

⑫

EUROPEAN PATENT APPLICATION

⑳ Application number: **85401239.0**

⑤① Int. Cl.⁴: **H 04 K 1/00**

㉔ Date of filing: **21.06.85**

③① Priority: **29.06.84 US 625885**

④③ Date of publication of application:
08.01.86 Bulletin 86/2

⑧④ Designated Contracting States:
CH DE FR GB IT LI NL SE

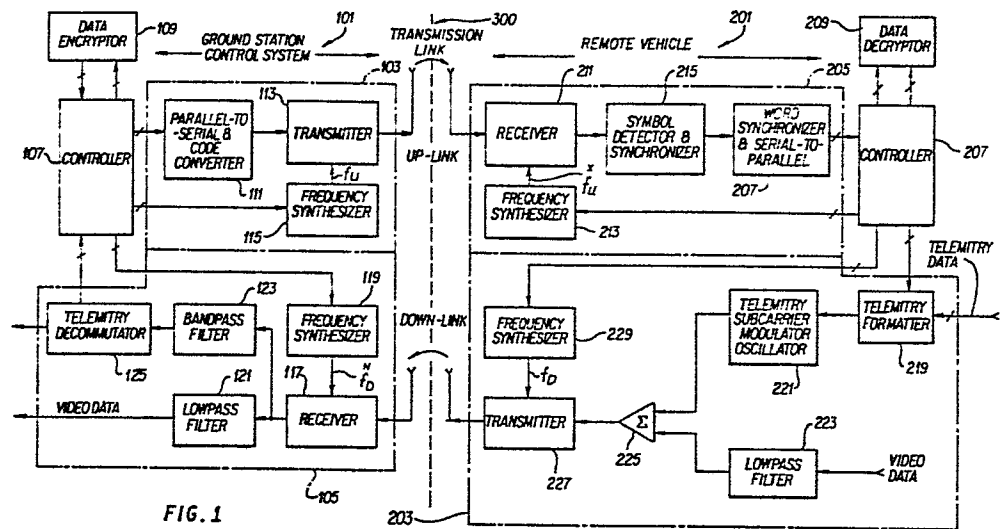
⑦① Applicant: **FAIRCHILD WESTON SYSTEMS INC.**
Fruitville & Packinghouse Roads
Sarasota Florida 33578(US)

⑦② Inventor: **Waggener, William N.**
2507 Espanola Avenue
Sarasota Florida 33579(US)

⑦④ Representative: **Chareyron, Lucien**
Schlumberger Limited Service Brevets c/o Giers 12, place
des Etats Unis B.P. 121
F-92124 Montrouge Cédex(FR)

⑤④ **Secure communication system.**

⑤⑦ A jam resistant, low-cost data link, wherein short burst messages are frequency-hopped on a message-by-message basis. The data link includes a transmitter and a receiver which initially are set at a common, predetermined frequency. The message transmitted during each burst includes encrypted data identifying the frequency at which the next message will be transmitted to enable the receiver to tune to that frequency. If the initial transmission is jammed, the transmitter and receiver are preprogrammed to change to a preset back-up frequency. The receiver will request retransmission before the next transmission frequency is changed if a received message is garbled.



|
SECURE COMMUNICATION SYSTEMBackground of the Invention1. Field of the Invention

5 The present invention relates to the field of secure data communication systems, and more particularly to such a system employing frequency-hopping techniques and encrypted data.

2. Description of the Prior Art

10 Various types of communications techniques are employed in order to ensure the security of the information being transmitted and to make such communications more resistant to intentional jamming or noise. For example, in a spread-spectrum communications system an initial narrow-band information signal is modulated with a pseudo-random code sequence having noise-like
15 properties which spreads the original narrow-band signal over a much larger bandwidth and at reduced amplitude. Assuming that both a transmitter and a receiver utilize the same pseudo-random sequence, detection and decoding of the information of the spread signal is simply a matter of synchronizing the pseudo-random code
20 generators of both the transmitter and receiver to the same initial bit position of the pseudo-random sequence. Such a spread-spectrum communication system offers good data security since a third party who wishes to decode the transmission would have to have in his possession the pseudo-random bit sequence and
25 would have to properly synchronize the sequence with that of the transmitter. In addition, such a system is inherently resistant to jamming, since the information borne by the spread-spectrum signal is spread out over a relatively wide band of frequencies. Thus, an attempt to jam such a signal by utilizing a high power
30 signal of relatively narrow bandwidth would merely degrade somewhat the reception of the broadband information signal and slightly increase the probability of errors in decoding the

signal. Alternatively, broadband jamming can be used to completely swamp the relatively low amplitude spread-spectrum signal. However, this is at the cost of having to employ a large number of powerful transmitters in order to broadcast enough energy over a broad enough bandwidth to ensure adequate jamming. In addition, such broadband jamming techniques can be relatively easily overcome simply by moving the fundamental carrier frequency of the transmitted information signal to an area not covered by the broadband jamming system. Also, such broadband systems tend to be relatively easy to detect and locate, thus subjecting them to conventional attack or electronic countermeasures.

A second type of secure data communication system utilizes a so-called "frequency-hopping" technique. In a frequency-hopping system, information is transmitted and received on frequencies which are frequently changed or "hopped". The frequency-hopping pattern is normally predetermined and built into the transmitter and receiver. The pattern can be generated in various ways, such as through the use of pseudo-random number generators in both the transmitter and receiver which, once synchronized to a particular initial frequency, will thereafter change frequencies in tandem with one another.

Data encryption is frequently employed in frequency-hopping systems in order to prevent unwanted reception of the data being transmitted. Further, it is known to transmit the messages in short bursts followed by a change in frequency to make it more difficult to jam the transmitted signal. This is because the burst transmitted signal will have a much higher effective signal-to-noise ratio, for a given amount of transmitted power, than a continuous tone-jamming signal would have of comparable power.

One drawback to current frequency-hopping systems is that although the hopping pattern is intended to be random, it is actually a deterministic pattern which can be derived by someone who observes the pattern of transmissions over a sufficiently long time period. The pattern can also be easily determined if a transmitter or receiver is captured and the frequency-hopping

pattern generator is subjected to study.

In addition, the transmitter and receiver in such a system must be initially synchronized to the beginning of the frequency-hopping pattern before each series of transmissions. If such synchronization does not occur (due, for example, to intentional jamming or noise), then the transmission of information from the transmitter to the receiver cannot take place.

Summary of the Invention

It is a general object of the invention to provide an improved method and apparatus for secure communications.

This and other objects are attained, in accordance with one aspect of the invention by a method of secure communications utilizing frequency-hopping and having at least a transmitter and a receiver, said method preventing intentional jamming and comprising the steps of: (a) generating at the transmitter an information signal including at least a portion representative of the frequency of transmission of the next informational signal; (b) transmitting the information signal at a transmission frequency determined by the frequency representative portion of an immediately preceding transmitted information signal; and (c) receiving the information signal at the receiver at a frequency determined by the frequency representative portion of the immediately preceding received information signal.

Another aspect includes a secure communications apparatus of the frequency-hopping type comprising: a transmitter including means for generating an information signal including at least a portion representative of the frequency of transmission of the next information signal, and means for transmitting the information signal at a transmission frequency determined by the frequency representative portion of an immediately preceding transmitted information signal; and a receiver for receiving the information signal, including means for tuning the receiver to a frequency determined by the frequency representative portion of the immediately preceding received information signal.

Brief Description of the Drawing Figures

5 These and other features and advantages of the present invention will be clear from the following detailed description of the preferred embodiment, when taken in conjunction with the drawing figures wherein:

 Figure 1 is a block diagram of a secure data communication system arranged in accordance with the present invention; and

10 Figure 2 shows diagrammatically a typical information signal as used in the present invention;

 Figure 3 shows diagrammatically the transmission of a series of information signals, such as shown in Figure 2, in accordance with the present invention; and

15 Figure 4 is a flow chart illustrating the operation of the secure data communication system of the present invention.

20
Detailed Description of the Preferred Embodiment

25 With reference to Figure 1, there is shown a block diagram of a secure communication system which utilizes the techniques of the present invention. The communication system comprises a pair of transceivers 101 and 201, each including a transmitter section 103
30 and 203, respectively, and a receiver section 105 and 205, respectively.

Both transceivers 101 and 201 include controllers 107 and 207, respectively. Each controller 107 or 207 may include or comprise a microprocessor and associated memory and input/output (I/O) circuits.

5 Controller 107 is in communication with a data encryptor 109 while controller 207 is in communication with a data decryptor 209. The function of data encryptor 109 and data decryptor 209 are explained below.

10 In one exemplary embodiment, the invention is designed to be used to enable communication between transceivers 101 and 201 to take place in a secure fashion, including a high resistance to jamming or noise which may occur over a transmission link 300. Transmission link 300 may, for example, be a radio link, fiber optic link, telephone link, etc.

15 For example, transceiver 101 may be set up as a ground based control system for controlling a remote vehicle (e.g. a pilotless surveillance aircraft) which includes transceiver 201. The transmission link 300 is a radio link. Transmitter section 103 is designed to transmit control signals via an up-link portion of
20 transmission link 300 to receiver section 205 of the remote vehicle. The pilotless vehicle includes various sensors and/or optical systems for observing a predetermined area. These sensors and/or imaging devices (not shown) feed telemetry and/or video signals into the transmitter section 203 for broadcast back to
25 transceiver 101 at the ground station via a down-link portion of transmission link 300. Receiver section 105 of transceiver 101 receives these down-link signals and further processes them or displays them. The up-link and down-link transmission frequencies may be either the same or different from each other.

30 The transmitter section 103 of transceiver 101 and receiver section 205 of transceiver 201 which communicate over the up-link portion of transmission link 300 utilize a burst-mode frequency-hopping technique in order to reduce susceptibility to portions of the broadcast spectrum which may be particularly noisy or where intentional jamming signals are present. To this end, control signals and other data or information are transmitted as

digital signals over the up-link by transmitter section 103 and are received by receiver section 205. As shown in Figure 2, a typical information signal 301 includes an initial preamble 303 of, for example, 128 bits, with the bit pattern chosen to enhance the ability of the receiver to establish symbol synchronization. When a differential bi-phase code is employed, for instance, an all "zero" pattern might be used. The purpose of the preamble bits is to enable a receiver to synchronize and lock on to the signal. Following the preamble is a short series of bits 305 (e.g. 24 bits) for frame synchronization purposes. The frame synchronization bits may be one of many different patterns such as those specified by the Interange Instrumentation Group (IRIG). The frame synch bits are utilized by a receiver to indicate the beginning of a message or a series of digital bytes or words.

Following the frame synch pattern are a series of bits 307 defining the actual message. The message bits may be of any predetermined number (e.g. 256 bits or thirty-two eight-bit bytes). The message data can include such things as control signals for steering the remote vehicle, signals for activating or turning off certain surveillance sensors, etc.

An important feature of the present invention is that at least a portion of the transmitted message 307 includes a word which is representative of the frequency on which the next information signal will be broadcast. This information is used by the receiver in the remote vehicle, as more fully explained below, to enable it to retune the receiver in order to receive the next message transmission at the new frequency.

The information signal may further include a series of parity check bits 309 (e.g. 16 bits) which, as explained more fully below, enable the receiver in the remote vehicle to determine whether it has correctly received a particular information signal. It is to be understood that the above arrangement of information signal 301 and the particular bit lengths and patterns employed are merely exemplary and may be suitably changed to other values or arrangements in accordance with a user's particular needs.

A second important feature of the invention is that at least the word representative of the next transmission frequency is encrypted, and preferably the entire sequence of message bits 307 is encrypted. Data encryption is performed by data encryptor 109 which can use any one of a number of well-known techniques for encrypting the message portion of the information signal. For example, the National Bureau of Standard's Data Encryption Standard (DES), as described in Federal Information Processing Standard Publication No. 46 January 1977, may be used. By employing the DES, the security of the message being transmitted by transmitter section 103 to receiver section 205 is relatively high, especially in view of the fact that only a few seconds will go by before the next transmission, at a different frequency, takes place.

Since the word representative of the next frequency of transmission is also encrypted it would be highly unlikely that someone would be tuned in to the proper frequency to receive the up-link transmission, and then also be able to decode it quickly enough in order to know which frequency the next data transmission would take place. Thus, someone who wished to eavesdrop on the up-link transmission or intentionally jam such transmission would have a very difficult time in doing so. Further, since the frequency-hopping pattern is determined only at the ground station (transceiver 101) there is no loss in security if the remote vehicle should fall into the possession of an unauthorized person. This is because the frequency-hopping pattern generated by controller 107 can be changed periodically and in a random fashion.

In addition, transceiver 205, which is situated in the remote vehicle, may include sensors for detecting the spectrum of any jamming signals which may be applied to either the up-link or down-link portions of transmission link 300. This spectral information for the jamming signals may be sent back to receiver section 105 of the ground station by transmitter section 203 of the remote vehicle over the down-link. This information can then be assimilated by controller 107 and used to change the

frequency-hopping pattern employed by transmitter section 103 in order to minimize the effects of such jamming signals on its transmission. The down-link information transmitted by transmitter section 203 of transceiver 201 to receiver section 105 of transceiver 101 may employ the same encryption and message format as employed in the up-link signal.

To further enhance the security of transmission of the information signals, each signal 301, such as shown in Figure 2, is sent as a short burst with a relatively long delay between each such burst, as shown in Figure 3. For example, if each information signal is 424 bits long and transmitted at approximately 20 kilobits per second, the duration T1 of information signal 301 will be approximately 21 milliseconds. As shown in Figure 3, the time T2 between each such information signal transmission is greater than the length of the information signal transmission itself, and preferably is much greater than the duration T1 of a single information signal transmission. Generally, sufficient time is allotted between each burst transmission to enable a receiver to check for errors in the transmission of the information signal and to perform the decryption process on at least the word representative of the next frequency of transmission. In the example given, this period of time is on the order of 3-4 seconds. While such a time period is adequate to enable error detection and decryption of the frequency representative word to take place, is much too short a time for another party, who does not have the decryption key, to decode the encrypted word representative of the next transmission frequency. Therefore, such an unauthorized party would not be able to decrypt the frequency representative word quickly enough to know what the next transmission frequency will be in order to retune his receiver to receive the next message.

In addition, the burst-mode of transmission makes it more difficult for an unauthorized third party to utilize radio-location techniques to home in on and locate and/or destroy either the ground station or remote vehicle. A further advantage of the burst-mode of message transmission is that each message is

effectively transmitted at a higher peak power due to the short duration of each transmission. This enables relatively low power components to be utilized and makes the transmitted signal more difficult to jam using broadband jamming techniques, since the jammer will need to employ a much higher average power across a much larger bandwidth in order to be assured of blanking out the burst-mode transmitted message.

Referring back to Figure 1, the operation of transceivers 101 and 201 will now be explained in more detail. Initially, instructions or other messages or information in a format similar to that shown in Figure 2 are generated by controller 107. Controller 107 is, for example, a microprocessor including a certain amount of random access memory (RAM) and read only memory (ROM), such as the 8085 processor sold by the Intel Corporation. The message generated by controller 107, either under program control or by input from an operator (not shown), is applied to data encryptor unit 109. Data encryptor 109 may implement any one of a number of well-known data encryption algorithms. For example, the Data Encryption Standard promulgated by the National Bureau of Standards is one such high-security encryption algorithm. One advantage to using the Data Encryption Standard is that there are available standard integrated circuit chips which perform the data encryption and data decryption functions. One such chip is the Intel 8294 data encryption unit.

After the message has been encrypted, it is returned to controller 107 for further processing and then output to transmitter section 103 of transceiver 101.

Transmitter 103 includes a parallel-to-serial and code converter unit 111 which takes the output of controller 107 (which is in parallel form) and converts it into a serial bit-stream for application to transmitter unit 113. The code converter portion of unit 111 changes the standard binary output of controller 107 into a differential bi-phase code for application to transmitter 113. A differential bi-phase code is one in which, for example, a "1" is represented by a change in phase from the previously transmitted signal while a "0" is represented by no change in

phase. Although other types of encoding schemes can be used, differential bi-phase coding has the advantage of being self-clocking and therefore does not require a separate synchronization signal.

5 The data signal applied to transmitter 113 is then used to modulate a carrier signal at a predetermined frequency using standard frequency shift keying (FSK) techniques. The particular frequency of transmission is determined by frequency synthesizer 115 whose setting, in turn, is determined by controller 107.
10 Frequency synthesizer 115 preferably is capable of being programmed to select from a large number of transmission frequencies to enable the transmitted messages to be frequency-hopped over a wide enough range so as to avoid most types of narrow-band jamming.

15 As mentioned earlier, each information signal 301 is sent as an individual unit in a short burst transmission. For example, if the data rate output by unit 111 is 20 kilobits per second, and assuming an information signal containing approximately 424 bits of data, then the length of transmission of an individual
20 information signal will be approximately 21 milliseconds. The exact timing of when the information signal is transmitted is under control of controller 107, as is the period of silence T2 (no transmission) between each information signal. These pauses in data transmission are designed to be just long enough for
25 receiver section 205 of transceiver 201 to detect the transmitted signal, check it for errors, and to decrypt the message contained therein.

30 The encrypted FSK signal 301 is then sent over transmission link 300 via the up-link section as shown in Figure 1. This up-link may be a radio communications channel, a fiber optics communication link, telephone line, or other such communications channel.

 After remote vehicle receiver section 205 of transceiver 201 receives the encrypted FSK signal it is processed for utilization by controller 207.

The incoming information signal 301 is first applied to receiver unit 211 whose reception frequency is controlled by frequency synthesizer 213. Frequency synthesizer 213 is in turn controlled by controller 207. Receiver unit 211 demodulates the received information signal and applies the demodulated signal to symbol detector and synchronizer unit 215. Symbol detector and synchronizer unit 215 operates in a well-known manner to detect preamble 303 of the information signal 301 (see Figure 2) and to synchronize a voltage-controlled oscillator (VCO) of a phase-locked loop (PLL), which are part of unit 215, to the symbol rate of the bits of the information signal. Once the received bits are detected and the phase-locked loop has been locked to the symbol rate of the bits of the information signal, the serial bit-stream is applied to word synchronizer and serial-to-parallel converter unit 217. Unit 217 operates in a well-known fashion to detect frame synchronization bits 305 (see Figure 2) of each information signal to produce a signal alerting controller 207 that the start of the message portion 307 of the information signal has been located. The serial data stream is then converted into parallel blocks (e.g. 8 bits wide) for application to controller 207.

Controller 207 is similar in structure to controller 107 and includes a microprocessor and both RAM and ROM memories. Controller 207 may further have stored in its memory one of a number of well-known error detection and/or error correction algorithms for determining whether the message portion of the information signal has been properly received. For example, simple error detection can be provided by inspecting the parity bits 309 appended to the end of each information signal and comparing them with the detected pattern of data bits in the encrypted message portion 307 of the information signal. Error correction can be provided by initially inserting a pattern of error correcting bits into the encrypted message portion 307 prior to transmission by transmitter section 103. For example, a code of the BCH (30, 25) type or Reed-Solomon encoding may be used.

If controller 207 detects an error in the received data message portion, or if the message is not received at all during a predetermined time period, an error signal is generated by controller 207 and applied to transmitter section 203 of the remote vehicle. It should be noted that error detection takes place prior to data decryption. This is because data decryption is a relatively slow process, whereas error detection can be performed within as little as a few microseconds after reception of the information signal using suitable hardware. This enables controller 207 to determine whether it has properly received message portion 307 of the information signal and to request retransmission immediately without bothering with data decryption.

If the received message is error free, controller 207 applies encrypted message portion 307 of the information signal 301 to data decryptor 209. Data decryptor 209 performs data decryption in accordance with the particular data encryption algorithm employed. Once decrypted, the information signal is returned to controller 207 for further processing. It should be noted that one portion of the decrypted message contains a word representative of the frequency of transmission of the next information signal to be transmitted from the ground station. Controller 207 then uses this frequency representative word to control the frequency selected by frequency synthesizer 213 which, in turn, is used to retune receiver 211 to the frequency the next information signal is to be transmitted on.

Thus it can be seen that information signal 301 transmitted by transmitter section 103 to receiver section 205 contains all the data necessary for receiver section 205 to know what the next transmission frequency will be. Unlike prior-art frequency-hopping systems, this means that receiver section 205 of the remote vehicle does not have to know ahead of time what the frequency-hopping pattern will be. This makes the design of the remote vehicle receiver section 205 simpler and enhances the security of the overall communication system since, if by some misfortune the remote vehicle were to fall into unwanted hands, there is nothing contained in its circuitry which would enable

someone to know what the frequency-hopping pattern is. This is because the frequency hopping pattern is generated solely by controller 107 at the ground station.

Although not essential to the basic operation of the invention, Figure 1 shows some additional elements for transmitting information from transmitter section 203 of the remote vehicle via the down-link portion of transmission link 300 to receiver section 105 of the ground station. Preferably, this down-link information includes signals indicative of the non-receipt or the erroneous receipt of a signal transmitted over the up-link portion, or an acknowledgment signal indicating that the signal transmitted over the up-link has been properly received. The error and acknowledgment signals are generated by controller 207 in response to the proper receipt or the non-receipt/improper receipt of the up-link information signal.

The acknowledgment or error signal is applied to telemetry formatter unit 219 which may also receive other telemetry data from sensors in the remote vehicle (not shown). If the remote vehicle is, for example, a pilotless observation aircraft, the telemetry data can be indicative of altitude, speed, camera angle, etc. The telemetry data can also include spectral information concerning the distribution of noise and/or jamming signals over the transmission link 300.

The acknowledge/error signals and other telemetry signals are then applied to a telemetry subcarrier modulator/oscillator 221. In addition, if visual observations are being made by a video camera (not shown) the video signal can be applied to a low-pass filter unit 223 whose output, along with the output of the telemetry subcarrier modulator/oscillator 221, is summed in summing device 225 and then applied to transmitter unit 227. The frequency of transmission of the down-link signal output by transmitter 227 is selected by frequency synthesizer 229 which, in turn, is controlled by controller 207. The down-link transmission frequency may be periodically changed, in a fashion similar to that employed with respect to the up-link frequency, in order to enhance the security of the down-link signal. Although no data

encryption is shown for use with the down-link signal, transmitter section 203 of the remote vehicle obviously can be modified to include data encryption of the telemetry and/or video signals, along with message-by-message frequency-hopping as is utilized with the up-link transmitter section 103.

5 The telemetry and/or video signals are sent over the down-link portion of transmission link 300 and are received and processed by receiver section 105 of the ground station. Receiver section 105 includes a receiver unit 117 which receives the down-link signal at a frequency determined by frequency synthesizer 119. Frequency synthesizer 119 tunes receiver 117 to a frequency determined by controller 107.

10 Receiver 117 demodulates the down-link signal and passes it to a low-pass filter 121 and a band-pass filter 123. The output of low-pass filter 121 contains video data information which may then be supplied to a display device, such as a TV monitor (not shown). The output of band-pass filter 123 contains telemetry information which is then applied to telemetry decommutator unit 125. The output of telemetry decommutator unit 125 is applied to controller 107 and may also be applied to instruments or other visual displays (not shown) for observation or other action by an operator. The telemetry information applied to controller 107 may be used to modify a subsequent information signal which will be transmitted over the up-link portion of transmission link 300.

15 It will be appreciated that controllers 107 and 207 may contain preprogrammed instructions relating to the operation and movement of the remote vehicle. Further, both controllers 107 and 207 are preprogrammed to try transmission and reception on an initial predetermined frequency to initiate communication. If communication cannot be established within a preselected number of attempts, then both controllers 107 and 207 are preprogrammed to begin trying a predetermined series of one or more fall-back frequencies until communication is established, as explained more fully below.

20 Figure 4 is a flowchart illustrating the various steps performed by the transceivers and controllers located both in the

ground base control system and the remote vehicle.

Prior to launching the remote vehicle, the initial transmission frequency of the first message is programmed into the memory contained in controller 207 of the remote vehicle. In addition, the data decryption key for decoding the encrypted data messages is stored in the memory of controller 207. The pattern of predetermined fall-back frequencies is also stored in the memories of controllers 107 and 207.

Controller 107 then selects the next up-link transmission frequency and generates an information signal (such as that shown in Fig. 2) including a word representative of the next frequency of transmission. The message portion 307 of information signal 301, including the word representative of the next frequency of transmission, is then encrypted and transmitted as a single burst during a predetermined time period, as determined by controller 107. The transmitted signal travels over the up-link portion of transmission link 300.

Meanwhile, receiver section 205 of the remote vehicle is tuned to the initial transmission frequency (as this frequency has been previously preprogrammed into the memory of controller 207) and awaits the transmission of the information signal. If an information signal 301 is detected the message portion 307 of the signal is checked for errors by controller 207 and, if properly received, the message portion 307 will then be decrypted by data decryptor 209. The decrypted portion of the word representative of the frequency of the next data word transmission is then utilized by controller 207 to retune receiver unit 211 to this next frequency.

If no signal is received within a predetermined time period or if the received signal contains errors, controller 207 generates an error signal which is then immediately transmitted by transmitter section 203 back to the ground station via down-link portion of transmission link 300. Both controllers 107 and 207 contain real-time clocks which can be synchronized prior to launching of the remote vehicle. By suitably programming the controllers 107 and 207, transmitter section 103 of the ground station can be

caused to transmit the information signals during preselected time periods and receiver section 205 of the remote vehicle can be caused to look for these signals during the predetermined time period.

5 If the message transmitted over the up-link is properly received by receiver section 205 then an acknowledgment signal is generated by controller 207 and sent back by transmitter section 203 to the ground station over the down-link. So long as the receiver section 105 of the ground station receives the
10 acknowledgment signal from the remote vehicle over the down-link, controller 107 will operate in a normal fashion causing the next message to be transmitted at the frequency specified by the frequency representative word portion of the previously transmitted information signal. If no acknowledgement signal is
15 received, or if an error signal is received by receiver section 105, controller 107 then will begin one of two different fall-back modes. If no down-link signal is received from the remote vehicle at all, then controller 107 will regenerate the initial information signal and attempt to retransmit it a predetermined
20 number of times over the up-link to the remote vehicle until a proper acknowledgment signal is transmitted by the remote vehicle back over the down-link. Controller 107 can also be programmed to cause the information signal to be retransmitted, but over a series of predetermined fall-back frequencies if communication
25 with the remote vehicle is not made within a predetermined time period. Likewise, controller 207 of the remote vehicle will begin retuning receiver unit 211 to these predetermined fall-back frequencies if a predetermined time period has elapsed without receiving any signal from the ground station over the up-link.

30 Once a proper acknowledgment signal has been received by receiver section 105 of the ground station, the up-link signal will be transmitted on the next preprogrammed frequency as described earlier. If, for some reason receiver section 205 of the remote vehicle receives the message but it contains errors or is otherwise garbled, controller 207 will generate an error signal which will then be transmitted via the down-link back to the

ground station. In the event this occurs, both controllers 107 and 207 are preprogrammed to begin utilizing a predetermined series of fall-back frequencies until communication between the ground station and the remote vehicle is reestablished. This ensures that if for some reason the information signal is improperly received by the remote vehicle due to intentional jamming or noise in a particular area of the transmission link, it will still be possible to reestablish communication at some other frequency.

While the present invention has been described in considerable detail, it is understood that various changes and modifications will fall within the scope of the invention. For example, while message-by-message frequency-hopping has been discussed, it will be understood that word-by-word or symbol-by-symbol frequency-hopping may also be utilized. In the case of word-by-word or symbol-by-symbol frequency hopping, the encrypted up-link command would contain the starting frequency of a pre-programmed hopping sequence to be used until a new command is received. In addition to data concerning the next frequency of transmission, the transmitted information signal may contain data designating the time of the next transmission or data concerning the predetermined pattern of fall-back frequencies which are to be utilized.

It should be understood that the foregoing detailed description of the preferred embodiment of the invention is merely illustrative, but not limitive, of the invention which is defined by the appended claims.

0167442

What is claimed is:

1. A method of secure communications utilizing frequency-hopping and having at least a transmitter and a receiver, said method preventing intentional jamming and being characterized by the steps of:

(a) generating at the transmitter an information signal including at least a portion representative of the frequency of transmission of the next informational signal;

(b) transmitting the information signal at a transmission frequency determined by the frequency representative portion of an immediately preceding transmitted information signal; and

(c) receiving the information signal at the receiver at a frequency determined by the frequency representative portion of the immediately preceding received information signal.

2. The method of claim 1 characterized in that step (a) includes the step of encrypting at least the frequency representative portion and step (c) includes the step of decrypting at least the encrypted frequency representative portion.

3. The method of claim 1 or 2 characterized in that in step (b) the information signal is transmitted as a short burst, with the time between each transmitted information signal being greater than the time of transmission for an information signal.

4. The method of claim 1, 2 or 3 characterized in that in both the transmitter and receiver are initially tuned to a same predetermined frequency.

5. The method of any previous claim characterized by the steps of:

(d) detecting at the receiver whether the transmitted information signal is properly received;

(e) transmitting an acknowledgement signal from the receiver to the transmitter if the transmitted signal is properly received, otherwise transmitting an error signal if the transmitted signal is not properly received and tuning the receiver to a predetermined

fall-back frequency; and

(f) detecting at the transmitter the presence of the acknowledgement or error signals and continuing normal operation of the transmitter in response to detection of the acknowledgement signal, otherwise causing the transmitter to begin transmitting at the predetermined fall-back frequency in response to detection of the error signal or the absence of either the acknowledgement or error signals.

6. The method of claim 5 characterized in that the transmitter looks for the acknowledgement and error signals during predetermined time periods.

7. The method of claim 5 or 6 characterized in that there is more than one predetermined fall-back frequency, such that if communication between a transmitter and receiver cannot be initiated at a first predetermined fall-back frequency, additional fall-back frequencies are tried until communication is established.

8. The method of claim 7 characterized in that at least the initial fall-back frequency is the same as the transmission frequency.

9. The method of any one of claims 5-8 characterized in that step (d) is performed after receiving the information signal but prior to decrypting at least the encrypted frequency representative portion.

10. A secure communications apparatus of the frequency-hopping type characterized by:

a transmitter including means for generating an information signal including at least a portion representative of the frequency of transmission of the next information signal, and means for transmitting the information signal at a transmission frequency determined by the frequency representative portion of an immediately preceding transmitted information signal; and

0167442

a receiver for receiving the information signal, including means for tuning the receiver to a frequency determined by the frequency representative portion of the immediately preceding received information signal.

11. Apparatus of claim 10 characterized in that the transmitter includes means for encrypting at least the frequency representative portion and the receiver includes means for decrypting at least the encrypted frequency representative portion.

12. Apparatus of claim 10 or 11 characterized in that the transmitter includes means for transmitting the information signal as a short burst, with the time between each transmitted information signal being greater than the time of transmission for an informational signal.

13. Apparatus of claim 10, 11 or 12 characterized in that both the transmitter and receiver each include means for initially tuning the transmitter and receiver, respectively, to a same predetermined frequency.

14. Apparatus of any one of claims 10-13 characterized by:

means for detecting at the receiver whether the transmitted information signal is properly received;

means for transmitting an acknowledgment signal from the receiver to the transmitter if the transmitted signal is properly received, and for transmitting an error signal if the transmitted signal is not properly received and for tuning the receiver to a predetermined fall-back frequency; and

means for detecting at the transmitter the presence of the acknowledgment and error signals and for enabling normal operation of the transmitter in response to detection of the acknowledgment signal, and for causing the transmitter to begin transmitting at the predetermined fall-back frequency in response to detection of the error signal or the absence of either the acknowledgment or error signals.

15. Apparatus of claim 14 characterized in that the transmitter includes means for searching for the acknowledgment or error signals during predetermined time periods.

16. Apparatus of claim 14 or 15 characterized in that the transmitter includes means for successively transmitting at a predetermined series of fall-back frequencies and the receiver includes means for successively tuning the receiver to the predetermined series of fall-back frequencies, whereby if communication between a transmitter and receiver cannot be initiated at a first predetermined fall-back frequency, additional fall-back frequencies are tried until communication is established.

17. Apparatus of claim 16 characterized in that at least the initial one of the predetermined series of fall-back frequencies is the same as the transmission frequency.

18. Apparatus of any one of claims 14-17 characterized in that said means for transmitting the information signal transmits at a transmission frequency which initially is a predetermined frequency and thereafter is a frequency determined by the encrypted frequency representative portion of the immediately preceding transmitted information signal; and

said receiver for receiving the information signal includes means for initially tuning the receiver to the predetermined frequency, means for decrypting at least the encrypted frequency representative portion, and means for retuning the receiver to the frequency indicated by the decryption of the encrypted frequency representative portion for reception of the next transmitted information signal.

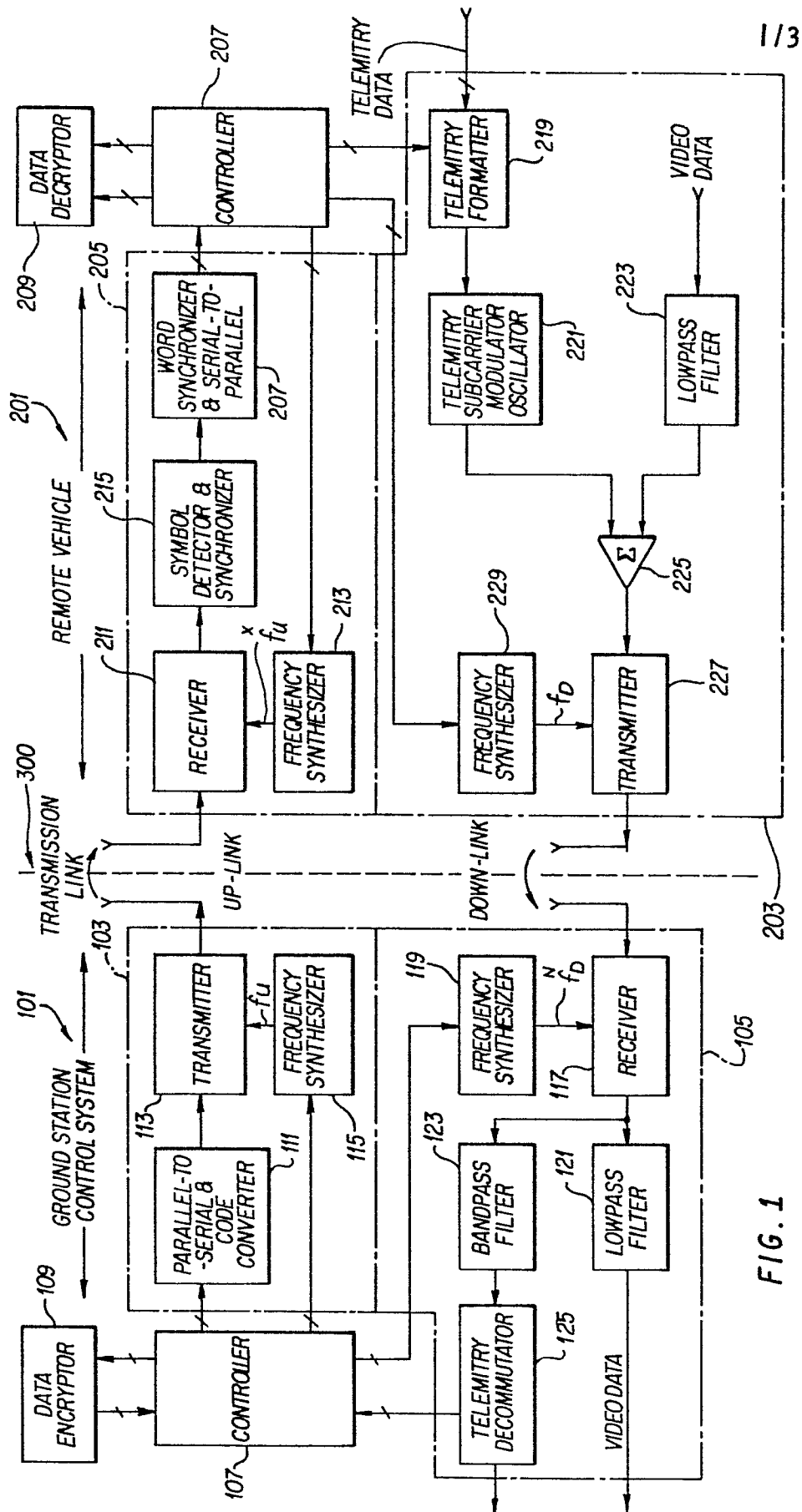
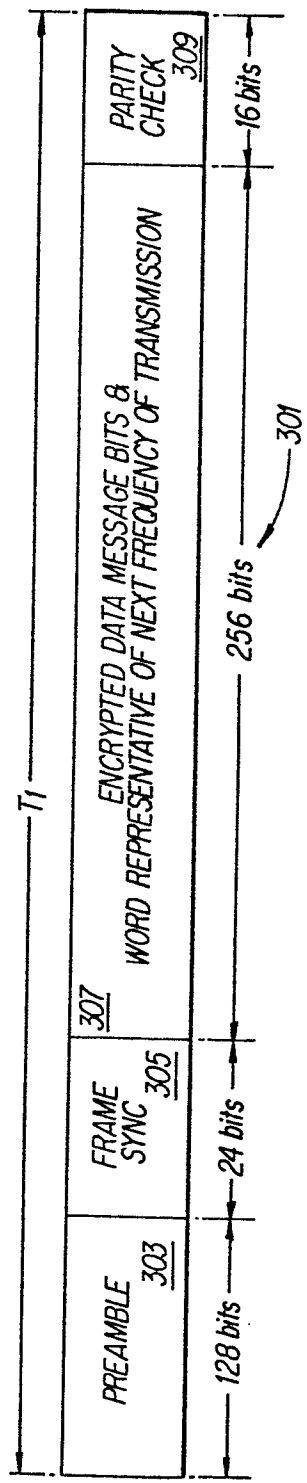
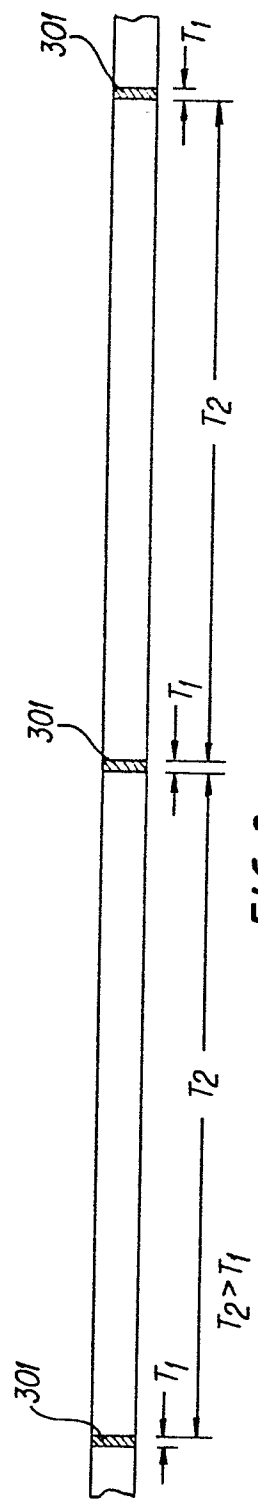


FIG. 1



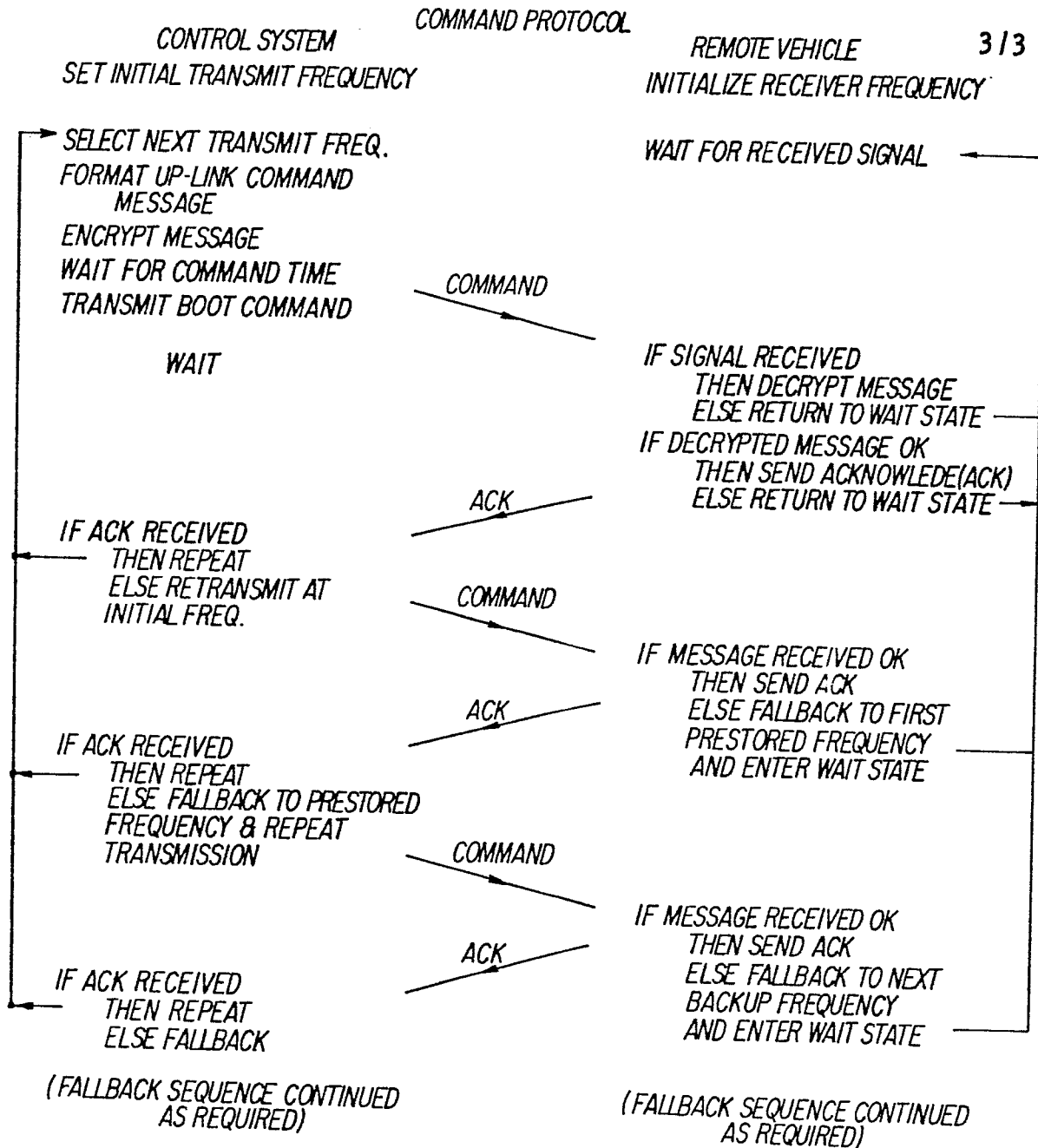


FIG. 4