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

(11) EP 2 039 583 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.03.2009 Bulletin 2009/13

(51) Int Cl.:
B61L 3/22 *(2006.01)*

(21) Application number: **08252720.1**

(22) Date of filing: **15.08.2008**

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

(30) Priority: **18.09.2007 JP 2007240874**

(71) Applicant: **Hitachi Ltd.**
Chiyoda-ku
Tokyo 100-8280 (JP)

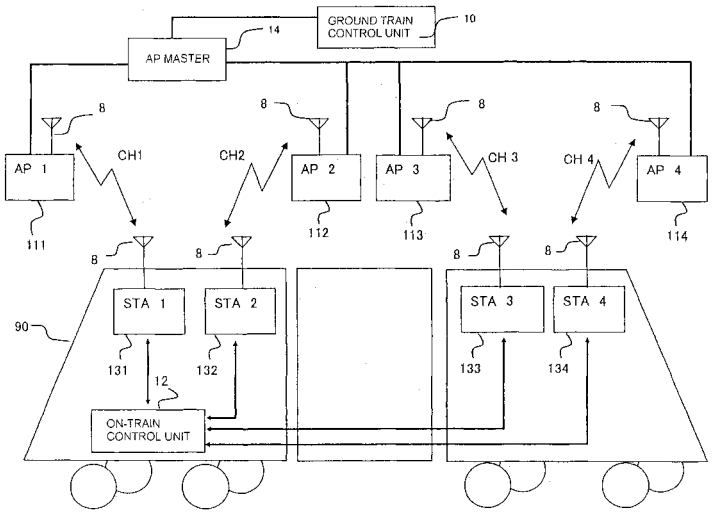
(72) Inventors:
- **Yorishige, Tsuyoshi**
  Tokyo 100-8220 (JP)
- **Nagatsugu, Yoshihide**
  c/o Hitachi,Ltd.Intell Prop. Group
  Tokyo 100-8220 (JP)
- **Sakai, Kenichi,**
  c/o Hitachi,Ltd.Intell.Prop.Group
  Tokyo 100-8220 (JP)
- **Taoka, Hiroshi**
  c/o Hitachi,Ltd. Intell.Prop.group
  Tokyo 100-8220 (JP)

(74) Representative: **Paget, Hugh Charles Edward et al**
Mewburn Ellis LLP
33 Gutter Lane
London
EC2V 8AS (GB)

(54) Railway radio control system

(57) Train control system establishing radio communication between a plurality of on-train radio control apparatuses moving on a predetermined path and a plurality of ground train radio control units disposed along a predetermined path, so as to establish parallel simultaneous radio communications on a plurality of radio communication channels of various communication frequencies between the plurality of on-train radio communication apparatuses and the plurality of ground train radio control units, wherein
one radio communication channel is selected out of the plurality of radio communication channels to perform an authentication request and an authentication process, wherein an encryption key obtained by the authentication process is used as a common encryption key shared by the plurality of on-train radio control units to encrypt data communication between the plurality of on-train radio control units and the plurality of ground train radio control units.

Fig. 1



EP 2 039 583 A1

Description

BACKGROUND OF THE INVENTION

Field of the invention

[0001] The present invention relates to the art of realizing a stable data communication by establishing a plurality of radio communication channels between a train and a communication base station, the art of train control performed via radio and the art of a safe and stable data communication system using a plurality of radio communications that adopt a data encryption system of data transmitted on radio communication channels and a security authentication technique required for entering the radio-controlled zone.

Description of the related art

[0002] Communication systems are utilized to perform train control via a "blocking system" in which only a single train is accepted to travel within a single section.

[0003] Recently, there are demands to cut down costs related to the train communication system by introducing a radio communication system. In the United States and China, a CBTC (Communication Based Train Control) system is being introduced to perform train control via radio communication.

[0004] On the other hand, in Europe, the introduction of a system called ERTMS/ETCS is started. ERTMS/ETCS utilizes GSM-R (GSM-Railway) using a GSM network as the radio communication system.

[0005] In a train control system that realizes bidirectional communication of mutual control information between a ground train control unit of the train and a on-train control unit of the train performing radio control of the train using a radio band, which is an open network, the data is encrypted before radio transmission so as to ensure the confidentiality of data, and the received data is decrypted, thereby protecting the data information from the exterior.

[0006] International publication 98/41435 (patent document 1) discloses a method for controlling the train by transmitting the control information for operating the train safely on a railroad via wire to the train. The disclosure realizes a train control system having a high security extent by providing a radio control unit, a data encryption system and a radio transmitter malfunction detection system for utilizing radio communication for train control.

[0007] Japanese patent application laid-open publication 2006-129432 (patent document 2) discloses a train authentication technique of a train control system using radio communication. The key used for encrypting and decrypting data on the communication channels is determined per each train, which is notified from a ground train control unit through the authentication process of the train. The authentication process is performed at the ground train control unit in response to an authentication request sent from an on-train control unit via an on-train radio control unit. The authentication process is performed with the aim to prevent impersonation access to the whole system. Further, the authentication process is performed at the start up of the train, the entry of the train to the control section and periodically during traveling of the train to update the encryption key, so as to change the encryption pattern of data of the train and to prevent the data from being read from the exterior.

[0008] The arrangement of establishing a plurality of radio communication channels between the on-train control unit of a single train and the ground train control unit is aimed at realizing a stable and continuous data communication between the on-train control unit and the ground train control unit by realizing redundant radio communication channels. This art realizes a highly reliable data communication by providing redundant multiple radio communication channels using multiple CHs, multiple antennas and radio control units under the following radio communication environments: (1) preventing interference bymultipath fading of radio waves withinbuildings in the urban area or within tunnels; (2) preventing interference by noise from other radio communication systems; and (3) change in radio status caused by the movement of the train.

[0009] When the ground train control unit recognizes start up or system entry of the train, the control system must perform an authentication process to notify information such as acceptance to enter system or an encryption key allocated uniquely to each train. If this authentication process must be performed with all the plurality of radio communication channels of a single train, the ground train supervising system must perform a large number of processes determined by the number of trains times the number of radio communication channels, by which the process load becomes excessive.

[0010] The above-mentioned system also has another drawback in that the encryption rules determinedbetween the on-train control unit and the ground train control unit by the authentication process must be set to correspond to the number of radio communication channels per a single train, and the processing load related to data communication becomes excessive.

[0011] The object of providing redundant radio communication channels is as mentioned earlier. According to the present system configuration in which the defection of data is prevented since other radio communication channels are connected even if one radio communication channel is disconnected, some radio communication channels may not be able to perform the authentication process at the time of initial start up of the train according for example to the position of the train, the environment of the radio or the apparatus status of the radio control unit. Such radio communication channel may recover its connection by the movement of the train. If the authentication process is to be performed after the connection has recovered, there will be two types of radio communication channels connected, the radio communication

channel for performing data communication for train control anda radio communication channel for performing authentication process, and since the processing mode of the ground train control unit differs for each of the radio communication channels for a single train, the process performed by the ground train control unit becomes too complex.

SUMMARY OF THE INVENTION

[0012] The object of the present invention is to provide a train control system having redundant data communication channels using a plurality of radio communication channels using difference channels (CH) between the on-train control unit and the ground train control unit so as to prevent disconnection of communication of control data in the bidirectional radio communication between the on-train control unit and the ground train control unit in a train control system, wherein each of the radio communication channels are made effective as safe and stable data communication channels.

[0013] The present invention provides a train control system establishing radio communication between a plurality of on-train radio control apparatuses moving on a predetermined track and a plurality of ground train radio control units disposed along a predetermined track, so as to establish parallel simultaneous radio communications on a plurality of radio communication channels of various communication frequencies between the plurality of on-train radio communication apparatuses and the plurality of ground train radio control units, characterized in that one radio communication channel is selected out of the plurality of radio communication channels to perform an authentication request and an authentication process, wherein an encryption key obtained by the authentication process is used as a common encryption key shared by the plurality of on-train radio control units to encrypt data communication between the plurality of on-train radio control units and the plurality of ground train radio control units.

[0014] The present invention also characterizes in that the authentication request and the authentication process required at the time of entry of the on-train radio control unit to the train control system or at the initial start up of the on-train radio control unit are performed by switching the selected radio communication channels.

[0015] The present invention also characterizes in that a supervising system of the on-train radio control unit for selecting a single radio communication channel and performing the authentication request generates a random number for the authentication process, and hands over the random number to only the radio communication channel for performing the authentication request and the authentication process.

[0016] The present invention further characterizes in that the data on the plurality of radio communication channels are encrypted using an encryption key generated by a ground train supervising system and notified via the ground train radio control unit to the on-train radio control unit, wherein the encryption key is notified from the ground train radio control unit while performing authentication of a single radio communication channel, and the supervising system of the ground train radio control unit shares the encryption key with other on-train radio control units to be used for encrypting data sent via other radio communication channels that have not performed authentication, so that the data sent on all the plurality of radio communication channels established between the on-train radio control units and the ground train radio control units can be encrypted.

[0017] The present invention also characterizes in that the supervising system of the on-train radio control unit observes the status of radio waves of a plurality of radio communication channels and the status of apparatuses of the on-train radio control units, so as to determine a single radio communication channel for performing the authentication process and to start the authentication process.

[0018] The present invention further characterizes in that the train control system is equipped with an authentication retry function in which if the authentication process is not completed within a certain period of time or if radio communication is disconnected during the authentication process, the authentication process is discontinued and terminated, then the supervising system selects another radio communication channel to restart the authentication process, so as to switch the radio communication channel to retry the authentication request and the authentication process.

[0019] The present invention also characterizes in that when the authentication is completed via a single radio communication channel, data communication of the on-train radio control unit within the train control system is accepted, and the supervising system of the on-train radio control apparatus shares the authentication completion information and the encryption key with other radio communication channels, so that the data communication on the remaining radio communication channels are also accepted and started, by which the data communication of the train control system is activated.

[0020] According to the present invention, data is communicated via a plurality of radio communication channels between the on-train control unit of a single train and the ground train control unit so as to ensure the redundancy of data communication, and a secure and appropriate authentication is performed by executing a security authentication between the on-train and ground train control units using one of the plurality of radio communication channels. Further, by sharing the encryption key obtained by the authentication process with other radio communication channels to start data communication, the security of data sent via the redundant radio communication channels can be guaranteed effectively.

[0021] Further according to the present invention, the authentication process is performed via only one radio communication channel, so that compared to the system

in which all the radio communication channels must perform the authenticationprocess, the loadof authenticating a single train is very small. This is also effective from the viewpoint of reducing load of the ground train control unit that controls the plurality of trains traveling on one railroad track.

[0022] Further according to the present invention, the authentication request and the authentication process required during initial start up of the on-train radio control unit or the entry of the on-train radio control unit to the train control system is performed by switching the selected radio communication channels, so that even if the radio communication status or the status of the radio transmitter or the antenna is not good, the authentication process can be performed by switching to another radio communication channel, so that the plurality of radio communication channels can be performed effectively under a condition in which the authentication process is required.

[0023] Moreover, according to the present invention, the supervising system of the on-train radio control unit for selecting a single radio communication channel and executing the authentication request generates random numbers for the authentication process, and hands over the random number only to the radio communication channel that performs the authentication request and the authentication process, so that the authentication request and the authentication process can be performed effectively only by the supervising system and the radio communication channel performing the authentication process.

[0024] Further according to the present invention, the data on the plurality of radio communication channels is encrypted using an encryption key generated by the ground train supervising system and notified via the round-based radio control unit to the on-train radio control unit. The encryption key is notified from the ground train radio control unit upon performing authentication on a single radio communication channel, and the supervising system of the ground train radio control unit demands the on-train radio control unit to share the encryption key for encrypting data with other radio communication channels that have not performed authentication. Thereby, the data on all the plurality of radio communication channels between the on-train radio control unit and the ground train radio control unit can be encrypted, so that compared to the system where all the radio communication channels must perform the authentication process, the authentication process is restricted to a single radio communication channel, the load for performing the authentication process of a single train can be reduced, and the load applied to the ground train control unit that controls the plurality of trains traveling on one railroad track can be reduced.

[0025] Further according to the present invention, the radio wave status of the plurality of radio communication channels and the apparatus status of the on-train radio control unit is monitored by the supervising system of the on-train radio control unit, and by determining the single radio communication channel for performing the authentication process and starting the authentication process, the radio wave status of the plurality of radio communication channels and the apparatus status of the on-train radio control unit can be monitored efficiently, and the authentication process can be started efficiently, compared to the system in which a plurality of on-train radio control units monitor the status respectively.

[0026] The present invention can further be equipped with an authentication retry function that disconnects and terminates the authentication process if the authentication process is not completed within a certain period of time or if the radio communication is disconnected during the authentication process, and selects another radio communication channel to retry the authentication process by the supervising system so as to switch the radio communication channel for retrying the authentication request and the authentication process. Thus, even if the radio communication status or the radio transmitter/antenna status is not good, the radio communication can be switched to another radio communication channel to execute the authentication process, and the plurality of radio communication channels can be used effectively in a state where the authentication process is required.

[0027] Further according to the present invention, when the authentication process is completed via a single radio communication channel, data communication of the on-train radio control unit in the train control system is accepted, and the supervising system of the on-train radio control unit shares the authentication completion information and the encryption key with other radio communication channels, so that data communication via the remaining radio communication channels is also accepted and started, and the data communication of the train control system can be started. Thereby, the security of data encryption of the radio communication channels not having performed the authentication process is also ensured. In other words, all the data on the plurality of radio communication channels between the ground train control unit and a single train is protected by the same encryption key as the authentication process, and the present invention enables to overcome the drawback of the prior art having to distribute different encryption keys and increasing the decryption process load of the ground train control unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028]

FIG. 1 is a system configuration diagram illustrating the on-train and ground-based systems according to embodiment 1 of the present invention;

FIG. 2 is a flow chart of data communication of radio communication channels according to embodiment 1 of the present invention;

FIG. 3 is a chart of the flow during authentication

process of apparatuses according to embodiment 1 of the present invention; and

FIG. 4 is a flow chart of the data communication during the authentication process on the radio communication channel according to embodiment 1 of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0029] Now, we will describe the preferred embodiments of the present invention.

[0030] According to a representative preferred embodiment of the present invention, the data sent on the radio communication channels are encrypted for confidentiality. The plurality of radio communication channels formed between a single train and a ground train control unit use the same encryption key to encrypt the same control data, so that identical information are transmitted via the respective radio communication channels. There are a plurality of communication channels established between the ground train control unit and a single train, but since the same control data are encrypted using the same encryption key, the data sent via the plurality of radio communication paths will be the same. By adopting a system in which a radio communication channel preferentially used for data is set in advance, and when the radio communication path is disconnected or when an invalid data is received, the data sent via another radio communication channel is used for control, it becomes possible to prevent the transmission and reception of data, train control and train administration data sent via the plurality of radio communication channels from becoming extremely long and complicated.

[0031] An authentication process is performed to prevent impersonation access from the exterior of the system to the radio transmission channels. Through the authentication process, the encryption key generated by the ground train control unit is notified to the on-train control unit. When starting up the train, when entering the system, and each time when the encryption key is updated periodically while the train is moving, the authentication process is performed between the train and the ground train control unit.

[0032] The authentication process recognizes the authentication request from the train via the radio communication path, and determines whether or not to accept access of the train to the system. When access is accepted, an encryption key used for encrypting the data on the radio communication channel is notified to the train. If authentication requests are sent via each of the plurality of radio communication channels between the ground train control unit and a single train, the ground train control unit must receive a large number of authentication requests corresponding to the number of radio communication channels to authenticate only a single train, so that when it is necessary to authenticate multiple trains, the process to be performed at the ground train control unit will become too complex and the load will become excessive. By restricting the number of radio communication channels subjected to authentication-processtoone, and having only one authentication request for a single radio communication channel to be output per a single train, the process load of the ground train control unit can be reduced.

[0033] There is a possibility that data communication on the radio communication channel cannot be performed such as due to radio wave interference caused by noise, differences in radio wave property due to installation positions of the antennas, the distance between the ground base station, the malfunction of the radio communication control unit or the antenna, and so on. The present system corresponds to such data communication malfunction by establishing a plurality of radio communication channels.

[0034] Though the authentication process is performed on a single radio communication channel, if the above-mentioned problems causing defective data communication occurs and the radio communication control unit cannot perform the authentication process, switching among the plurality of radio communication channels is performed for example by the following processes:

(A) If the authentication process is not completed within a fixed period of time, the on-train control unit switches the authentication process/ authentication request to another radio communication system.

(B) The on-train control unit designates the radio communication channel for performing the authentication process by recognizing the data communication statuses such as the apparatus status of the radio communication control unit and the status of the radio communication.

[0035] According to a representative embodiment of the present invention, data communication is performed via a plurality of radio communication channels established between the on-train control unit of a single train and the ground train control unit, so as to ensure the redundancy of data communication. Further, by executing a security authentication between the on-train and ground train control units using a single radio communication channel out of the plurality of radio communication channels, it becomes possible to perform a secure and appropriate authentication effectively, and by sharing the encryption key obtained in the security authentication process with other radio communication channels when data communication is started, security of data can be guaranteed in the redundant radio communication channels.

[0036] The authentication process performed when starting up the train, when entering the system and when updating the encryption key is performed by selecting one of the plurality of radio communication paths, so that even if the radio communication status or the statuses of the radio transmitter or the antenna is not good, the

authentication process can be performed by switching to another radio communication channel, so that the plurality of radio transmission channels can be used effectively in such a state where authentication process is necessary.

[0037] Compared to the case where the authentication process is performed for all the radio communication channels, the present system restricts the authentication process to be performed by only a single radio communication channel, so that the load of the authentication process is very small. Therefore, the load on the ground train control unit that controls the large number of trains on a single track can be effectively reduced.

[0038] When an authentication process is performed for all the plurality of radio communication channels, the channels will have various different encryption keys, and the load of the decryption process by the ground train control unit becomes excessive. However, according to the present invention in which the train is authenticated using a single radio communication channel, the encryption key obtained via the authentication process by the on-train control unit is distributed and shared with other on-train control units, so that the data encryption of the radio communication channels that did not perform authentication process will also be security-ensured. In other words, all the data communicated on the plurality of radio communication channels between the ground train control unit and a single train are protected by the same encryption key as that used in the authentication process.

[0039] Now, the preferred embodiment of the present invention will be described in detail with reference to the drawings.

[Embodiment 1]

[0040] FIG. 1 is a diagram showing the on-train and ground train control units according to embodiment 1 of the present invention. In FIG. 1, the ground-based facilities include a ground train control unit 10 that generates information to a train 90 accompanying the bidirectional data communication with the train 90, and a ground train radio communication apparatus AP 111 for realizing radio communication (hereinafter referred to as ground train radio control apparatus: AP). A supervising system AP master 14 of the plurality of ground train radio control units that exist along the railroad tracks is arranged between the ground train control unit 10 and the AP 111.

[0041] In FIG. 1, an on-train control unit 12 functioning as the supervising system of the train 90 and an on-train radio control unit STA 131 for performing radio communication (hereinafter referred to as on-train radio control unit: STA) are provided as the train-based facilities. According to the present embodiments, four STAs, STA 131, STA 132, STA 133 and STA 134 are disposed on a train 90, with four radio communication channels formed between the on-train control unit 12 and the ground train control unit 10. Here, each STA has established radio communication channels with the AP 111, AP 112, AP 113 and AP 114.

[0042] The respective radio communication channels use different channels (CH), and when the on-train radio control units STA 131, STA 132, STA 133 and STA 134 each having an antenna 8 communicate with the base-stations AP 111, AP 112, AP 113 and AP 114 having different installationenvironments and each having an antenna 8, the environments of the radio communication channels are set to be varied, so that when the radio transmission path is disconnected due to radio wave environment or the status of operation of the on-train radio communication system STA, the data from another on-train radio communication system STA is used for processing data of the on-train control unit 12.

[0043] FIG. 2 is a data communication flow chart of the radio communication channel according to embodiment 1 of the present invention. In FIG. 2, the train 90 communicates data with the ground-based facility. The information that the ground train control unit 10 wishes to send to a single train is at first transmitted to the AP master 14. The information having been subjected to encryption process in the AP master 14 is then send to each of the APs 111 through 114. Each AP 111 through 114 transmits the encrypted train control information to each STA 131 through 134 having established radio communication, respectively, and each STA 131 through 134 having received the data sends the decrypted data to the on-train control unit 12.

[0044] When data is to be sent from the train 90 to the ground, the on-train control unit 12 hands over the data that must be sent to the ground to each STA 131 through 134. Each STA 131 through 13 encrypts the data and sends the data to each AP 111 through 114 having established radio communication channels. The AP 111 through 114 notifies the received data to the AP master 14, and the AP master 14 decrypts the data. The decrypted data from the on-train control unit 12 is notified from the AP master 14 to the ground train control unit 10.

[0045] The on-train control unit 12 usually uses data from a single STA for control, but if data reception error such as the missing of data or missing of data update occurs, or if data disconnection of the radio communication channel occurs, the data received by other STA are used for control. This redundancy of radio communication channels enables to prevent data from the ground train control unit 10 from being discontinued.

[0046] The radio communication channels are open networks, so that the data must be encrypted to ensure confidentiality of the data. The encryption key required for the encryption is generated by the ground train control unit 10 per each train 90, and during the authentication process performed during start up of the train or the system entry of the train, the key is handed over from the ground train control unit 10 to the on-train control unit 12.

[0047] FIG. 3 is a flowchart showing the authentication process performed among the various apparatuses according to embodiment 1 of the present invention. At first, the on-train control unit 12 generates a random number.

The on-train control unit 12 selects an STA 13 for performing authentication, and outputs an authentication request by handing over the generated random number. The STA 13 transmits the random number to the AP master 14 via a radio communication channel. The AP master 14 encrypts the random number using an authentication key shared in advance by the STA 13 and the AP master 14. The data is sent to the STA 13, and the STA 13 decrypts the same. Once more, the STA 13 receives the random number again from the on-train control unit 12 that had been received previously, and compares the same with the random number that had been encrypted and decrypted using the authentication key so as to confirm that they match.

[0048] Next, the ground train control unit 10 generates a random number. The ground train control unit 10 hands over the generated random number to the AP master 14. The AP master 14 transmits the random number to the STA 13 using AP 11 having a secured radio communication channel that is performing authentication process. The STA 13 encrypts the random number using an authentication key shared in advance by the STA 13 and the AP master 14. The data is sent to the AP master 14, and the AP master 14 decrypts the same. Once more, theAPmaster 14 receives the random number again from the ground train control unit 10 that had been received previously, and compares the same with the random number that had been encrypted and decrypted using the authentication key, so as to confirm that they match.

[0049] Once the matching of the random numbers is confirmed by the two sets of random number encryption-decryption sequences mentioned above, the authentication is completed, and the ground train control unit 10 encrypts the encryption key determined uniquely for each train, which is notified to the on-train control unit 12 via the radio communication channel established between the AP master 14 and the STA 13.

[0050] The on-train control unit 12 subjects the encryption key received at the time of completion of authentication to a sharing process to share the same with other STAs not subjected to the authentication process, and then notifies that the authentication has completed. Thereby, radio communication using all four STAs is started.

[0051] FIG. 4 is a data communication flow chart illustrating the authentication process performed using radio communication channels according to embodiment 1 of the present invention. In FIG. 4, STA 131 is performing the authentication process. The authentication process is performed using a single radio communication channel 41 via the process shown in FIG. 3. When the authentication process is not completed within a certain period of time, if the radio communication status is deteriorated during the procedure, or if the STA 131 malfunctions, the on-train control unit 12 performs an discontinuation-termination process of the authentication process, and outputs an authentication process request to STA 132 so as to switch the STA performing the authentication process. This arrangement constitutes an authentication retry function.

[0052] The encryption key notified from the ground train control unit 10 through the authentication process is shared via the on-train control unit 12 with other STAs 132, 133 and 134. Thus, all the radio communication channels have completed the authentication process and are able to communicate data using the distributed encryption key, so that the data communication of all four radio communication channels are protected from interception from the exterior.

[0053] The authentication is performed using a single wire communication channel and single STA. If the authentication is not completed within a certain period of time and the authentication key is not notified to the on-train control unit 12, the system is equipped with a retry function to perform an authentication discontinuation-termination process so as to switch the authentication request to another STA to retry the authentication.

[0054] According to the above-described system of the present invention, even if only a single radio communication channel is used to perform authentication and the radio communication status is deteriorated or the STA malfunctions, the authentication process can be performed by switching the STA used for authentication.

[0055] If the present invention is not applied and the authentication process must be performed for each of the plurality of radio communication channels, the authentication process must be performed for four times per a single train, and the process load of the AP master 14 and the ground train control unit 10 becomes excessive.

[0056] Further, if the present invention is not applied and the radio communication status of the target radio communication channel is not good so that authentication process cannot be performed, data communication cannot be performed until the radio communication status is improved. In such case, the on-train control unit 12 must perform an authentication process corresponding to the radio communication status in addition to performing the train control based on the communicated data, and the performance load of the system becomes excessive.

[0057] By applying the train control unit according to embodiment 1 of the present invention to perform the authentication process using an STA administering a single radio communication channel and share the encryption key obtained through the authentication process with other STAs administering other radio communication channels, the STAs not having performed the authentication process can also share the encryption key to perform encryption anddecryptionofdata. Thus, even in STAs not having established radio communication during the authentication process can share the encryption key after the authentication of a single STA has completed, so that when radio communication has been established while the train is moving, encrypted data can be communicated immediately.

[0058] The present invention is applicable to signaling systems for moving vehicles such as railway cars, monorails and light rail transits (LRT). The present invention is applicable not only to railway cars, but also to systems aimed at performing highly reliable transmission on an open network by adopting redundant data communication using a plurality of radio communication channels.

Claims

1. A train control system establishing radio communication between a plurality of on-train radio control apparatuses moving on a predetermined path and a plurality of ground train radio control units disposed along a predetermined path, so as to establish parallel simultaneous radio communications on a plurality of radio communication channels of various communication frequencies between the plurality of on-train radio communication apparatuses and the plurality of ground train radio control units, **characterized in that**
one radio communication channel is selected out of the plurality of radio communication channels to perform an authentication request and an authentication process, wherein an encryption key obtained by the authentication process is used as a common encryption key shared by the plurality of on-train radio control units to encrypt data communication between the plurality of on-train radio control units and the plurality of ground train radio control units.

2. The train control system according to claim 1, wherein the authentication request and the authentication process required at the time of entry of the on-train radio control unit to the train control system or at the initial start up of the on-train radio control unit are performed by switching the selected radio communication channels.

3. The train control system according to claim 2, wherein a supervising system of the on-train radio control unit for selecting a single radio communication channel and performing the authentication request generates a random number for the authentication process, and hands over the random number to only the radio communication channel for performing the authentication request and the authentication process.

4. The train control system according to claim 2, wherein the data on the plurality of radio communication channels are encrypted using an encryption key generated by a ground train supervising system and notified via the ground train radio control unit to the on-train radio control unit, wherein the encryption key is notified from the ground train radio control unit while performing authentication of a single radio communication channel, and the supervising system of the ground train radio control unit shares the encryption key with other on-train radio control units to be used for encrypting data sent on other radio communication channels that have not performed authentication, so that the data sent on all the plurality of radio communication channels established between the on-train radio control units and the ground train radio control units can be encrypted.

5. The train control system according to claim 1 or claim 2, wherein the supervising system of the on-train radio control unit observes the status of radio waves of a plurality of radio communication channels and the status of apparatuses of the on-train radio control units, so as to determine a single radio communication channel for performing the authentication process and to start the authentication process.

6. The train control system according to claim 5, wherein the train control system is equipped with an authentication retry function in which if the authentication process is not completed within a certain period of time or if video communication is disconnected during the authentication process, the authentication process is discontinued and terminated, then the supervising system selects another radio communication channel to restart the authentication process, so as to switch the radio communication channel to retry the authentication request and the authentication process.

7. The train control system according to claim 5, wherein when the authentication is completed via a single radio communication channel, data communication of the on-train radio control unit within the train control system is accepted, and the supervising system of the on-train radio control apparatus shares the authentication completion information and the encryption key with other radio communication channels, so that the data communication on the remaining radio communication channels are also accepted and started, by which the data communication of the train control system is activated.

Fig. 1

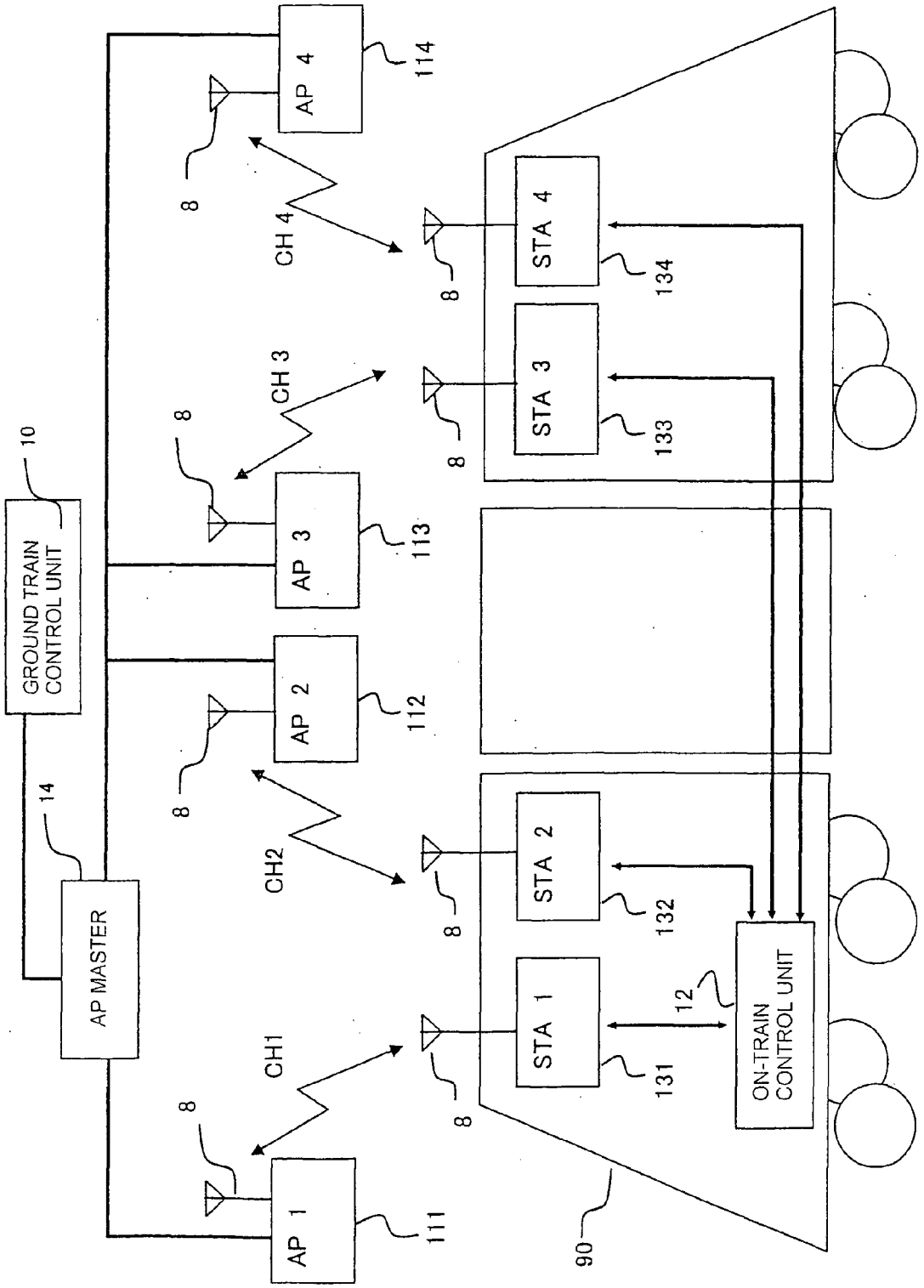

GROUND TRAIN CONTROL UNIT
10
AP MASTER
14
AP 1
111
AP 2
112
AP 3
113
AP 4
114
CH1
CH2
CH 3
CH 4
8
STA 1
131
STA 2
132
STA 3
133
STA 4
134
12
ON-TRAIN CONTROL UNIT
90

Fig. 2

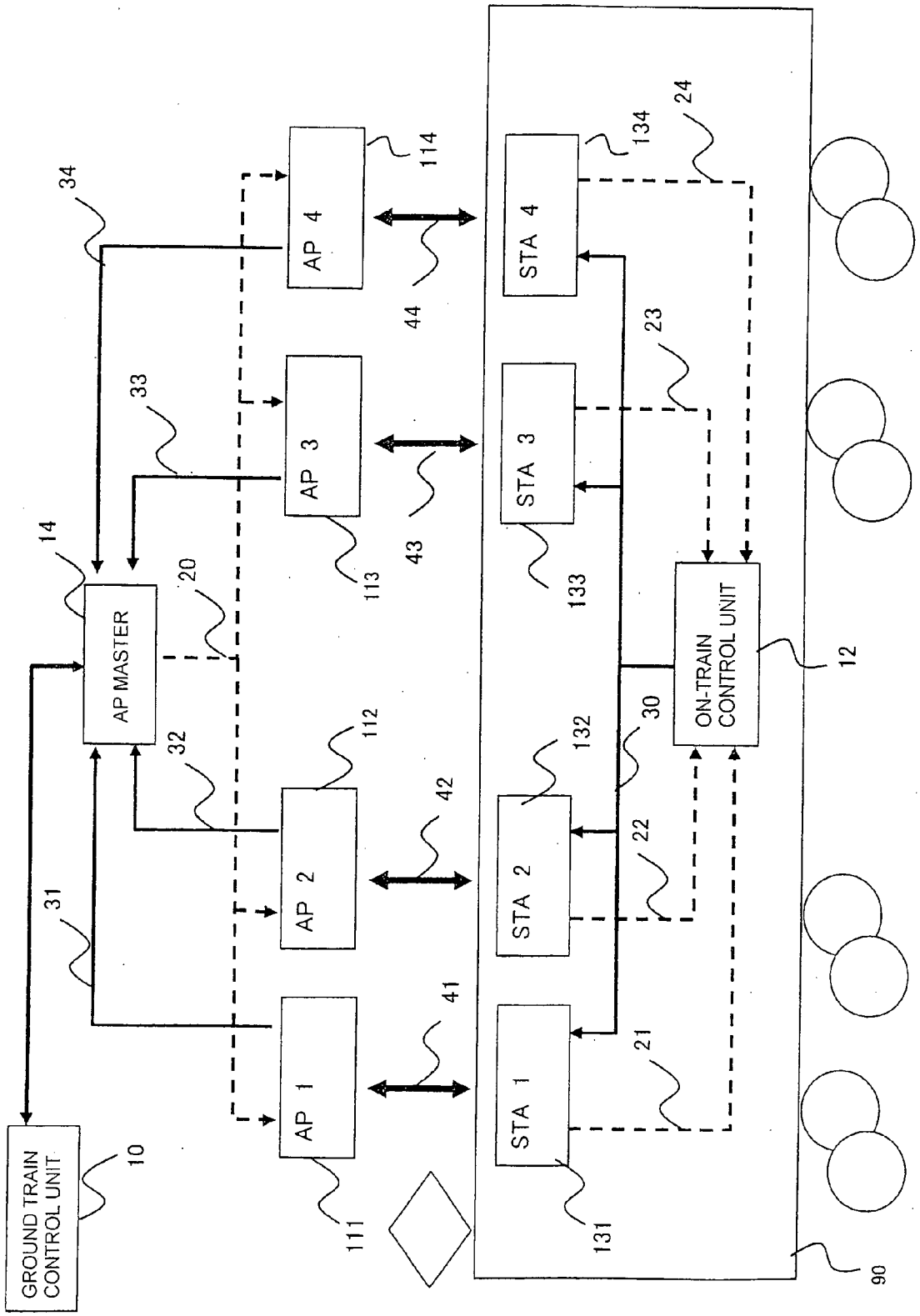

GROUND TRAIN CONTROL UNIT
10
AP MASTER
14
20
AP 1
AP 2
AP 3
AP 4
111
112
113
114
31
32
33
34
41
42
43
44
STA 1
STA 2
STA 3
STA 4
131
132
133
134
21
22
23
24
30
ON-TRAIN CONTROL UNIT
12
90

Fig. 3

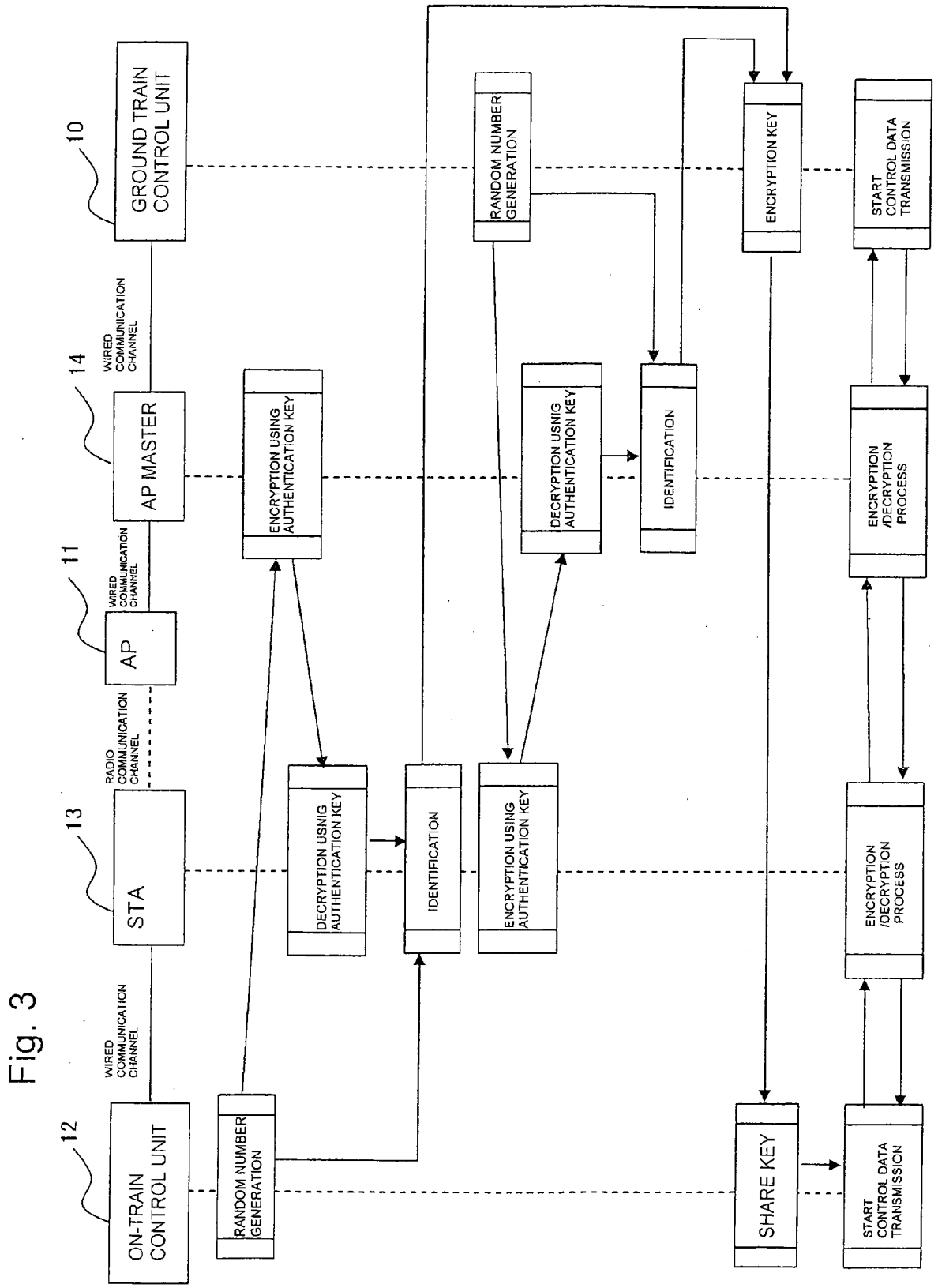
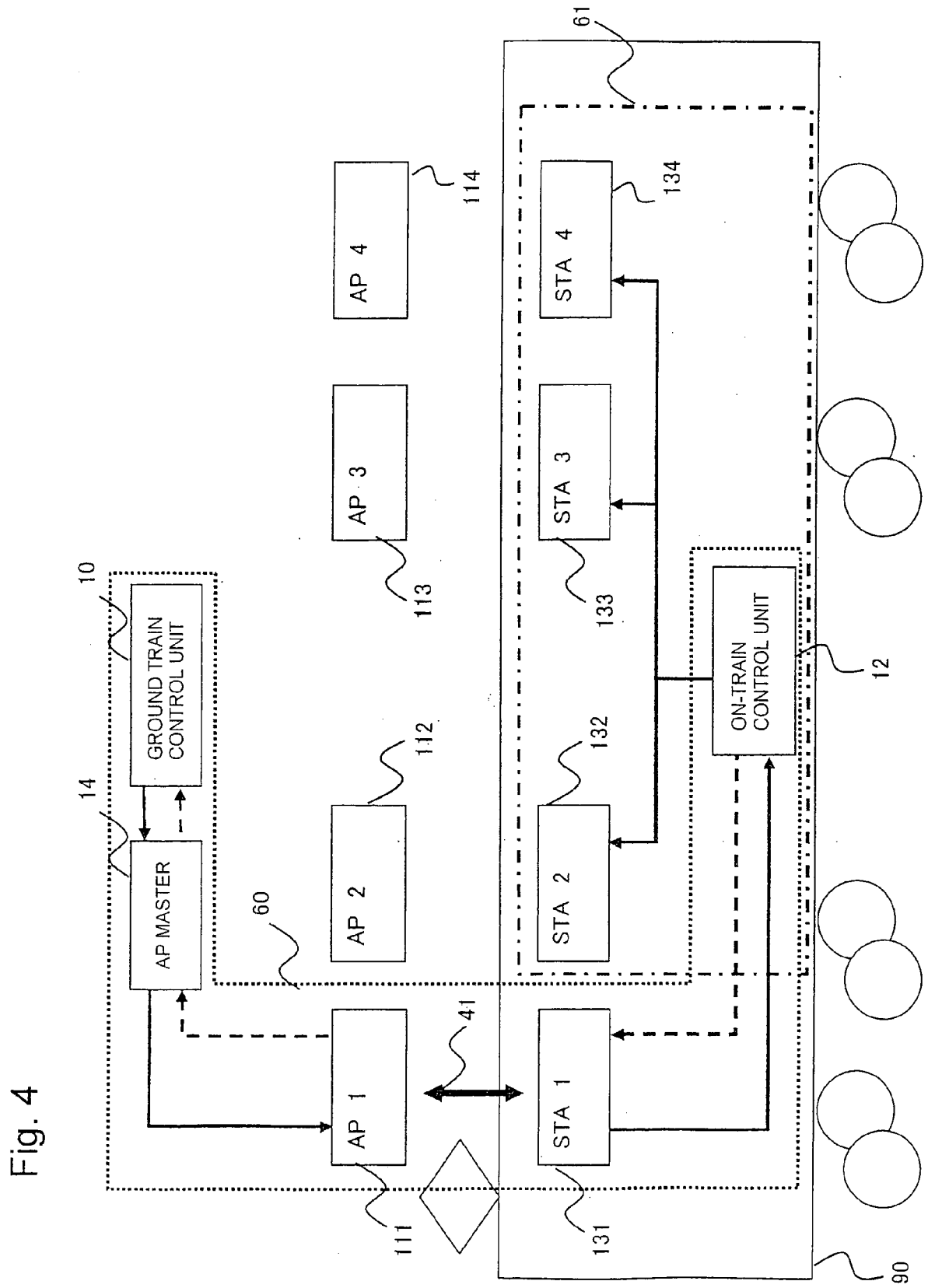

GROUND TRAIN CONTROL UNIT
10
WIRED COMMUNICATION CHANNEL
AP MASTER
14
WIRED COMMUNICATION CHANNEL
AP
11
RADIO COMMUNICATION CHANNEL
STA
13
WIRED COMMUNICATION CHANNEL
ON-TRAIN CONTROL UNIT
12
RANDOM NUMBER GENERATION
ENCRYPTION USING AUTHENTICATION KEY
DECRYPTION USNIG AUTHENTICATION KEY
IDENTIFICATION
ENCRYPTION USING AUTHENTICATION KEY
DECRYPTION USNIG AUTHENTICATION KEY
IDENTIFICATION
RANDOM NUMBER GENERATION
ENCRYPTION KEY
SHARE KEY
START CONTROL DATA TRANSMISSION
ENCRYPTION /DECRYPTION PROCESS
ENCRYPTION /DECRYPTION PROCESS
START CONTROL DATA TRANSMISSION

Fig. 4


GROUND TRAIN CONTROL UNIT
AP MASTER
AP 1
AP 2
AP 3
AP 4
STA 1
STA 2
STA 3
STA 4
ON-TRAIN CONTROL UNIT
10
12
14
41
60
61
90
111
112
113
114
131
132
133
134

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 08 25 2720

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
D,A	JP 2006 129432 A (HITACHI LTD) 18 May 2006 (2006-05-18) * paragraphs [0104], [0105]; figures 13,14 *		INV. B61L3/22 H04W12/04 H04B7/02
A	EP 0 970 868 A (HITACHI LTD [JP]) 12 January 2000 (2000-01-12)		
D,A	& WO 98/41435 A (HITACHI LTD [JP]; YOKOSUKA YASUSHI [JP]; MAEKAWA KEIJI [JP]; KAWABATA) 24 September 1998 (1998-09-24)		
A	DE 43 10 644 A1 (DEUTSCHE AEROSPACE [DE]) 6 October 1994 (1994-10-06) * figure 1 *		
A	US 2007/028099 A1 (ENTIN LEONID [IL] ET AL) 1 February 2007 (2007-02-01) * paragraphs [0009], [0027] *		
			TECHNICAL FIELDS SEARCHED (IPC)
			B61L H04Q H04W H04B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Berlin	21 November 2008	Kampouris, Alexandre

CATEGORY OF CITED DOCUMENTS

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

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

& : member of the same patent family, corresponding document

2

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 25 2720

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

21-11-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2006129432 A	18-05-2006	NONE	
EP 0970868 A	12-01-2000	CN 1508036 A	30-06-2004
		WO 9841435 A1	24-09-1998
		JP 3269635 B2	25-03-2002
WO 9841435 A	24-09-1998	CN 1508036 A	30-06-2004
		EP 0970868 A1	12-01-2000
		JP 3269635 B2	25-03-2002
DE 4310644 A1	06-10-1994	EP 0621701 A1	26-10-1994
		ES 2160109 T3	01-11-2001
US 2007028099 A1	01-02-2007	EP 1668814 A1	14-06-2006
		WO 2005025122 A1	17-03-2005

EPO FORM P0459

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

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- JP 10041435 A **[0006]**
- JP 2006129432 A **[0007]**