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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 October 2020 (22.10.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/210990 A1

(51) International Patent Classification:
H04W 4/80 (2018.01) *B60R 25/10* (2013.01)

(21) International Application Number:
PCT/CN2019/082911

(22) International Filing Date:
16 April 2019 (16.04.2019)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors: **REVADIGAR, Girish, Shivalingappa**; 11 North Buona Vista Drive #17-08, The Metropolis Tower 2, 138589 (SG). **WEI, Zhuo**; 11 North Buona Vista Drive #17-08, The Metropolis Tower 2, 138589 (SG). **LI, Tieyan**; 11 North Buona Vista Drive #17-08, The Metropolis Tower 2, 138589 (SG). **YANG, Yanjiang**; 11 North Buona Vista Drive #17-08, The Metropolis Tower 2, 138589 (SG). **YU, Hai**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(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, JO, 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,

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A CONNECTION BETWEEN A USER DEVICE AND A VEHICLE USING BLUETOOTH LOW ENERGY TECHNOLOGY

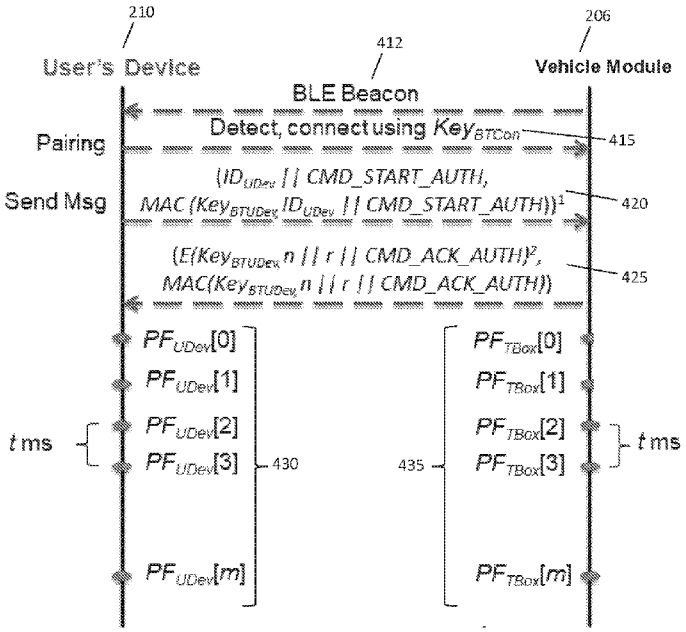

FIGURE 4

(57) Abstract: This document describes a system and method for authenticating a Bluetooth connection between a user device and a vehicle using Bluetooth Low Energy (BLE) technology. In particular, the invention utilizes the physical layer features of the BLE channel between the user device and the vehicle to authenticate the Bluetooth connection between the user device and the vehicle.

WO 2020/210990 A1

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

SYSTEM AND METHOD FOR AUTHENTICATING A CONNECTION BETWEEN A USER DEVICE AND A VEHICLE USING BLUETOOTH LOW ENERGY TECHNOLOGY

Field of the Invention

This invention relates to a system and method for authenticating a Bluetooth connection between a user device and a vehicle using Bluetooth Low Energy (BLE) technology. In particular, the invention utilizes the physical layer features of the BLE channel between the user device and the vehicle to authenticate the Bluetooth connection between the user device and the vehicle.

Summary of the Prior Art

Due to a convergence of technologies, an ever increasing number of devices are now able to seamlessly communicate wirelessly with the Internet or wirelessly exchange communications between themselves. As a result of this convergence, keyless entry systems for vehicles/automobiles are becoming more and more popular due to their ease of use, e.g. the physical car key may no longer be required and a mobile device may be configured to perform the function of the physical car key. This also allows multiple users to be authorized by the car's owner to use his/her car. These systems typically utilize a digital key that is loaded into or stored within the user's personal device e.g. a mobile phone, whereby this digital key is provided to the user by a trusted entity. This is usually done when the vehicle is delivered to the use and typically, Bluetooth Low Energy (BLE) technology will be used to allow the car and the user's device to communicate with each other. Such architecture is illustrated by system 100 in Figure 1 whereby vehicle 105 is in wireless communication with users 102, 104, 106 and the digital key to gain access to vehicle 105 has been provided to these users.

Existing keyless entry systems (KES) are vulnerable to cybersecurity attacks such as relay attacks. Some of the existing solutions use distance estimation methods to calculate the distance between the mobile device and the car (Vehicle Module) using the transmitted/received signal's features. In such solutions, the car will only accept commands from the device if the device is found to be within range of the car.

The existing KES solutions facilitate the unlocking and starting of the car when the physical key is in the pockets of the users. The digital key approach exemplifies another KES solution whereby the user's personal device e.g., mobile phone, will be loaded with an authorized 'digital key', and through the use of Bluetooth technology, the phone would then

be able to unlock and start the car through this wireless communication technology. In both the scenarios described above, the physical key or the phone will transmit commands to the car when it is within range of the car. In order to detect whether the key or phone is within proximity of the car, existing solutions will then measure the wireless signal strength between the car and the key/phone. In other words, if a strong signal is measured this indicates that the communicating devices (car and key/user's device) are near to each other (in range). Thus, the car will then be configured to accept the commands sent by nearby user devices/key whose signal strength are above a certain threshold.

Many existing KES solutions suffer from active attacks such as replay and relay attacks. In relay attacks, an attacker will relay the command messages between the car and key/user's device even if they are far away or outside the range of the car or key/user device. When a key or user's device is under attack, the attacker's device will communicate with the real key/user's device and the attacker will impersonate the car, meaning, the attacker's device will spoof the commands/messages sent by the car for finding the key in its range. When the real key/user's device receives to this spoofed message that is sent by attacker's device, the real key/user's device will respond to the message as it would assume that the message is from the user's legitimate/own car. The attacker then captures/records the signal transmitted from the actual key/user's device, and proceeds to amplifies and transmits this relayed signal to the car. Upon receiving the messages sent by the attacker's device, the car will mistakenly interpret these commands as commands sent by the original key/user's device. Thus, the attacker can easily unlock and steal the car. Similarly, the attacker can also record and replay the messages between car and key/user's device to unlock and steal the car. These are some of the more serious threats faced by KES, and thus, it is important to ensure that wireless communications between the device and the car are highly secure.

For the above reasons, those skilled in the art are constantly striving to come up with a system and method for authenticating data transmission between a vehicle and the vehicle owner's mobile device with the objective of establishing a secure communications channel.

Summary of the Invention

The above and other problems are solved and an advance in the art is made by systems and methods provided by embodiments in accordance with the invention.

A first advantage of embodiments of systems and methods in accordance with the invention is that the system provides robust mutual authentication between a user's vehicle

and the user's personal device, when the user is approaching the car, and also when the user is already near the car.

A second advantage of embodiments of systems and methods in accordance with the invention is that the system is able to detect and mitigate active attacks and man-in-the-middle type attacks during the authentication process thereby preventing vehicle theft from occurring and preventing the compromise of the vehicle's critical components.

A third advantage of embodiments of systems and methods in accordance with the invention is that the system can be easily integrated into any device or module that is Bluetooth Low Energy (BLE) enabled.

The above advantages are provided by embodiments of a system in accordance with the invention operating in the following manner.

According to a first aspect of the invention, a vehicle authenticating system is disclosed, the system comprising: a user device that is configured to: generate an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and a vehicle module; communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device further configured to: validate the acknowledgement instruction using the BUD Key K_{BTUDev}; record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the first aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises: the user device being configured to: filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver}, wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev}; generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk}, wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev}; communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to: validate the verification and authentication check instructions using the BUD Key K_{BTUDev}; extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and communicate the approval instruction to the user device; the user device further configured to: validate the approval instruction using the BUD Key K_{BTUDev}; and authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

With reference to the first aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the first aspect of the invention, before the initiation instruction is generated by the user device, the user device is configured to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a second aspect of the invention, a vehicle authenticating system is disclosed, the system comprising: a user device that is configured to: encrypt an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh}; hash the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message; communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device further configured to: verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted

acknowledgement message is verified; record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the second aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the user device being configured to: filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command; hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message; encrypt an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command; hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message; communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to: verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified; extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted authentication

check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified; encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command; hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; communicate the approval instruction to the user device; the user device further configured to: verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and authenticate the vehicle module based on the approval command in the decrypted approval message.

With reference to the second aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the second aspect of the invention, before the initiation instruction is encrypted by the user device, the user device is configured to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a third aspect of the invention, a user device for authenticating communications with a vehicle module, the user device comprising: a processor; and a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to: generate an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and the vehicle module; communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: retrieve a corresponding BUD Key K_{BTUDev},

from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device further comprising instructions for directing the processor to: validate the acknowledgement instruction using the BUD Key K_{BTUDev}; record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the third aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises: the user device comprising instructions for directing the processor to: filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver}, wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev}; generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk}, wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev}; communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module configured to: validate the verification and authentication check instructions using the BUD Key K_{BTUDev}; extract the Correction Data *C* from the decrypted verification message, and filter the extracted

Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and communicate the approval instruction to the user device; the user device further comprising instructions for directing the processor to: validate the approval instruction using the BUD Key K_{BTUDev}; and authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

With reference to the third aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the third aspect of the invention, before the initiation instruction is generated by the user device, the user device comprises instructions for directing the processor to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a fourth aspect of the invention, a user device for authenticating communications with a vehicle module is disclosed, the user device comprising: a processor; and a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to: encrypt an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh}; hash the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an initiation instruction based on

the encrypted initiation message and the signed-hashed-encrypted initiation message; communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device further comprising instructions for directing the processor to: verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified; record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the fourth aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises: the user device comprising instructions for directing the processor to filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command; hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message; encrypt an authentication check message,

m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command; hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message; communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module comprising instructions for directing the processor to: verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified; extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified; encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command; hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; communicate the approval instruction to the user device; the user device further comprising instructions for directing the processor to: verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and authenticate the vehicle module based on the approval command in the decrypted approval message.

With reference to the fourth aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the fourth aspect of the invention, before the initiation instruction is encrypted by the user device, the user device comprises instructions for directing the processor to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a fifth aspect of the invention, a vehicle module for authenticating communications with a user device is disclosed, the vehicle module comprising: a processor; and a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to: receive an initiation instruction from the user device, wherein the initiation instruction is generated based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, whereby the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and the vehicle module; retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; communicate the acknowledgement instruction to the user device such that upon receiving the acknowledgement instruction, the user device configured to: validate the acknowledgement instruction using the BUD Key K_{BTUDev}; record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the fifth aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises: the user device comprising instructions for directing the processor to: filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver}, wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev}; generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk}, wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev}; communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module comprises instructions for directing the processor to: validate the verification and authentication check instructions using the BUD Key K_{BTUDev}; extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and communicate the approval instruction to the user device; the user device further comprising instructions for directing the processor to: validate the approval instruction using the BUD Key K_{BTUDev}; and authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

With reference to the fifth aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the fifth aspect of the invention, before the initiation instruction is generated by the user device, the user device comprises instructions for directing the processor to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a sixth aspect of the invention, a vehicle module for authenticating communications with a user device is disclosed, the vehicle module comprising: a processor; and a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to: receive an initiation instruction from the user device, wherein the initiation instruction is generated based on an encrypted initiation message and a signed-hashed-encrypted initiation message, the initiation message, m_o, which comprises an identity of the user device ID_{UDev} and an initiation command, is encrypted using a Public Key Infrastructure (PKI)-Public Key associated with the vehicle module, Key_{Pub_Veh}, and the encrypted initiation message is hashed using a Bluetooth User Device (BUD) Key K_{BTUDev}, and signed using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; communicate the acknowledgement instruction to the user device such that upon receiving the acknowledgement instruction, the user device configured to: verify the signed-hashed-encrypted acknowledgement message in the

acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified; record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the sixth aspect of the invention, the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises: the user device comprising instructions for directing the processor to filter the set of physical layer features PF_{UDev} using a low pass filter; generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command; hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message; encrypt an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command; hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message; communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module comprising instructions for directing the processor to: verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified; extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy

Extractor mechanism; verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified; encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command; hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; communicate the approval instruction to the user device; the user device further comprising instructions for directing the processor to: verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and authenticate the vehicle module based on the approval command in the decrypted approval message.

With reference to the sixth aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the sixth aspect of the invention, before the initiation instruction is encrypted by the user device, the user device comprises instructions for directing the processor to: establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to a seventh aspect of the invention, a method for authenticating a Bluetooth connection between a user device and a vehicle module is disclosed, the method comprising: generating an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user

device and a vehicle module; communicating the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key K_{BTUDev}, and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the method further comprising: validating, using the user device, the acknowledgement instruction using the BUD Key K_{BTUDev}; recording a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticating the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the seventh aspect of the invention, the validating of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the steps of: filtering, using the user device, the set of physical layer features PF_{UDev} using a low pass filter; generating a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; generating a verification instruction based on an encrypted verification message and a verification MAC M_{Ver}, wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev}; generating an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk}, wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev}; communicating the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

validate the verification and authentication check instructions using the BUD Key K_{BTUDev}; extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and communicate the approval instruction to the user device; the method further comprising: validating, using the user device, the approval instruction using the BUD Key K_{BTUDev}; and authenticating the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

With reference to the seventh aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the seventh aspect of the invention, before the initiation instruction is generated by the user device, the method comprises the step of: establishing a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

According to an eigth aspect of the invention, a method for authenticating a Bluetooth connection between a user device and a vehicle module, the method comprising: encrypting an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh}; hashing the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generating an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message;

communicating the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to: verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; communicate the acknowledgement instruction to the user device; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the method further comprising the steps of: verifying, using the user device, the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypting the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified; recording a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticating the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

With reference to the eigth aspect of the invention, the validating of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the steps of: filtering, using the user device, the set of physical layer features PF_{UDev} using a low pass filter; generating a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism; encrypting a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command; hashing the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generating a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message; encrypting an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an

XOR operation between the random string *r* and the user string S_{UDev}, and an authentication check command; hashing the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generating an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message; communicating the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to: verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified; extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated; generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism; verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified; encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command; hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; communicate the approval instruction to the user device; the method further comprising the steps of: verifying the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypting the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and authenticating the vehicle module based on the approval command in the decrypted approval message.

With reference to the eigth aspect of the invention, the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

With reference to the eigth aspect of the invention, before the initiation instruction is encrypted by the user device, the method comprises the steps of: establishing a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

Brief Description of the Drawings

The above advantages and features in accordance with this invention are described in the following detailed description and are shown in the following drawings:

Figure 1 illustrating a block diagram representative of an existing keyless entry system for vehicles;

Figure 2 illustrating a block diagram representative of a keyless entry system for vehicles in accordance with embodiments of the invention;

Figure 3 illustrating a block diagram representative of components in an electronic device or module for implementing embodiments of the invention;

Figure 4 illustrating a timing diagram for establishing a Bluetooth Low Energy (BLE) connection between two devices and the recording of physical layer features of the BLE channel in accordance with embodiments of the invention;

Figure 5 illustrating a received signal strength variation as recorded by a user's device, a vehicle module and an adversary device;

Figure 6A and 6B illustrating block diagrams representative of cryptographically secure Fuzzy Extractor mechanism in accordance with embodiments of the invention;

Figure 7 illustrating a timing diagram for mutually authenticating the user device and the vehicle module based on the recorded physical layer features of the BLE channel in accordance with embodiments of the invention;

Figure 8 illustrating a timing diagram for establishing a Bluetooth Low Energy (BLE) connection between two devices and the recording of physical layer features of the BLE

channel utilizing Public Key Infrastructure (PKI) in accordance with embodiments of the invention; and

Figure 9 illustrating a timing diagram for mutually authenticating the user device and the vehicle module based on the recorded physical layer features of the BLE channel using PKI in accordance with embodiments of the invention.

Detailed Description

This invention describes a system and method for authenticating a Bluetooth connection between a user's device and a vehicle using Bluetooth Low Energy (BLE) technology. In particular, the invention utilizes the physical layer features of the BLE channel between the user's device and the vehicle to mutually authenticate the Bluetooth connection between the user's device and the vehicle.

The system allows for the secure and automatic authentication of user's mobile/personal device with the car using Bluetooth Low Energy (BLE) technology. This system detects and confirms the proximity of user's device to the car and vice versa. The solution does this by exploiting the unique physical layer features of the BLE channel between the user's device and the car. An example of a physical layer feature is the received signal strength (RSS) as detected by the user's device or by the car. The wireless channel's physical features cannot be spoofed by an attacker and is extremely hard to predict. The mutual authentication steps to subsequently authenticate the recorded RSS features are designed based on a cryptographically secure Fuzzy Extractor mechanism and this system may be applied to two types of schemes, one for symmetric key based scenarios, and the other for Public Key Infrastructure (PKI) based scenarios.

Figure 2 illustrates a block diagram of keyless entry system 200 for vehicles in accordance with embodiments of the invention. System 200 comprises vehicle 205 and devices 210 and 220 that belong to user 215. Vehicle 205 is provided with vehicle module 206 that is configured to handle vehicle 205's external communications with other sources and vehicle module 206 and user devices 210 and 220 are all Bluetooth enabled. In accordance with embodiments of the invention, vehicle module 206 may comprise an electronic module, a computing device and/or a wireless transceiver which is configured to receive, process, and transmit instructions relating to vehicle 205. One skilled in the art will recognize that vehicle module 206 may comprise any combinations or types of electronic devices that are able to perform the functions mentioned above without departing from this invention.

Prior to establishing a Bluetooth connection between devices 210, 220 and vehicle module 206, a Bluetooth Connection Key, Key_{BTCon}, is shared between devices 210, 220 and vehicle module 206 by a trusted entity. Once installed within the respective devices or module, this Bluetooth Connection Key, Key_{BTCon}, will be bound to the device or module and may not be transferred out to another device or module as this key, Key_{BTCon} will be used to establish a Bluetooth connection and for encrypting Bluetooth Low Energy (BLE) communications between devices 210, 220 and module 206.

A Bluetooth User Device Key, Key_{BTUDev}, is also shared between devices 210, 220 and vehicle module 206 by a trusted entity. Once installed within the respective devices or module, this Bluetooth User Device Key, Key_{BTUDev}, will be bound to the device or module and may not be transferred out to another device or module as this key, Key_{BTUDev} will be used for encrypting commands and data that are sent through the BLE communications between devices 210, 220 and module 206 thereby increasing the security of the transmitted data.

Figure 3 illustrates a block diagram representative of components of an electronic device 300 that is provided within user devices 210, 220 and module 206 for implementing embodiments in accordance with embodiments of the invention. One skilled in the art will recognize that the exact configuration of each electronic device provided within the user devices or the vehicle module may be different and the exact configuration of electronic device 300 may vary and Figure 3 is provided by way of example only.

In embodiments of the invention, device 300 comprises controller 301 and user interface 302. User interface 302 is arranged to enable manual interactions between a user and electronic device 300 and for this purpose includes the input/output components required for the user to enter instructions to control electronic device 300. A person skilled in the art will recognize that components of user interface 302 may vary from embodiment to embodiment but will typically include one or more of display 340 that may be touchscreen enabled, keyboard 335 and track-pad 336.

Controller 301 is in data communication with user interface 302 via bus 315 and includes memory 320, Central Processing Unit (CPU) 305 mounted on a circuit board that processes instructions and data for performing the method of this embodiment, an operating system 306, an input/output (I/O) interface 330 for communicating with user interface 302 and a communications interface, in this embodiment in the form of a network card 350. Network card 350 may, for example, be utilized to send data from electronic device 300 via a

wired or wireless network to other processing devices or to receive data via the wired or wireless network. Wireless networks that may be utilized by network card 350 include, but are not limited to, Wireless-Fidelity (Wi-Fi), Bluetooth, Near Field Communication (NFC), cellular networks, satellite networks, telecommunication networks, Wide Area Networks (WAN) and etc.

Memory 320 and operating system 306 are in data communication with CPU 305 via bus 310. The memory components include both volatile and non-volatile memory and more than one of each type of memory, including Random Access Memory (RAM) 320, Read Only Memory (ROM) 325 and a mass storage device 345, the last comprising one or more solid-state drives (SSDs). Memory 320 also includes secure storage 346 for securely storing secret keys, or private keys. It should be noted that the contents within secure storage 346 are only accessible by a super-user or administrator of device 300 and may not be accessed by any user of device 300. One skilled in the art will recognize that the memory components described above comprise non-transitory computer-readable media and shall be taken to comprise all computer-readable media except for a transitory, propagating signal. Typically, the instructions are stored as program code in the memory components but can also be hardwired. Memory 320 may include a kernel and/or programming modules such as a software application that may be stored in either volatile or non-volatile memory.

Herein the term “CPU” is used to refer generically to any device or component that can process such instructions and may include: a microprocessor, microcontroller, programmable logic device or other computational device. That is, CPU 305 may be provided by any suitable logic circuitry for receiving inputs, processing them in accordance with instructions stored in memory and generating outputs (for example to the memory components or on display 340). In this embodiment, CPU 305 may be a single core or multi-core processor with memory addressable space. In one example, CPU 305 may be multi-core, comprising—for example—an 8 core CPU.

In the subsequent sections, for brevity, reference is made only to the interactions between user device 210 and vehicle module 206. One skilled in the art will recognize that user device 210 may be replaced with device 220 or any other similar devices without departing from this invention.

As illustrated in Figure 4, vehicle module 206 is configured to periodically transmit BLE beacons that contain the unique credentials/Identity of the vehicle 205. This is illustrated at step 412. When user 215 starts walking towards vehicle 205 and when user

215 is within communication range of the vehicle's BLE beacons, the user's personal device(s) 210 will detect and receive the BLE beacon transmitted from vehicle module 206. The vehicle's ID/credentials as contained in the BLE beacon is then used to identify that the vehicle 205 belongs to user 215.

In accordance with embodiments of the invention, at step 415, when device 210 has determined that vehicle 205 belongs to user 215, device 210 will establish a Bluetooth pairing between device 210 and vehicle module 206 using the Bluetooth Connection Key, Key_{BTCon}, that was previously shared between device 210 and vehicle module 206 by a trusted entity.

Once the Bluetooth pairing has been completed, device 210 will then generate an initiation instruction defined as (ID_{UDev} || *CMD_START_AUTH*, MAC (Key_{BTUDev}, ID_{UDev} || *CMD_START_AUTH*)) where initiation Message Authentication Code M_{Ini} is defined as MAC (Key_{BTUDev}, ID_{UDev} || *CMD_START_AUTH*), ID_{UDev} is defined as the identity of the user's device 210 and *CMD_START_AUTH* is an initiation command identifier for instructing vehicle module 206 to initiate communications. The notation MAC (k, m) is a message authentication code using SHA-256 hash algorithm for a message *m* using a key *k*. At step 420, the initiation instruction is then communicated to vehicle module 206.

Upon receiving the initiation instruction, vehicle module 206 will extract the identity ID_{UDev} of user device 210 is from the initiation instruction. The extracted identity ID_{UDev} is then used to retrieve a corresponding Bluetooth User Device (BUD) Key, Key_{BTUDev}, from a database linked to vehicle module 206. The corresponding BUD Key, Key_{BTUDev}, is then used to validate the initiation instruction. Once validated, vehicle module 206 will then generate an acknowledgement instruction at step 425 whereby the acknowledgement instruction is defined as (*E(Key_{BTUDev}, n || r || CMD_ACK_AUTH), MAC(Key_{BTUDev}, n || r || CMD_ACK_AUTH)*), where acknowledgement Message Authentication Code MAC_{Ack} is defined as *MAC(Key_{BTUDev}, n || r || CMD_ACK_AUTH)*, the E(k, m) is an encryption function to encrypt message *m* with key *k*, CMD_ACK_AUTH is an acknowledgement command identifier for acknowledging a device, *n* is a nonce, and *r* is a random string. The acknowledgement instruction is then communicated to user device 210.

In embodiments of the invention, vehicle module 206 is then configured to record physical layer features (PF) of the Bluetooth Low Energy (BLE) channel established between the user device 210 and vehicle module 205. In embodiments of the invention, the physical features of the BLE channel may comprise received signal strength (RSS) measures that

were measured using a timer function with a *t* ms timeout for a particular time period, e.g. a few seconds (4 - 5 seconds) during which the user is walking towards his/her car. Alternatively, a challenge response protocol can be employed for a synchronized PF reading between two parties with nonce *n* being applied to all communications. Here, the response must be sent within channel coherence time which typically comprises a few milliseconds. The recording of the physical layer features of the BLE channel PF_{TBox} or PF_{Veh} by vehicle module 206 is illustrated as step 435. One skilled in the art will recognize that step 435 may take place prior to the communication of the acknowledgement instruction or after the communication of the acknowledgement instruction without departing from the invention.

Upon receiving the acknowledgement instruction, user device 210 will then validate the received acknowledgement instruction using the BUD Key, Key_{BTUDev}. Upon successfully validating the instruction, the acknowledgement message is then decrypted using the BUD Key $Key_{BTUDev.}$ The acknowledgement command is then retrieved from the decrypted message and the acknowlemdgement command causes the user device 210 to then record a set of physical layer features PF_{UDev} of the BLE beacon's channel at step 430.

After step 430, both the user device 210 and vehicle module 206 will each have a set of physical layer features of the BLE beacon's channel recorded, i.e. PF_{UDev} for user device 210, and PF_{TBox} or PF_{Veh} for vehicle module 206. The recorded set of physical layer features PF_{UDev} and the set of physical layer features PF_{TBox} or PF_{Veh} are then mutually validated by a Fuzzy Extractor mechanism.

When the devices are connected over BLE, the wireless BLE channel exhibits reciprocity property, i.e. the wireless channels physical features e.g. signal strength, measured by both the legitimate devices in quick succession (within few a milliseconds) will be nearly the same. When two devices record these features over a short period of time, the overall variation observed by the two devices will be highly correlated. It should be noted that, the values may not be exactly similar; however, the overall trend or pattern of the two datasets will be nearly similar. Specifically, due to reciprocity property of the wireless channel, the recorded sets of PF_{UDev} and PF_{TBox} or PF_{Veh} will both show high correlation in their variation trends even though the individually recorded values may not be exactly same because of in-channel noise, hardware factors, etc.

At the same time, when an adversary or eavesdropper (third device/attacker) eavesdrops on the communication between the two legitimate devices (user's device and the vehicle module) and records the signal features, his/her channel features will be totally

different compared to the recording done by legitimate devices. This is because, although the adversary is in the vicinity of the legitimate devices, the signal captured by him/her will be different due to the multi-path effects of the wireless channel, i.e., the signal takes different multiple paths to reach the adversary's device. Hence, the adversary cannot even guess the values obtained by car and user's device. Even if the adversary were to adopt the same scheme as the legitimate devices, he/she cannot be successful in authenticating the communications between the user device and the vehicle module. Figure 6 illustrates the received signal strength variation as recorded by user device, vehicle module and adversary for the above scenario whereby plot 505 shows the recorded RSS for the user device, plot 510 shows the recorded RSS for the vehicle module and 515 shows the recorded RSS for the adversary.

Further, it should be noted that the invention allows both parties to detect active man-in-the-middle attacks as symmetric keys and signal variation patterns are employed to detect and authenticate the devices. Only the pair of connected wireless devices can have similar RSS values due to reciprocity property of wireless channel. This means that adversaries or other BLE devices in the vicinity of legitimate devices cannot predict the RSS values obtained by legitimate parties. The RSS trend can be used to confirm if the user is really approaching i.e., RSS value increases as the user approaches the vehicle. Hence, both the party's user's device and vehicle module can confirm this behaviour. Therefore, the invention provides strong mutual authentication with the help of Physical layer features of wireless channel (BLE) that cannot be spoofed or guessed by an adversary/eavesdropper. The legitimate parties will get know by their physical layer features if there is any attack during authentication. Thus, relay and impersonation attacks are mitigated by the invention.

In order to authenticate the physical layer features of the BLE beacon's channel as recorded by the user device 210 and the vehicle module 206, a cryptographically secure Fuzzy Extractor based mechanism is employed. A Fuzzy extractor mechanism consists of a pair of functions: Generate (Gen) 605 and Reproduce (Rep) 610 whereby the properties of these two functions 605, 610 are shown in Figure 6A. The Gen function takes an input, a set of values w and produces a string s and set H. The Rep function takes two inputs, a set w' which is nearly same as w, but has some errors with respect to w, and H produced by Gen, to produce s which is exactly same as the s produced by Gen. The exact workings of the Fuzzy Extractor mechanism are omitted for brevity.

Hence, as illustrated in Figure 6B, when the Gen function 605 is used on the physical layer features of the BLE beacon's channel as recorded by the user device, the Gen function

takes in as its input the set of PF_{UDev} and produces two outputs s_{UDev} and *C*. As for the Rep function 610, this function is applied by vehicle module 206 by taking as its input the physical layer features of the BLE beacon's channel as recorded by the vehicle module, PF_{TBox} or PF_{Veh} and *C* to produce s_{Veh} that will be similar as that of s_{UDev}.

The mutual authentication of the physical layer features of the BLE beacon's channel as recorded by both the user device 210 and vehicle module 206 is illustrated in Figure 7. At step 705, user device 210 first applies a low pass filter to PF_{UDev} to remove any spikes that may occur due to noise in the channel. Subsequently at step 710, the Gen function is then applied to the set of recorded physical layer features of the BLE beacon's channel PF_{UDev} to generate string s_{UDev} and Correction Data *C*.

A verification instruction defined as ($E(Key_{BTUDev}, n \,||\, C \,||\, CMD\_HLP)$, $MAC(Key_{BTUDev}, n \,||\, C \,||\, CMD\_HLP)$) is then generated at step 715, where verification Message Authentication Code M_{Ver} is defined as $MAC(Key_{BTUDev}, n \,||\, C \,||\, CMD\_HLP)$, and CMD_HLP is a verification command identifier for instructing the vehicle module initiate mutual authentication steps.

At step 725, an authentication check instruction defined as $E(Key_{BTUDev}, n \,||\, (r \text{ XOR } s_{UDev}) \,||\, CMD\_AUTH\_CHK)$, $MAC(Key_{BTUDev}, n \,||\, (r \text{ XOR } s_{UDev}) \,||\, CMD\_AUTH\_CHK)$) is then generated, where authentication check Message Authentication Code M_{Auth_chk} is defined as $MAC(Key_{BTUDev}, n \,||\, (r \text{ XOR } s_{UDev}) \,||\, CMD\_AUTH\_CHK)$, and CMD_AUTH_CHK is an authentication check command identifier for instructing the vehicle module to compare the recorded physical layer features of the BLE beacon and XOR is a logic XOR operation.

Upon receiving the verification instruction and decrypting and validating the verification instruction, at step 720, C parameters are extracted from the verification instruction. Vehicle module 206 then applies filtering and at step 730, the Rep function is applied to the set of recorded physical layer features of the BLE beacon's channel PF_{TBox} or PF_{Veh} and *C* to produce s_{Veh}.

Upon receiving the authentication check instruction and decrypting and validating the authentication check instruction, vehicle module 206 verifies whether $((r \text{ XOR } s_{UDev})$ as extracted from the authentication check message is same as $(_r \text{ XOR } s_{Veh})$ that was generated by vehicle module 206. This is done at step 732. If it is determined that both are the same, then the authentication is considered successful, and an approval instruction defined as ($E(Key_{BTUDev}, n \,||\, CMD\_AUTH\_OK)$, $MAC(Key_{BTUDev}, n \,||\, CMD\_AUTH\_OK)$) is generated where approval Message Authentication Code M_{Apprv} is defined as $MAC(Key_{BTUDev},$

n || CMD_AUTH_OK), CMD_AUTH_OK is an approval command identifier and the approval instruction is sent to user device 210 at step 735.

Conversely, if the verification fails, an error instruction defined as (E(Key_{BTUDev}, *n* || CMD_AUTH_FAIL), MAC(Key_{BTUDev}, *n* || CMD_AUTH_FAIL)) is generated where error Message Authentication Code M_{Error} is defined as MAC(Key_{BTUDev}, *n* || CMD_AUTH_FAIL), CMD_AUTH_FAIL is an error command identifier and the error instruction is sent to user device 210 and the authentication is then rejected at step 740.

Upon receiving the instructions, the user device will validate either the received approval instruction or the error instruction using the BUD Key Key_{BTUDev}. Once validated, the user device then proceeds to decrypt either the approval or error instruction.

In embodiments of the invention, if the Bluetooth on a user's device is not turned on while he/she is approaching the vehicle, automatic detection and authentication with the vehicle may not occur. Hence, in such a scenario, when the notices the device's status indicates that the device is not connected to the vehicle, the user then turns on Bluetooth on his user device to enable the device to connect to the vehicle. Upon successfully pairing the device with the vehicle's module, the user device will detect that the user is already near the car using RSS information obtained during the pairing step. The user will then be notified via an application on their device to wave his/her device towards the vehicle, i.e. to move the device in random manner a few times. If the device is a smartphone, the user will just need to wave it towards the vehicle, and if the device is a smartwatch worn on wrist, the user just needs to wave the watch in the direction of the vehicle to authenticate as described above.

Second Embodiment: Public Key Infrastructure (PKI) Based Solution

In another embodiment of the invention, in addition to pre-sharing the Bluetooth Connection Key, Key_{BTCon}, the Bluetooth User Device Key, Key_{BTUDev}, between devices 210, 220 and vehicle module 206 by a trusted entity, public-private key pairs are also provided by the trusted entity to devices 210, 220 and vehicle module 206.

As illustrated in Figure 8, vehicle module 206 is configured to periodically transmit BLE beacons that contain the unique credentials/Identity of the vehicle 205. This is illustrated as step 810. When user 215 is within communication range of the vehicle's BLE beacons, the user's personal device(s) 210 will detect and receive the BLE beacon transmitted from vehicle module 206. The vehicle's ID/credentials as contained in the BLE beacon is then used to identify that the vehicle 205 belongs to user 215.

In accordance with embodiments of the invention, at step 815, when device 210 has determined that vehicle 205 belongs to user 215, device 210 will establish a Bluetooth pairing between device 210 and vehicle module 206 using the Bluetooth Connection Key, Key_{BTCon}, that was previously shared between device 210 and vehicle module 206 by a trusted entity.

Once the Bluetooth pairing has been completed, device 210 will then generate an initiation instruction defined as ($E(Key_{Pub\_Veh}, m_0)$, $S(Key_{Priv\_Udev}, m_1)$), where initiation message m_0 is defined as (ID_{UDev} || CMD_START_AUTH), ID_{UDev} is the identity of the user's device, and CMD_START_AUTH is the initiation command identifier for instructing vehicle module 206 to initiate communications. The encryption function E(k, m) causes message *m* to be encrypted with key *k*, m_1 is defined as $H(Key_{BTUDev}, E(Key_{Pub\_Veh}, m_0))$, and the signing function S(k, m) causes message *m* to be signed using key *k*. H comprises a hash function that performs the hash using SHA-256 hash algorithm. At step 820, the initiation instruction is then communicated to vehicle module 206.

Upon receiving the initiation instruction, the vehicle module 206 will verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, and when it is verified, the vehicle module 206 then decrypts the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}. Based on the decrypted initiation message, a corresponding Key K_{BTUDev}, for ID_{UDev} is then retrieved from a database.

Vehicle module 206 will then generate an acknowledgement instruction at step 825 whereby the acknowledgement instruction is defined as ($E(Key_{BTUDev}, m_2)$, $S(Key_{Priv\_Veh}, m_3)$), where, m_2 is defined as (*n* || *r* || CMD_ACK_AUTH), where CMD_ACK_AUTH is an acknowledgement command identifier for acknowledging a device, *n* is a nonce, and *r* is a random string, and m3 is defined as $H(Key_{BTUDev}, E(Key_{BTUDev}, m_2))$. The acknowledgement instruction is then communicated to user device 210.

In embodiments of the invention, vehicle module 206 is then configured to record physical layer features (PF) of the Bluetooth Low Energy (BLE) channel established between the user device 210 and vehicle module 205. In embodiments of the invention, the physical features of the BLE channel may comprise received signal strength (RSS) measures that were measured using a timer function with a *t* ms timeout for a particular time period, e.g. a few seconds (4 - 5 seconds) during which the user is walking towards his/her car. Alternatively, a challenge response protocol can be employed for a synchronized PF reading

between two parties with nonce *n* being applied to all communications. Here, the response must be sent within channel coherence time which typically comprises a few milliseconds. The recording of the physical layer features of the BLE channel PF_{TBox} or PF_{Veh} by vehicle module 206 is illustrated as step 835. One skilled in the art will recognize that step 835 may take place prior to the communication of the acknowledgement instruction or after the communication of the acknowledgement instruction without departing from the invention.

Upon receiving the acknowledgement instruction, user device 210 will then verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}. The encrypted acknowledgement message is then decrypted using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified. Once the message is decrypted, the user device 210 then proceeds to record a set of physical layer features PF_{UDev} of the BLE beacon's channel at step 830.

After step 830, both the user device 210 and vehicle module 206 will each have a set of physical layer features of the BLE beacon's channel recorded, i.e. PF_{UDev} for user device 210, and PF_{TBox} or PF_{Veh} for vehicle module 206. The recorded set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} or or PF_{Veh} are then mutually validated by a Fuzzy Extractor mechanism which has been described in detail in the previous embodiment.

The mutual authentication of the physical layer features of the BLE beacon's channel as recorded by both the user device 210 and vehicle module 206 is illustrated in Figure 9. At step 905, user device 210 first applies a low pass filter to PF_{UDev} to remove any spikes that may occur due to noise in the channel. Subsequently at step 910, the Gen function is then applied to the set of recorded physical layer features of the BLE beacon's channel PF_{UDev} to generate user string s_{UDev} and Correction Data *C*.

A verification instruction defined as $(E(Key_{BTUDev}, m_4), S(Key_{Priv\_Udev}, m_5))$ is generated at step 915, where m_4 is defined as (n || C || CMD_HLP), where CMD_HLP is a verification command identifier for instructing the vehicle module initiate mutual authentication steps, m_5 is defined as $H(Key_{BTUDev}, E(Key_{BTUDev}, m_4))$.

At step 925, an authentication check instruction defined as $(E(Key_{BTUDev}, m_6), S((Key_{Priv\_Udev}, m_7))$ is then generated, where m_6 is defined as (n || (r XOR s_{UDev}) || CMD_AUTH_CHK), where CMD_AUTH_CHK is an authentication check command identifier for instructing the vehicle module to compare the recorded physical layer features

of the BLE beacon and XOR is a logic XOR operation and m_7 is defined as $H(Key_{BTUDev}, E(Key_{BTUDev}, m_6))$.

Upon receiving the verification instruction, the signed-hashed-encrypted verification message in the verification instruction is verified using a PKI-Public Key associated with the user device, Key_{Pub_UDev}. The encrypted verification message is then decrypted using the corresponding BUD Key K_{BTUDev}, and the Correction Data *C* is extracted from the decrypted verification message. The vehicle module then filters the extracted Correction Data *C* and the set of physical layer features PF_{TBox} or PF_{Veh} using a low pass filter when the verification instruction is validated at step 920. A vehicle string S_{Veh} is then generated by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism at step 930.

Similarly, upon receiving the authentication check instruction, the signed-hashed-encrypted authentication check message in the authentication check instruction is verified using a PKI-Public Key associated with the user device, Key_{Pub_UDev}. The encrypted authentication check message is then decrypted using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified.

Upon decrypting and validating the authentication check instruction, vehicle module 206 verifies whether ((*r* XOR s_{UDev}) as extracted from the authentication check message is same as ($_r$ XOR s_{Veh}) that was generated by vehicle module 206. This is done at step 932. If it is determined that both are the same, then the authentication is considered successful, and an approval instruction defined as $(E(Key_{BTUDev}, m_8), S(Key_{Priv\_Veh}, m_9))$ is generated, where m_8 = (*n* || CMD_AUTH_OK), m_9 = $H(Key_{BTUDev}, E(Key_{BTUDev}, m_8))$, and CMD_AUTH_OK is an approval command identifier to approve the mutual authentication. The approval instruction is then sent to user device 210 at step 935.

Conversely, if the verification fails, an error instruction defined as $(E(Key_{BTUDev}, m_{10}), S(Key_{Priv\_Veh}, m_{11}))$ is generated and mutual authentication is rejected, where m_{10} is defined as (*n* || CMD_AUTH_FAIL), where m_{11} is defined as $H(Key_{BTUDev}, E(Key_{BTUDev}, m_{10}))$, and CMD_AUTH_FAIL is the error command to reject the mutual authentication process. The error instruction is then sent to user device 210 at step 940.

Upon receiving the approval instructions, the user device will verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}. The encrypted approval message is then decrypted using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval

message is verified. The authentication of the user device and the vehicle module is then completed based on the approval command in the decrypted approval message.

Conversely, upon receiving the error instructions, the user device will verify the signed-hashed-encrypted error message in the error instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}. The encrypted error message is then decrypted using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted error message is verified. The authentication of the vehicle module and the user device is then rejected based on the error command in the decrypted approval message.

In accordance with another embodiment of the invention, with reference to Figures 2 and 3, either one of user devices 210 or 220 may be used to authenticate Bluetooth or wireless communications with vehicle module 206. In particular, user device 210 has a processor 305 and a non-transitory media 320 readable by the processor 305 whereby the non-transitory media 320 is configured to store instructions. When these instructions are executed by the processor 305, the instructions cause processor 305 to: generate an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device 210 and the vehicle module 206; communicate the initiation instruction to the vehicle module 206 such that upon receiving the initiation instruction, the vehicle module 206 is configured to: retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key K_{BTUDev}; and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; communicate the acknowledgement instruction to the user device 210; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device 210 further comprising instructions for directing the processor to: validate the acknowledgement instruction using the BUD Key K_{BTUDev}; record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticate the vehicle module 206 when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

In accordance with yet another embodiment of the invention, with reference to Figures 2 and 3, either one of user devices 210 or 220 may be used to authenticate Bluetooth or wireless communications with vehicle module 206. In particular, user device 210 has a processor 305 and a non-transitory media 320 readable by the processor 305 whereby the non-transitory media 320 is configured to store instructions. When these instructions are executed by the processor 305, the instructions cause processor 305 to: encrypt an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh}; hash the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; generate an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message; communicate the initiation instruction to the vehicle module 206 such that upon receiving the initiation instruction, the vehicle module 206 is configured to: verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module 206, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; communicate the acknowledgement instruction to the user device 210; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; the user device 210 further comprising instructions for directing the processor to: verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified; record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticate the vehicle module 206 when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

In accordance with yet another embodiment of the invention, with reference to Figures 2 and 3, vehicle module 206 may be used to authenticate Bluetooth or wireless communications with either one of user devices 210 or 220. In particular, user device 210 has a processor 305 and a non-transitory media 320 readable by the processor 305 whereby the non-transitory media 320 is configured to store instructions. When these instructions are executed by the processor 305, the instructions cause processor 305 to: receive an initiation instruction from the user device, wherein the initiation instruction is generated based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini}, whereby the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device 210 and the vehicle module 206; retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev}; generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated, wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev}; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; communicate the acknowledgement instruction to the user device 210 such that upon receiving the acknowledgement instruction, the user device 210 is configured to: validate the acknowledgement instruction using the BUD Key K_{BTUDev}; record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

In accordance with yet another embodiment of the invention, with reference to Figures 2 and 3, vehicle module 206 may be used to authenticate Bluetooth or wireless communications with either one of user devices 210 or 220. In particular, user device 210 has a processor 305 and a non-transitory media 320 readable by the processor 305 whereby the non-transitory media 320 is configured to store instructions. When these instructions are executed by the processor 305, the instructions cause processor 305 to: receive an initiation instruction from the user device 210, wherein the initiation instruction is generated based on an encrypted initiation message and a signed-hashed-encrypted initiation message, the initiation message, m_o, which comprises an identity of the user device ID_{UDev} and an initiation

command, is encrypted using a Public Key Infrastructure (PKI)-Public Key associated with the vehicle module, Key_{Pub_Veh}, and the encrypted initiation message is hashed using a Bluetooth User Device (BUD) Key K_{BTUDev}, and signed using a PKI-Private Key associated with the user device, Key_{Priv_UDev}; verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev}, decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified; encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev}; hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh}; generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message; record a set of physical layer features PF_{Veh} of the BLE beacon's channel; communicate the acknowledgement instruction to the user device 210 such that upon receiving the acknowledgement instruction, the user device 210 is configured to: verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh}, decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified; record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and authenticate the vehicle module 206 when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

The above is a description of embodiments of a system and process in accordance with the present invention as set forth in the following claims. It is envisioned that others may and will design alternatives that fall within the scope of the following claims.

CLAIMS:

1. A vehicle authenticating system comprising:
a user device that is configured to:
generate an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini},
wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and a vehicle module;
communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:
retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev};
generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated,
wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev};
communicate the acknowledgement instruction to the user device;
record a set of physical layer features PF_{Veh} of the BLE beacon's channel;
the user device further configured to:
validate the acknowledgement instruction using the BUD Key K_{BTUDev};
record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and
authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

2. The system according to claim 1 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises:
the user device being configured to:

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver},

wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev};

generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk},

wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev};

communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

validate the verification and authentication check instructions using the BUD Key K_{BTUDev};

extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and

communicate the approval instruction to the user device;

the user device further configured to:

validate the approval instruction using the BUD Key K_{BTUDev}; and

authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

3. The system according to claims 1 or 2 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

4. The system according to any one of claims 1 to 3 wherein before the initiation instruction is generated by the user device, the user device is configured to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

5. A vehicle authenticating system comprising:

a user device that is configured to:

encrypt an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh};

hash the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message;

communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:

verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified;

encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev};

hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message;

communicate the acknowledgement instruction to the user device;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

the user device further configured to:

verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified;

record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and

authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

6. The system according to claim 5 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the user device being configured to:

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command;

hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message;

encrypt an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command;

hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message;

communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified;

extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified;

encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command;

hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh};

communicate the approval instruction to the user device;

the user device further configured to:

verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and

authenticate the vehicle module based on the approval command in the decrypted approval message.

7. The system according to claims 5 or 6 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

8. The system according to any one of claims 5 to 7 wherein before the initiation instruction is encrypted by the user device, the user device is configured to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

9. A user device for authenticating communications with a vehicle module, the user device comprising:

a processor; and

a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to:

generate an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini},

wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and the vehicle module;

communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:

retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev};

generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated,

wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev};

communicate the acknowledgement instruction to the user device;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

the user device further comprising instructions for directing the processor to:

validate the acknowledgement instruction using the BUD Key K_{BTUDev};

record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and

authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

10. The user device according to claim 9 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises:

the user device comprising instructions for directing the processor to:

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver},

wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev};

generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk},

wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev};

communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

validate the verification and authentication check instructions using the BUD Key K_{BTUDev};

extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and

communicate the approval instruction to the user device;

the user device further comprising instructions for directing the processor to:

validate the approval instruction using the BUD Key K_{BTUDev}; and

authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

11. The user device according to claims 9 or 10 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

12. The user device according to any one of claims 9 to 11 wherein before the initiation instruction is generated by the user device, the user device comprises instructions for directing the processor to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

13. A user device for authenticating communications with a vehicle module, the user device comprising:

a processor; and

a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to:

encrypt an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh};

hash the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message;

communicate the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:

verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified;

encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev};

hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message;

communicate the acknowledgement instruction to the user device;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

the user device further comprising instructions for directing the processor to:

verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified;

record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and

authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

14. The user device according to claim 13 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises:

the user device comprising instructions for directing the processor to

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command;

hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message;

encrypt an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command;

hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message;

communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified;

extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified;

encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command;

hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh};

communicate the approval instruction to the user device;

the user device further comprising instructions for directing the processor to:

verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and

authenticate the vehicle module based on the approval command in the decrypted approval message.

15. The user device according to claims 13 or 14 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user

device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

16. The user device according to any one of claims 13 to 15 wherein before the initiation instruction is encrypted by the user device, the user device comprises instructions for directing the processor to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

17. A vehicle module for authenticating communications with a user device, the vehicle module comprising:

a processor; and

a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to:

receive an initiation instruction from the user device,

wherein the initiation instruction is generated based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini},

whereby the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and the vehicle module;

retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev};

generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated,

wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev};

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

communicate the acknowledgement instruction to the user device such that upon receiving the acknowledgement instruction, the user device is configured to:

validate the acknowledgement instruction using the BUD Key K_{BTUDev};

record a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and

authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

18. The vehicle module according to claim 17 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises:

the user device is configured to:

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

generate a verification instruction based on an encrypted verification message and a verification MAC M_{Ver},

wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev};

generate an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk},

wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev};

communicate the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication

check instructions, the vehicle module comprises instructions for directing the processor to:

validate the verification and authentication check instructions using the BUD Key K_{BTUDev};

extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and

communicate the approval instruction to the user device;

the user device is further configured to:

validate the approval instruction using the BUD Key K_{BTUDev}; and

authenticate the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

19. The vehicle module according to claims 17 or 18 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

20. The vehicle module according to any one of claims 17 to 19 wherein before the initiation instruction is generated by the user device, the user device comprises instructions for directing the processor to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

21. A vehicle module for authenticating communications with a user device, the vehicle module comprising:

a processor; and

a non-transitory media readable by the processor, the non-transitory media storing instructions that when executed by the processor, cause the processor to:

receive an initiation instruction from the user device,

wherein the initiation instruction is generated based on an encrypted initiation message and a signed-hashed-encrypted initiation message,

the initiation message, m_o, which comprises an identity of the user device ID_{UDev} and an initiation command, is encrypted using a Public Key Infrastructure (PKI)-Public Key associated with the vehicle module, Key_{Pub_Veh}, and

the encrypted initiation message is hashed using a Bluetooth User Device (BUD) Key K_{BTUDev}, and signed using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified;

encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev};

hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

communicate the acknowledgement instruction to the user device such that upon receiving the acknowledgement instruction, the user device is configured to:

verify the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified;

record a set of physical layer features PF_{UDev} of the BLE beacon's channel; and

authenticate the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

22. The vehicle module according to claim 21 wherein the validation of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises:

the user device is configured to

filter the set of physical layer features PF_{UDev} using a low pass filter;

generate a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

encrypt a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command;

hash the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message;

encrypt an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command;

hash the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generate an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message;

communicate the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module comprising instructions for directing the processor to:

verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified;

extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified;

encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command;

hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user

string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh};

communicate the approval instruction to the user device;

the user device is further configured to:

verify the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypt the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and

authenticate the vehicle module based on the approval command in the decrypted approval message.

23. The vehicle module according to claims 21 or 22 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

24. The vehicle module according to any one of claims 21 to 23 wherein before the initiation instruction is encrypted by the user device, the user device comprises instructions for directing the processor to:

establish a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

25. A method for authenticating a Bluetooth connection between a user device and a vehicle module, the method comprising:

generating an initiation instruction based on an identity of the user device ID_{UDev}, an initiation command, and an initiation Message Authentication Code (MAC) M_{Ini},

wherein the MAC M_{Ini} is generated based on the identity of the user device ID_{UDev}, the initiation command and a Bluetooth User Device (BUD) Key K_{BTUDev} that is shared between the user device and a vehicle module;

communicating the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:

retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the received initiation instruction and validate the initiation instruction using the retrieved corresponding BUD Key K_{BTUDev};

generate an acknowledgement instruction based on an encrypted acknowledgement message and an acknowledgement MAC M_{Ack}, when the initiation instruction is validated,

wherein the acknowledgement message comprises a nonce *n*, a random string *r*, and an acknowledgement command and the acknowledgement message is encrypted using the corresponding BUD Key $K_{BTUDev;}$ and the acknowledgement MAC M_{Ack} is generated based on the acknowledgement message and the corresponding BUD Key K_{BTUDev};

communicate the acknowledgement instruction to the user device;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

the method further comprising:

validating, using the user device, the acknowledgement instruction using the BUD Key K_{BTUDev};

recording a set of physical layer features PF_{UDev} of the BLE beacon's channel when the acknowledgement instruction is validated; and

authenticating the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

26. The method according to claim 25 wherein the validating of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the steps of:

filtering, using the user device, the set of physical layer features PF_{UDev} using a low pass filter;

generating a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

generating a verification instruction based on an encrypted verification message and a verification MAC M_{Ver},

wherein the verification message comprising the nonce *n*, the Correction Data *C*, and a verification command is encrypted using the BUD Key K_{BTUDev}, and the verification MAC M_{Ver}, is generated based on the verification message and the BUD Key K_{BTUDev};

generating an authentication check instruction based on an encrypted authentication check message and an authentication check MAC M_{Auth_Chk},

wherein the authentication check message comprising the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command is encrypted using the BUD Key K_{BTUDev}, and the authentication check MAC M_{Auth_Chk}, is generated based on the authentication check message and the BUD Key K_{BTUDev};

communicating the verification instruction and the authentication check instruction to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

validate the verification and authentication check instructions using the BUD Key K_{BTUDev};

extract the Correction Data *C* from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

generate an approval instruction based on an encrypted approval message and an approval MAC M_{Apprv}, wherein the approval message comprising the nonce *n*, and an approval command is encrypted using the corresponding BUD Key K_{BTUDev}, and the approval MAC M_{Apprv}, is generated based on the approval message and the corresponding BUD Key K_{BTUDev}, when the authentication check instruction is validated and when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh}; and

communicate the approval instruction to the user device;

the method further comprising:

validating, using the user device, the approval instruction using the BUD Key K_{BTUDev}; and

authenticating the vehicle module based on the approval command in the decrypted approval message when the approval instruction is validated.

27. The method according to claims 25 or 26 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user

device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

28. The method according to any one of claims 25 to 27 wherein before the initiation instruction is generated by the user device, the method comprises the step of:

establishing a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

29. A method for authenticating a Bluetooth connection between a user device and a vehicle module, the method comprising:

encrypting an initiation message, m_o, comprising an identity of the user device ID_{UDev} and an initiation command, using a Public Key Infrastructure (PKI)-Public Key associated with a vehicle module, Key_{Pub_Veh};

hashing the encrypted initiation message using a Bluetooth User Device (BUD) Key K_{BTUDev}, and sign the hashed-encrypted initiation message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generating an initiation instruction based on the encrypted initiation message and the signed-hashed-encrypted initiation message;

communicating the initiation instruction to the vehicle module such that upon receiving the initiation instruction, the vehicle module is configured to:

verify the signed-hashed-encrypted initiation message in the initiation instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted initiation message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh} and retrieve a corresponding BUD Key K_{BTUDev}, from a database, based on the decrypted initiation message when the signed-hashed-encrypted initiation message is verified;

encrypt an acknowledgement message, m_2, comprising a nonce *n*, a random string *r*, and an acknowledgement command, using the corresponding BUD Key K_{BTUDev};

hash the encrypted acknowledgement message using the corresponding BUD Key K_{BTUDev}, and sign the hashed-encrypted acknowledgement message using the PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an acknowledgement instruction based on the encrypted acknowledgement message and the signed-hashed-encrypted acknowledgement message;

communicate the acknowledgement instruction to the user device;

record a set of physical layer features PF_{Veh} of the BLE beacon's channel;

the method further comprising the steps of:

verifying, using the user device, the signed-hashed-encrypted acknowledgement message in the acknowledgement instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypting the encrypted acknowledgement message using the BUD Key K_{BTUDev} when the signed-hashed-encrypted acknowledgement message is verified;

recording a set of physical layer features PF_{UDev} of the BLE beacon's channel; and

authenticating the vehicle module when the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} are validated by a Fuzzy Extractor mechanism.

30. The method according to claim 29 wherein the validating of the set of physical layer features PF_{UDev} and the set of physical layer features PF_{Veh} by the Fuzzy Extractor mechanism comprises the steps of:

filtering, using the user device, the set of physical layer features PF_{UDev} using a low pass filter;

generating a user string S_{UDev} and a Correction Data *C* by providing the filtered set of physical layer features PF_{UDev} to a Generate (Gen) function of the Fuzzy Extractor mechanism;

encrypting a verification message, m_4, using the BUD Key K_{BTUDev}, wherein the verification message m_4, comprises the nonce *n*, the Correction Data *C*, and a verification command;

hashing the encrypted verification message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted verification message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generating a verification instruction based on the encrypted verification message and the signed-hashed-encrypted verification message;

encrypting an authentication check message, m_6, using the BUD Key K_{BTUDev}, wherein the authentication check message m_6, comprises the nonce *n*, an *XOR* operation between the random string *r* and the user string S_{UDev}, and an authentication check command;

hashing the encrypted authentication check message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the user device, Key_{Priv_UDev};

generating an authentication check instruction based on the encrypted authentication check message and the signed-hashed-encrypted authentication check message;

communicating the verification and the authentication check instructions to the vehicle module such that upon receiving the verification and authentication check instructions, the vehicle module is configured to:

verify the signed-hashed-encrypted verification message in the verification instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted verification message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted verification message is verified;

extract the Correction Data *C*, from the decrypted verification message, and filter the extracted Correction Data *C* and the set of physical layer features PF_{Veh} using a low pass filter when the verification instruction is validated;

generate a vehicle string S_{Veh} by providing the filtered set of physical layer features PF_{Veh} and the filtered Correction Data *C* to a Reproduce (Rep) function of the Fuzzy Extractor mechanism;

verify the signed-hashed-encrypted authentication check message in the authentication check instruction using a PKI-Public Key associated with the user device, Key_{Pub_UDev},

decrypt the encrypted authentication check message using the corresponding BUD Key K_{BTUDev}, when the signed-hashed-encrypted authentication check message is verified;

encrypt an approval message, m_8, using the BUD Key K_{BTUDev}, wherein the approval message m_8, comprises the nonce *n*, and an approval command;

hash the encrypted approval message using the BUD Key K_{BTUDev}, and sign the hashed-encrypted authentication check message using a PKI-Private Key associated with the vehicle module, Key_{Priv_Veh};

generate an approval instruction based on the encrypted approval message and the signed-hashed-encrypted approval message, when it is determined that the *XOR* operation between the random string *r* and the user string S_{UDev} matches an *XOR* operation between the random string *r* and the vehicle string S_{Veh};

communicate the approval instruction to the user device;

the method further comprising the steps of:

verifying the signed-hashed-encrypted approval message in the approval instruction using a PKI-Public Key associated with the vehicle module, Key_{Pub_Veh},

decrypting the encrypted approval message using the BUD Key K_{BTUDev}, when the signed-hashed-encrypted approval message is verified; and

authenticating the vehicle module based on the approval command in the decrypted approval message.

31. The method according to claims 29 or 30 whereby the set of physical layer features PF_{UDev} comprises a first set of received signal strength values recorded by the user device and the set of physical layer features PF_{Veh} comprises a second set of received signal strength values recorded by the vehicle module.

32. The method according to any one of claims 29 to 31 wherein before the initiation instruction is encrypted by the user device, the method comprises the steps of:

establishing a Bluetooth pairing between the user device and the vehicle module using a Bluetooth Connection Key, Key_{BTCon}, when the BLE beacon emitted by the vehicle module is detected by the user device, whereby the Key K_{BTCon}, is shared between the user device and the vehicle module.

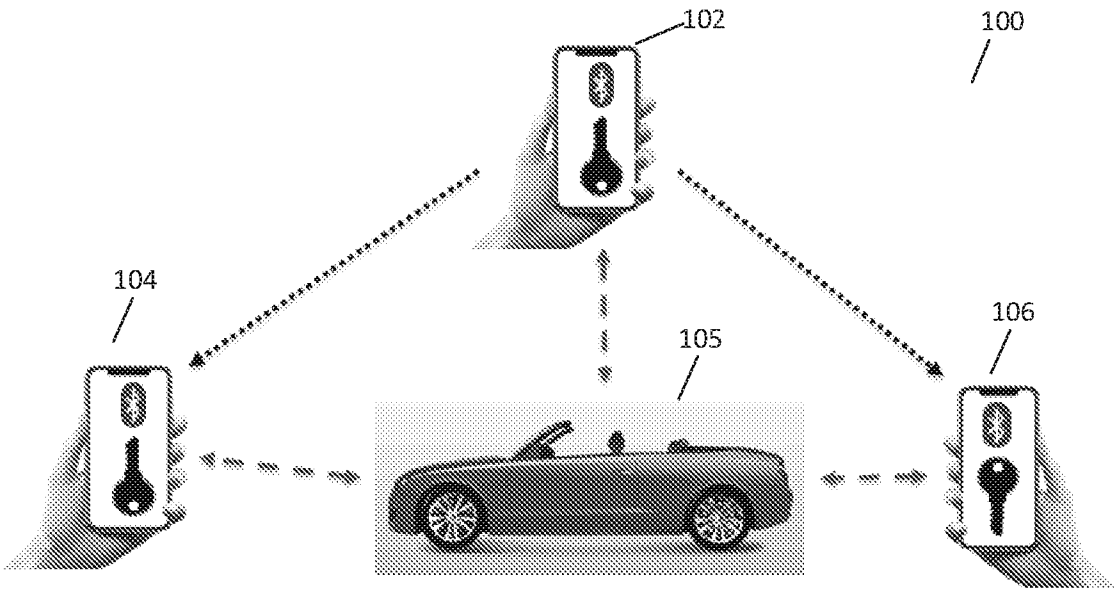

FIGURE 1

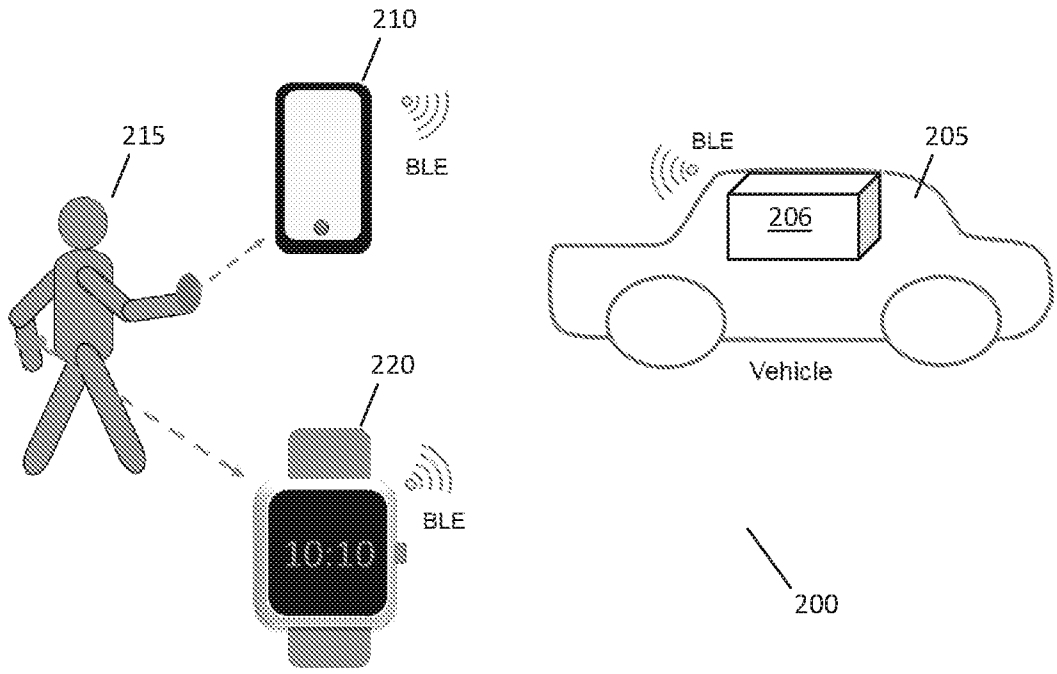

FIGURE 2

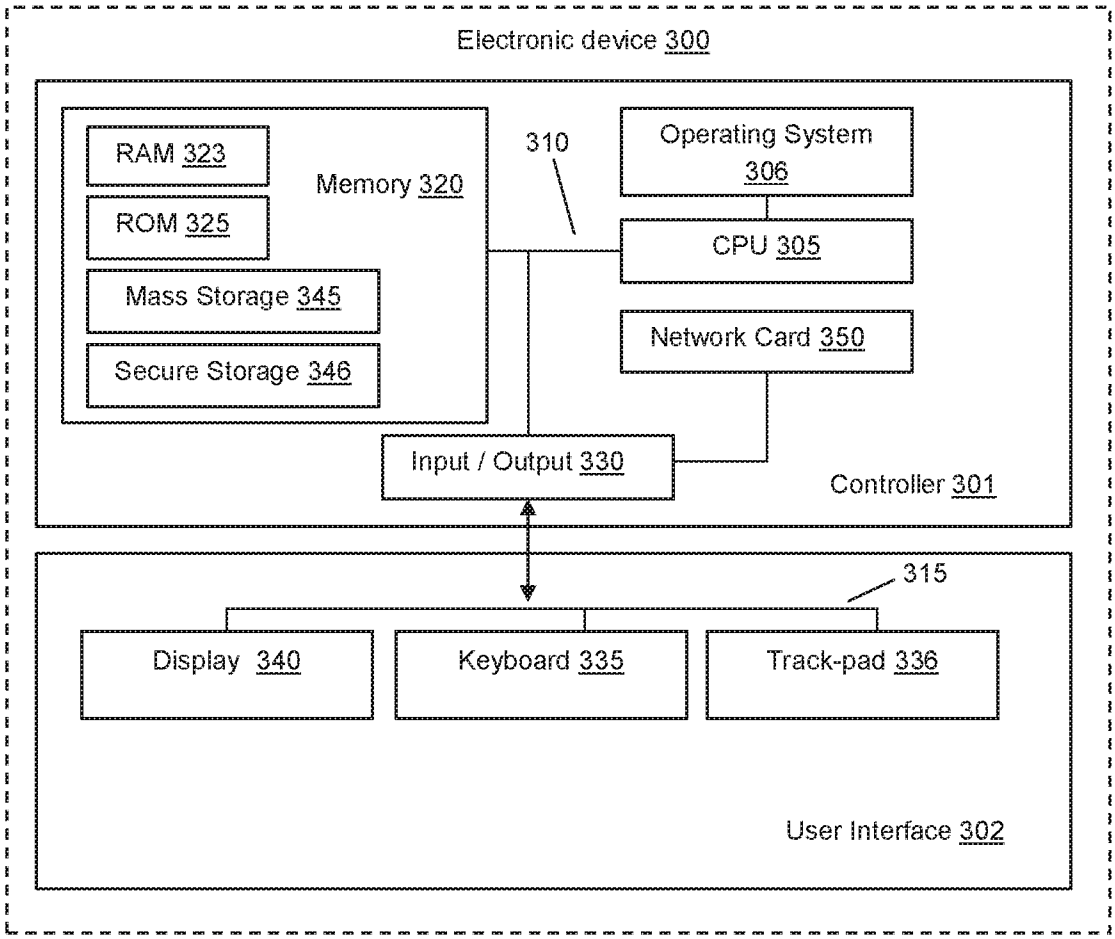
Electronic device 300
RAM 323
ROM 325
Memory 320
Mass Storage 345
Secure Storage 346
310
Operating System 306
CPU 305
Network Card 350
Input / Output 330
Controller 301
315
Display 340
Keyboard 335
Track-pad 336
User Interface 302

FIGURE 3

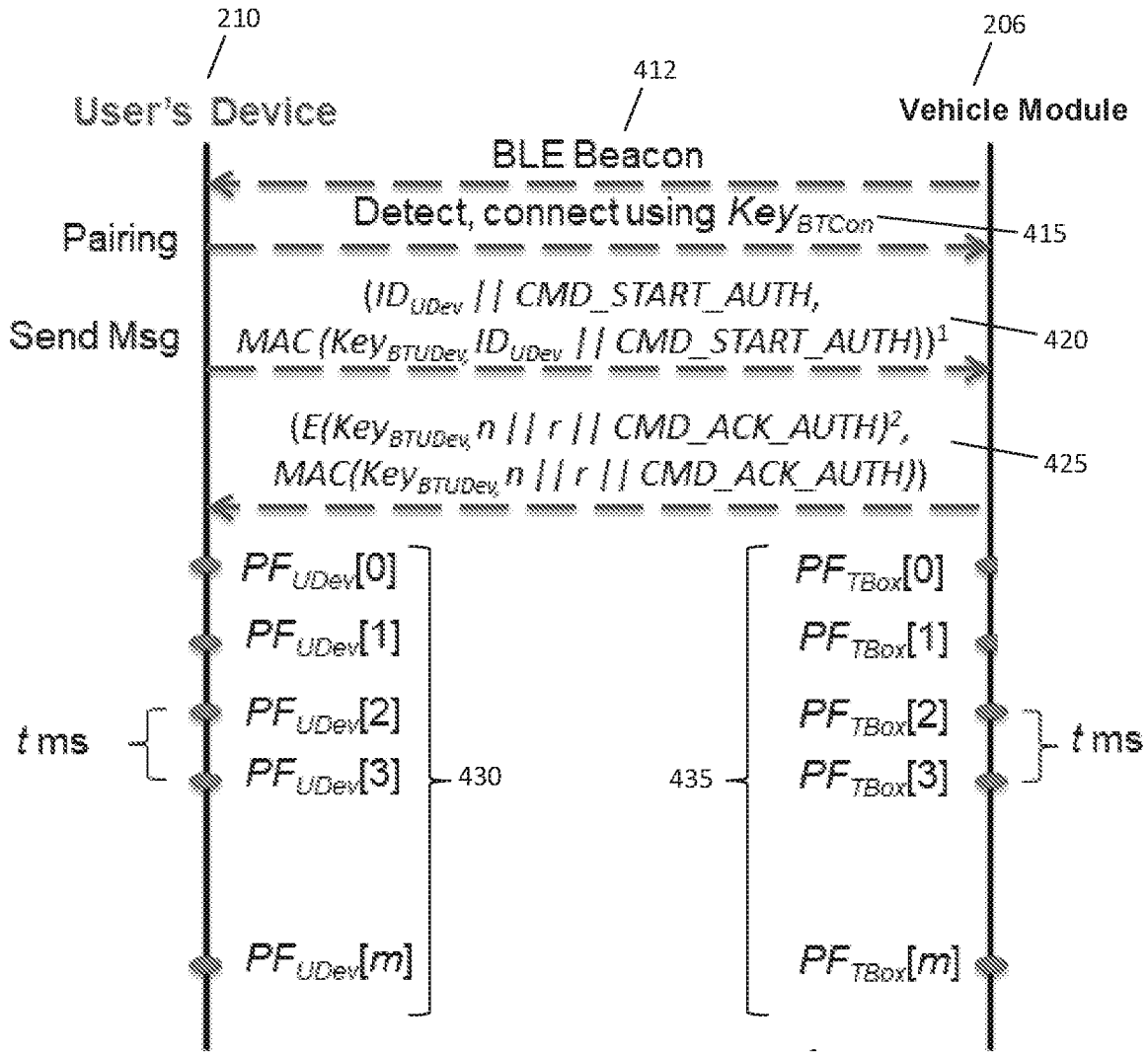
210
User's Device
412
BLE Beacon
206
Vehicle Module
Pairing
Detect, connect using Key_{BTCon}
415
Send Msg
$(ID_{UDev} || CMD\_START\_AUTH, MAC(Key_{BTUDev}, ID_{UDev} || CMD\_START\_AUTH))^1$
420
$(E(Key_{BTUDev}, n || r || CMD\_ACK\_AUTH)^2, MAC(Key_{BTUDev}, n || r || CMD\_ACK\_AUTH))$
425
$PF_{UDev}[0]$
$PF_{UDev}[1]$
$PF_{UDev}[2]$
$PF_{UDev}[3]$
$PF_{UDev}[m]$
t ms
430
$PF_{TBox}[0]$
$PF_{TBox}[1]$
$PF_{TBox}[2]$
$PF_{TBox}[3]$
$PF_{TBox}[m]$
435
t ms

FIGURE 4

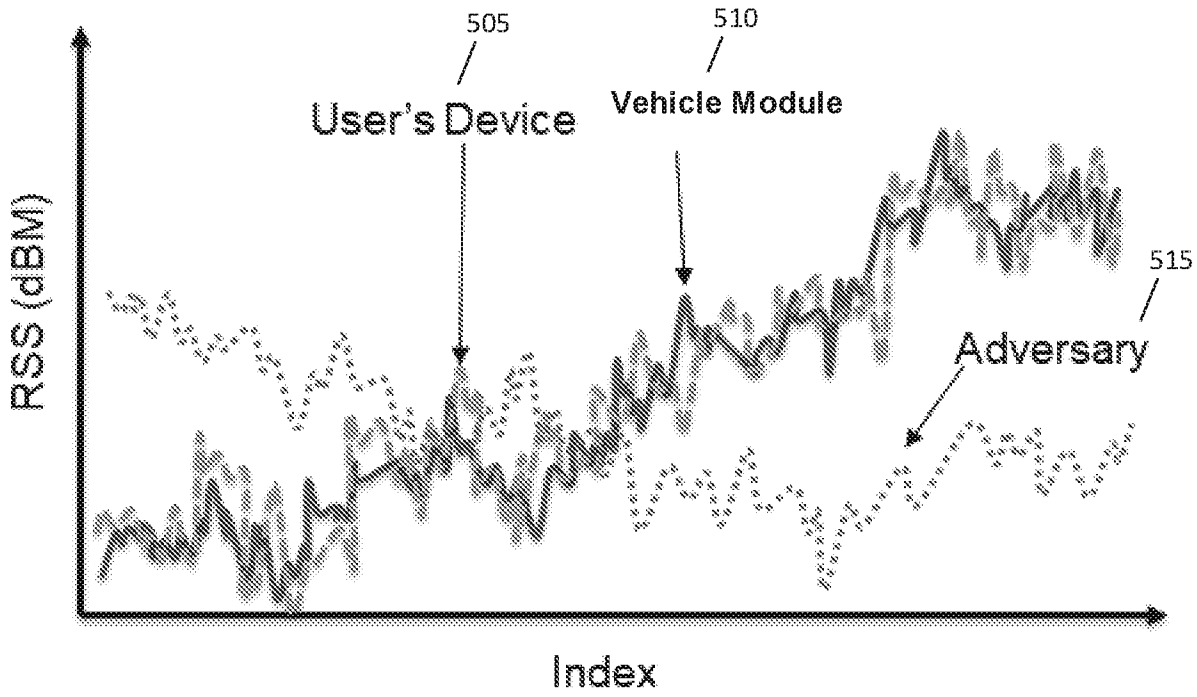

FIGURE 5

FIGURE 6A

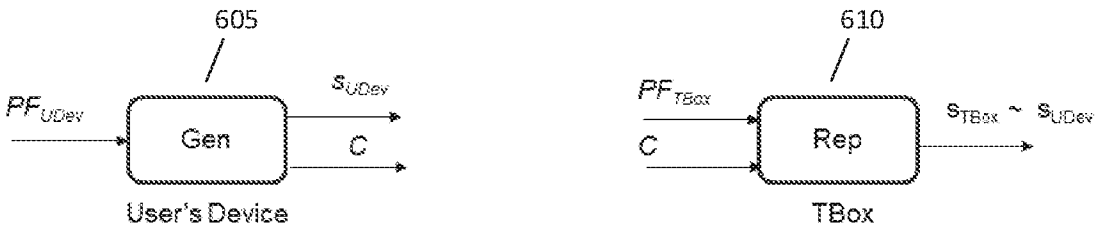

FIGURE 6B

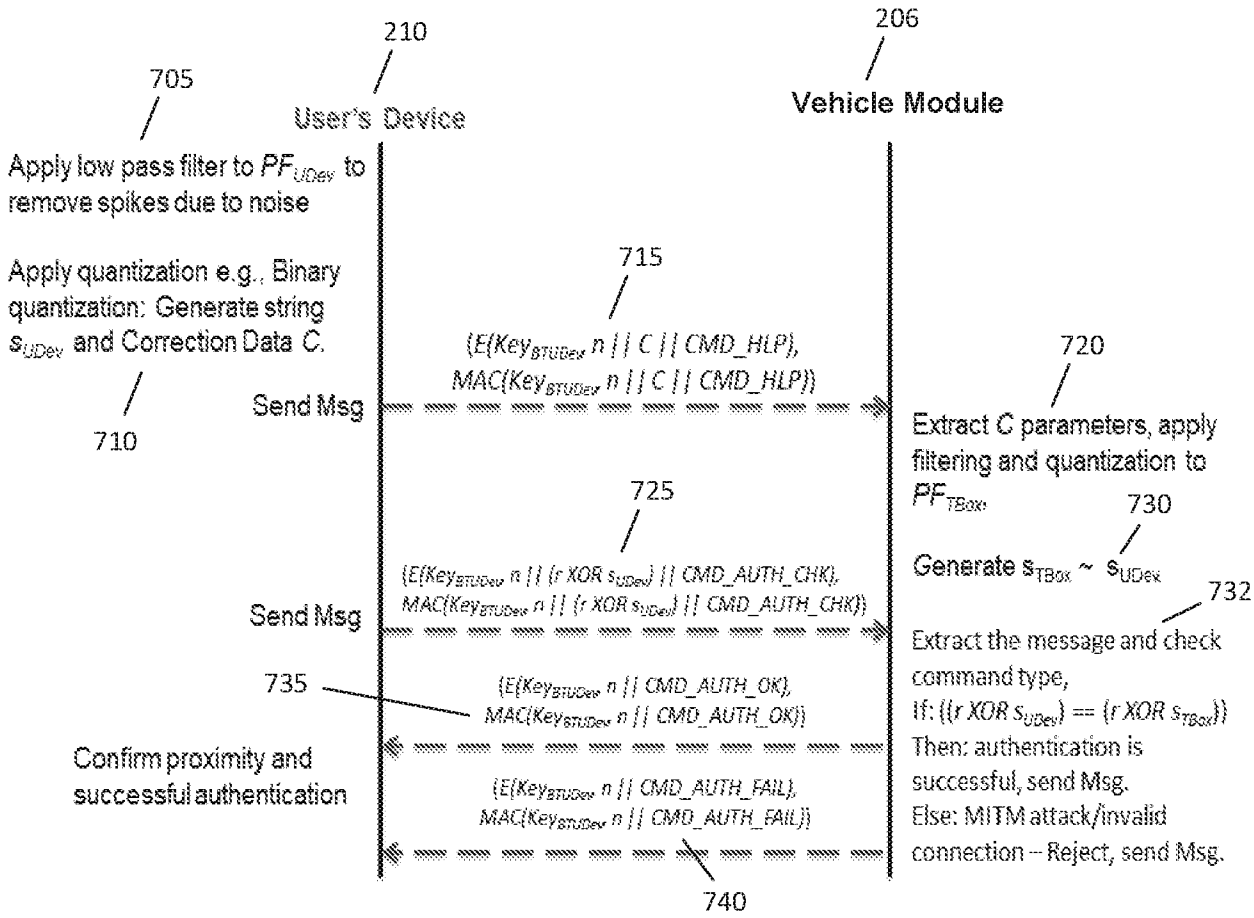
210
206
705
User's Device
Vehicle Module
Apply low pass filter to PF_{UDev} to remove spikes due to noise
Apply quantization e.g., Binary quantization: Generate string s_{UDev} and Correction Data C.
710
715
$(E(Key_{BTUDev}, n \mid\mid C \mid\mid CMD\_HLP), MAC(Key_{BTUDev}, n \mid\mid C \mid\mid CMD\_HLP))$
Send Msg
720
Extract C parameters, apply filtering and quantization to PF_{TBox}
725
730
Generate $s_{TBox} \sim s_{UDev}$
$(E(Key_{BTUDev}, n \mid\mid (r \text{ XOR } s_{UDev}) \mid\mid CMD\_AUTH\_CHK), MAC(Key_{BTUDev}, n \mid\mid (r \text{ XOR } s_{UDev}) \mid\mid CMD\_AUTH\_CHK))$
Send Msg
732
Extract the message and check command type,
If: $((r \text{ XOR } s_{UDev}) == (r \text{ XOR } s_{TBox}))$
Then: authentication is successful, send Msg.
Else: MITM attack/invalid connection – Reject, send Msg.
735
$(E(Key_{BTUDev}, n \mid\mid CMD\_AUTH\_OK), MAC(Key_{BTUDev}, n \mid\mid CMD\_AUTH\_OK))$
Confirm proximity and successful authentication
$(E(Key_{BTUDev}, n \mid\mid CMD\_AUTH\_FAIL), MAC(Key_{BTUDev}, n \mid\mid CMD\_AUTH\_FAIL))$
740

FIGURE 7

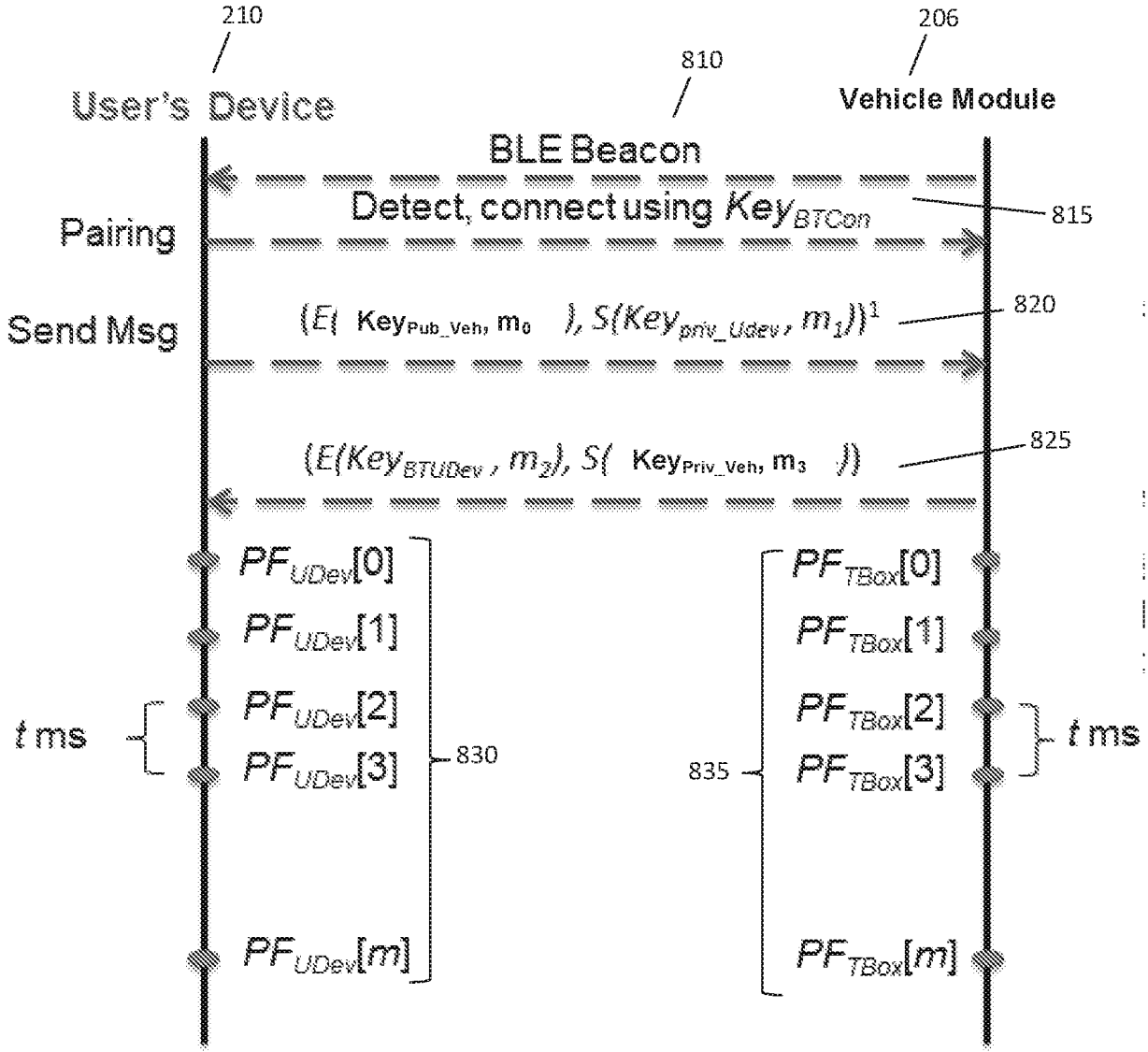
210
206
User's Device
810
Vehicle Module
BLE Beacon
Pairing
Detect, connect using Key_{BTCon}
815
Send Msg
$(E(\ Key_{Pub\_Veh}, m_0\ ), S(Key_{priv\_Udev}, m_1))^1$
820
$(E(Key_{BTUDev}, m_2), S(\ Key_{Priv\_Veh}, m_3\ ))$
825
$PF_{UDev}[0]$
$PF_{UDev}[1]$
$PF_{UDev}[2]$
$PF_{UDev}[3]$
$PF_{UDev}[m]$
t ms
830
$PF_{TBox}[0]$
$PF_{TBox}[1]$
$PF_{TBox}[2]$
$PF_{TBox}[3]$
$PF_{TBox}[m]$
835
t ms

FIGURE 8

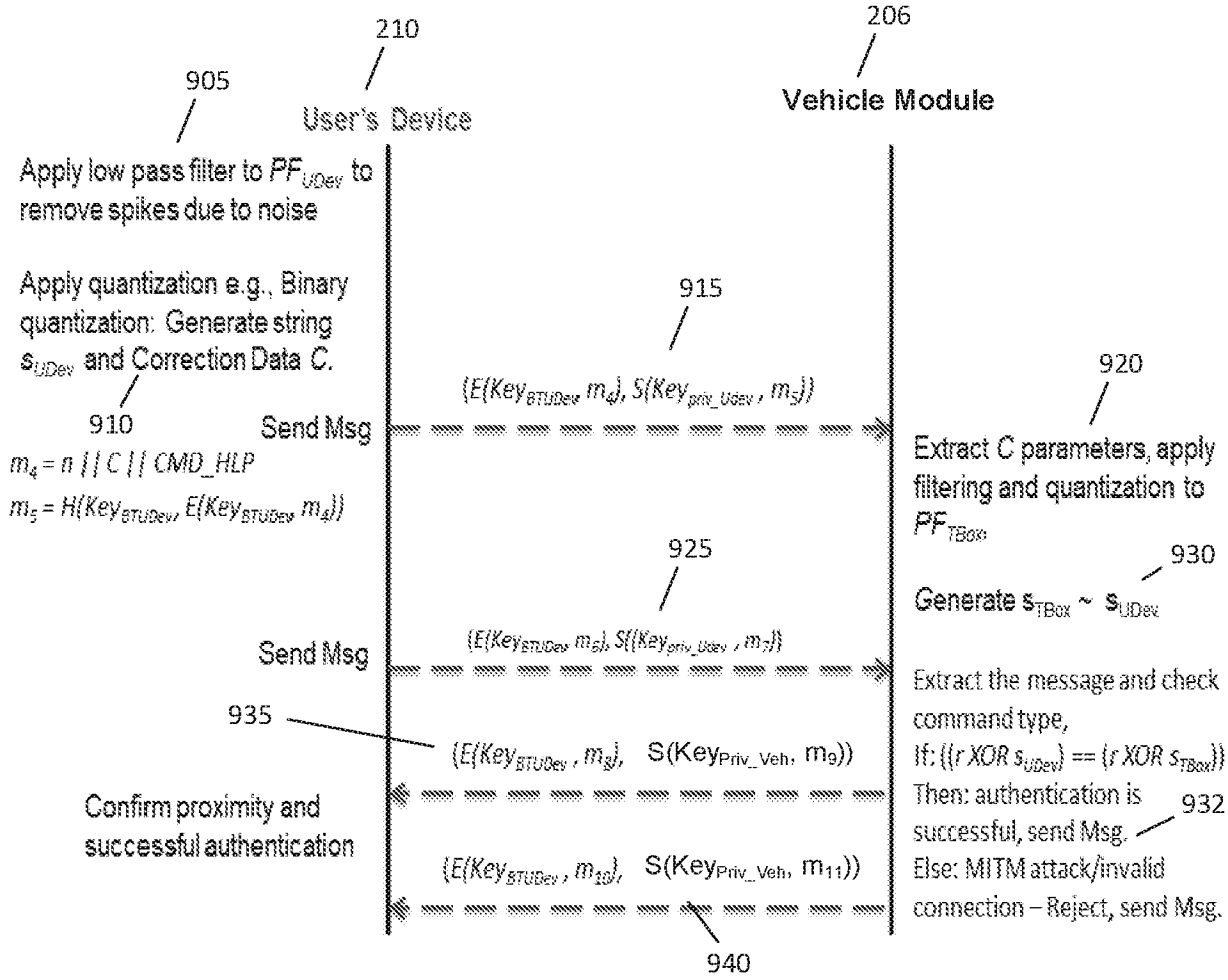
210
206
905
User's Device
Vehicle Module
Apply low pass filter to PF_{UDev} to remove spikes due to noise
Apply quantization e.g., Binary quantization: Generate string s_{UDev} and Correction Data C.
915
$(E(Key_{BTUDev}, m_4), S(Key_{priv\_Udev}, m_5))$
920
910
Send Msg
$m_4 = n \,||\, C \,||\, CMD\_HLP$
$m_5 = H(Key_{BTUDev}, E(Key_{BTUDev}, m_4))$
Extract C parameters, apply filtering and quantization to PF_{TBox}
925
930
Generate $s_{TBox} \sim s_{UDev}$
$(E(Key_{BTUDev}, m_6), S((Key_{priv\_Udev}, m_7))$
Send Msg
Extract the message and check command type,
935
$(E(Key_{BTUDev}, m_8), S(Key_{Priv\_Veh}, m_9))$
If: $((r\ XOR\ s_{UDev}) == (r\ XOR\ s_{TBox}))$
Then: authentication is successful, send Msg.
932
Confirm proximity and successful authentication
$(E(Key_{BTUDev}, m_{10}), S(Key_{Priv\_Veh}, m_{11}))$
Else: MITM attack/invalid connection – Reject, send Msg.
940

FIGURE 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/082911

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/80(2018.01)i; B60R 25/10(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L; B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT,CNKI,WPI,EPODOC:authentication,validate,bluetooth,physical,layer,random,feature,vehicle,car,identity,key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 107995608 A (FEITIAN TECHNOLOGIES CO., LTD.) 04 May 2018 (2018-05-04) description paragraphs [0048]-[0176]	1-32
A	CN 103945373 A (SHANGHAI VOLKSWAGEN AUTO CO., LTD.) 23 July 2014 (2014-07-23) the whole document	1-32
A	CN 107021065 A (HYUNDAI MOBIS CO., LTD.) 08 August 2017 (2017-08-08) the whole document	1-32
A	CN 108092991 A (WEIMA WISDOM TRAVEL TECHNOLOGY SHANGHAI CO., LTD.) 29 May 2018 (2018-05-29) the whole document	1-32
A	CN 105346502 A (KOSTAL SHANGHAI MANAGEMENT CO., LTD. et al.) 24 February 2016 (2016-02-24) the whole document	1-32

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 December 2019	**03 January 2020**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**RAN,Jianguo**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(10)-53961729**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/082911

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107995608	A	04 May 2018	None			
CN	103945373	A	23 July 2014	CN	103945373	B	01 May 2018
CN	107021065	A	08 August 2017	US	2017105120	A1	13 April 2017
				KR	20170041443	A	17 April 2017
				CN	107021065	B	24 September 2019
				DE	102016114234	A1	13 April 2017
CN	108092991	A	29 May 2018	None			
CN	105346502	A	24 February 2016	CN	105346502	B	12 October 2018