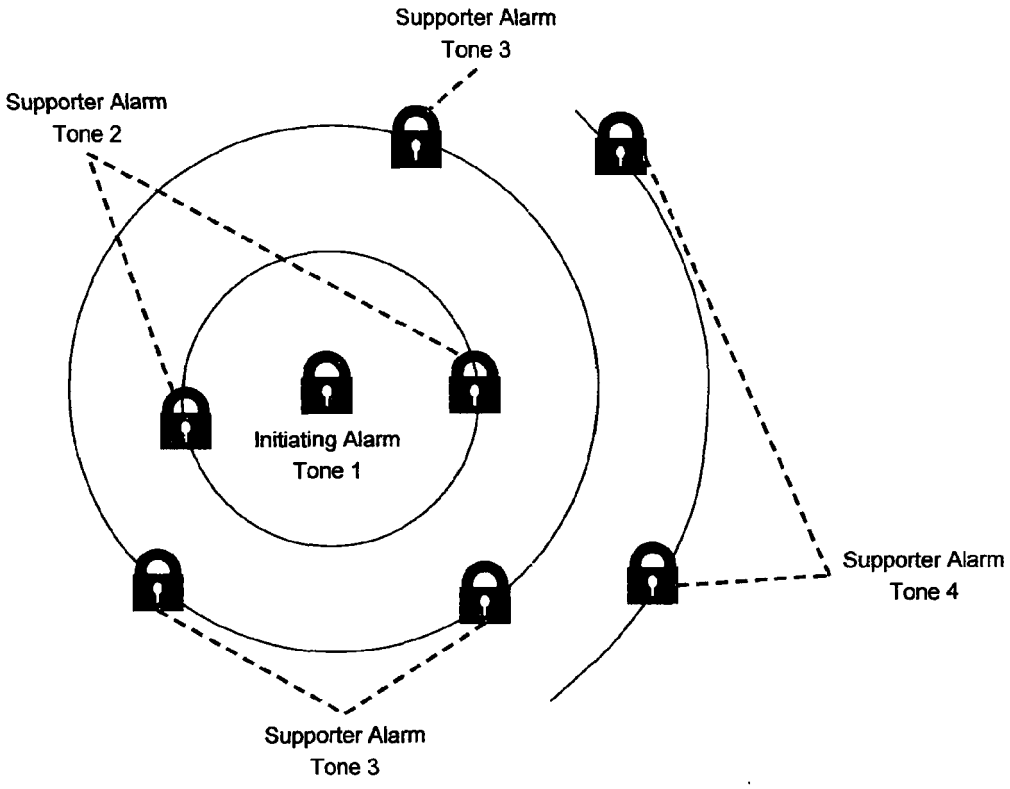

Figure 2: Cluster Lock System

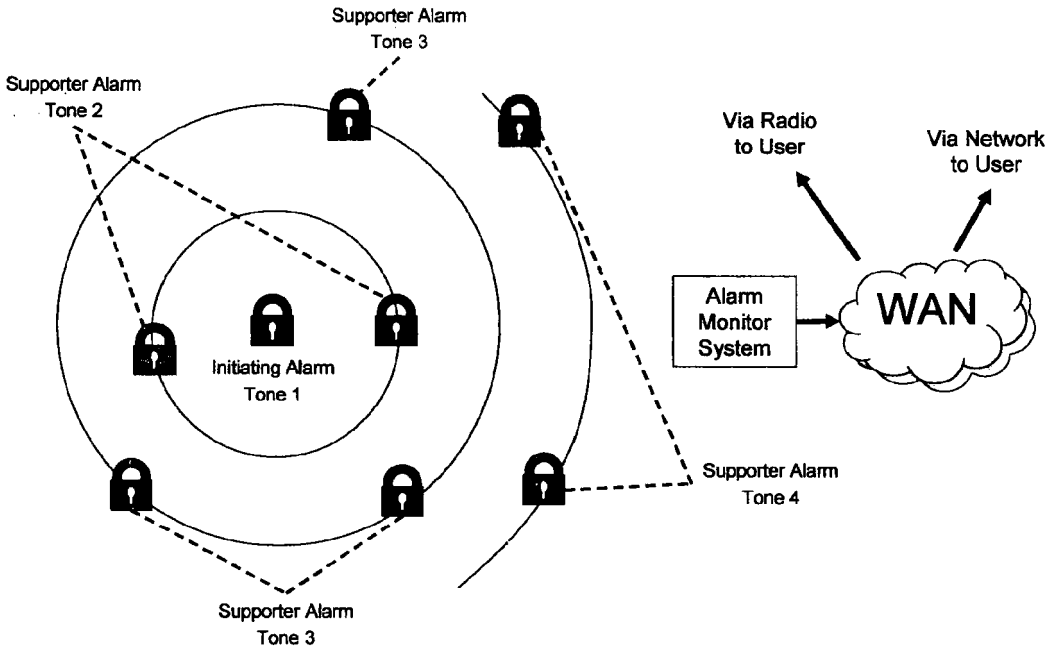

Figure 3: Off-Site Alarms

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2011193678 A **[0002]**
- US 2014002239 A **[0002]**