US 20040005872A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0005872 A1

Cervinka et al. (43) Pub. Date: Jan. 8, 2004

(54) JAMMING-RESISTANT WIRELESS TRANSMISSION OF SECURITY DATA

(75) Inventors: **Alexandre Cervinka**, Montreal (CA); **Jean-Louis Gauvreau**, La Prairie (CA)

Correspondence Address:
TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110 (US)

(73) Assignee: **Newtrax Technologies Inc.**, Montreal (CA)

(21) Appl. No.: **10/418,393**

(22) Filed: **Apr. 18, 2003**

(30) **Foreign Application Priority Data**

Jul. 3, 2002 (CA) 2,392,326

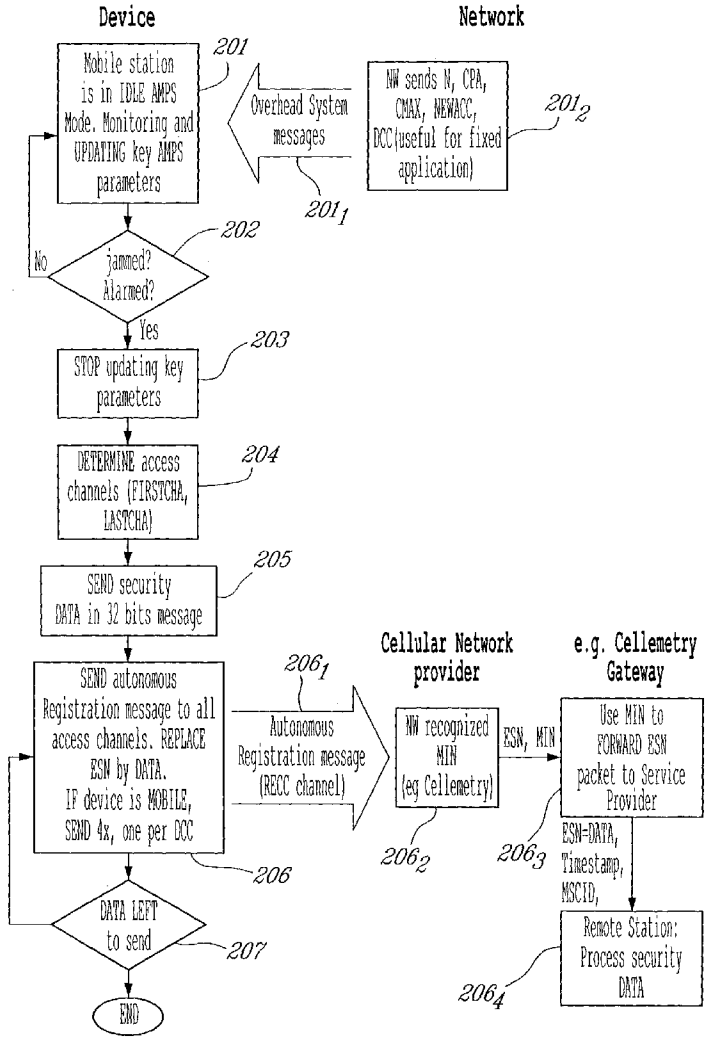
Publication Classification

(51) **Int. Cl.**[7] **H04M 1/66**

(52) **U.S. Cl.** **455/410**; 455/1; 455/411; 380/247

(57) **ABSTRACT**

A jamming-resistant method and system transmit security data through a wireless telecommunication network from a first station to a second station remote from the first station. Prior to transmission, common access channels of the wireless telecommunication network are determined. The security data are then transmitted from the first station to the second station through a plurality of the common access channels of the wireless telecommunication network. The security data may be transmitted from the first station to the second station without receiving local access parameters from the wireless telecommunication network at the time of transmission.



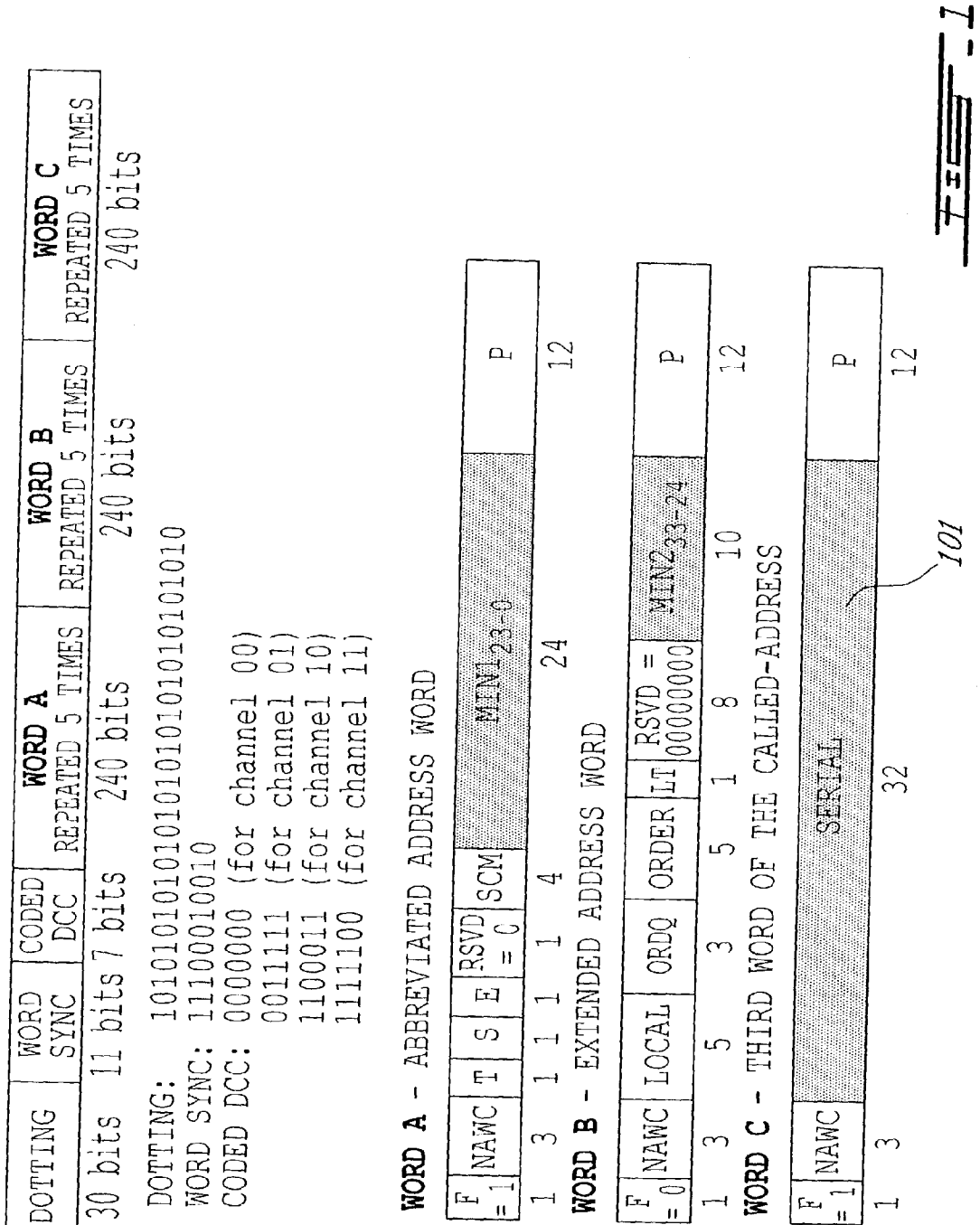

DOTTING
WORD SYNC
CODED DCC
WORD A
REPEATED 5 TIMES
WORD B
REPEATED 5 TIMES
WORD C
REPEATED 5 TIMES
30 bits 11 bits 7 bits 240 bits 240 bits 240 bits
DOTTING: 1010101010101010101010101010
WORD SYNC: 11100010010
CODED DCC: 0000000 (for channel 00)
0011111 (for channel 01)
1100011 (for channel 10)
1111100 (for channel 11)
WORD A - ABBREVIATED ADDRESS WORD
F = 1
NAWC
T
S
E
RSVD = 0
SCM
MIN1 23-0
P
1 3 1 1 1 1 4 24 12
WORD B - EXTENDED ADDRESS WORD
F = 0
NAWC
LOCAL
ORDQ
ORDER
LT
RSVD = 00000000
MIN2 23-24
P
1 3 5 3 5 1 8 10 12
WORD C - THIRD WORD OF THE CALLED-ADDRESS
F = 1
NAWC
SERIAL
P
1 3 32 12
101

FIG. 1

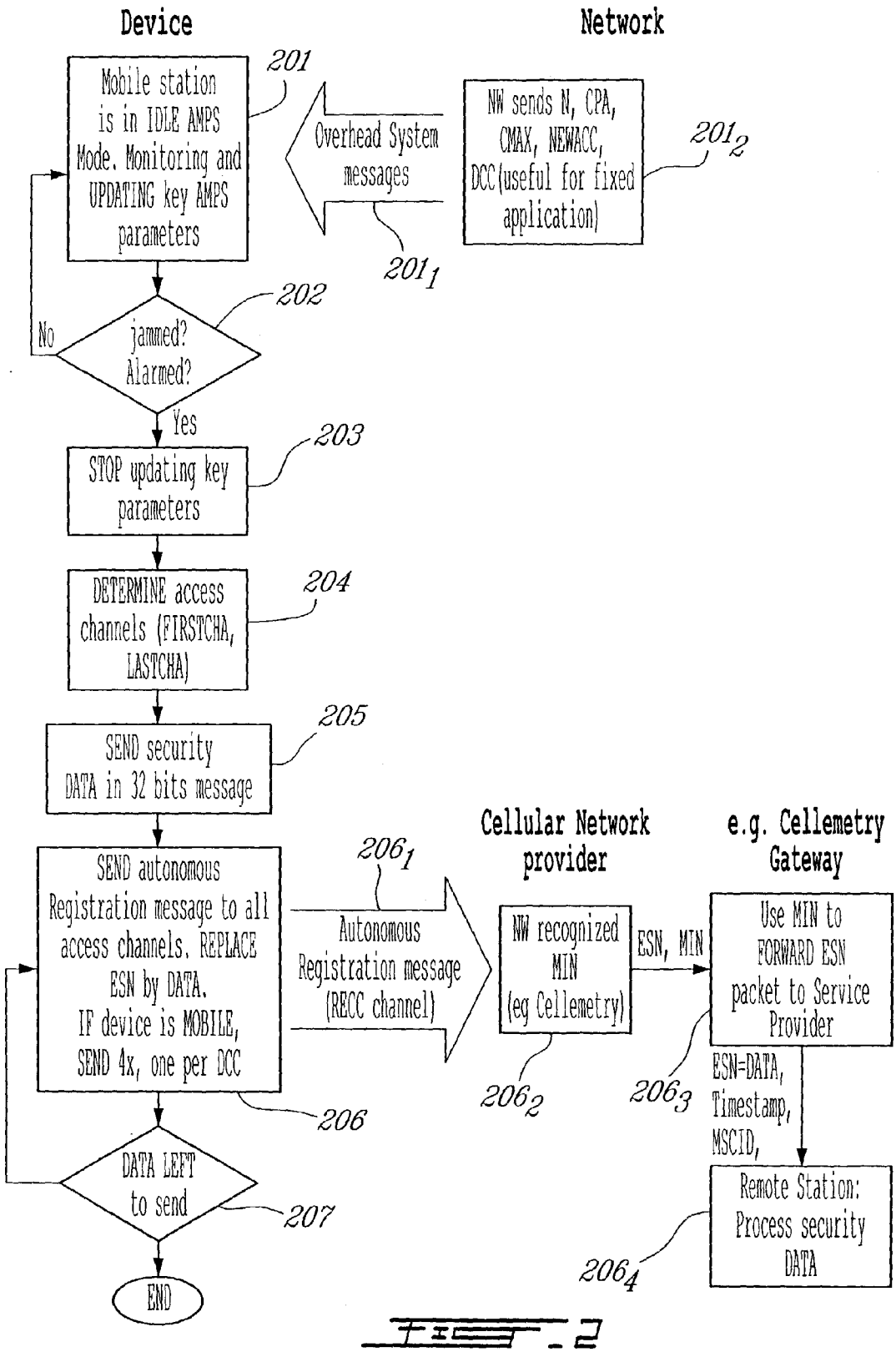

Device
Network
Mobile station is in IDLE AMPS Mode. Monitoring and UPDATING key AMPS parameters
201
Overhead System messages
NW sends N, CPA, CMAX, NEWACC, DCC(useful for fixed application)
201_2
201_1
jammed? Alarmed?
202
No
Yes
STOP updating key parameters
203
DETERMINE access channels (FIRSTCHA, LASTCHA)
204
SEND security DATA in 32 bits message
205
SEND autonomous Registration message to all access channels. REPLACE ESN by DATA. IF device is MOBILE, SEND 4x, one per DCC
206
206_1
Autonomous Registration message (RECC channel)
Cellular Network provider
NW recognized MIN (eg Cellemetry)
206_2
ESN, MIN
e.g. Cellemetry Gateway
Use MIN to FORWARD ESN packet to Service Provider
206_3
ESN=DATA, Timestamp, MSCID,
Remote Station: Process security DATA
206_4
DATA LEFT to send
207
END

FIG. 2

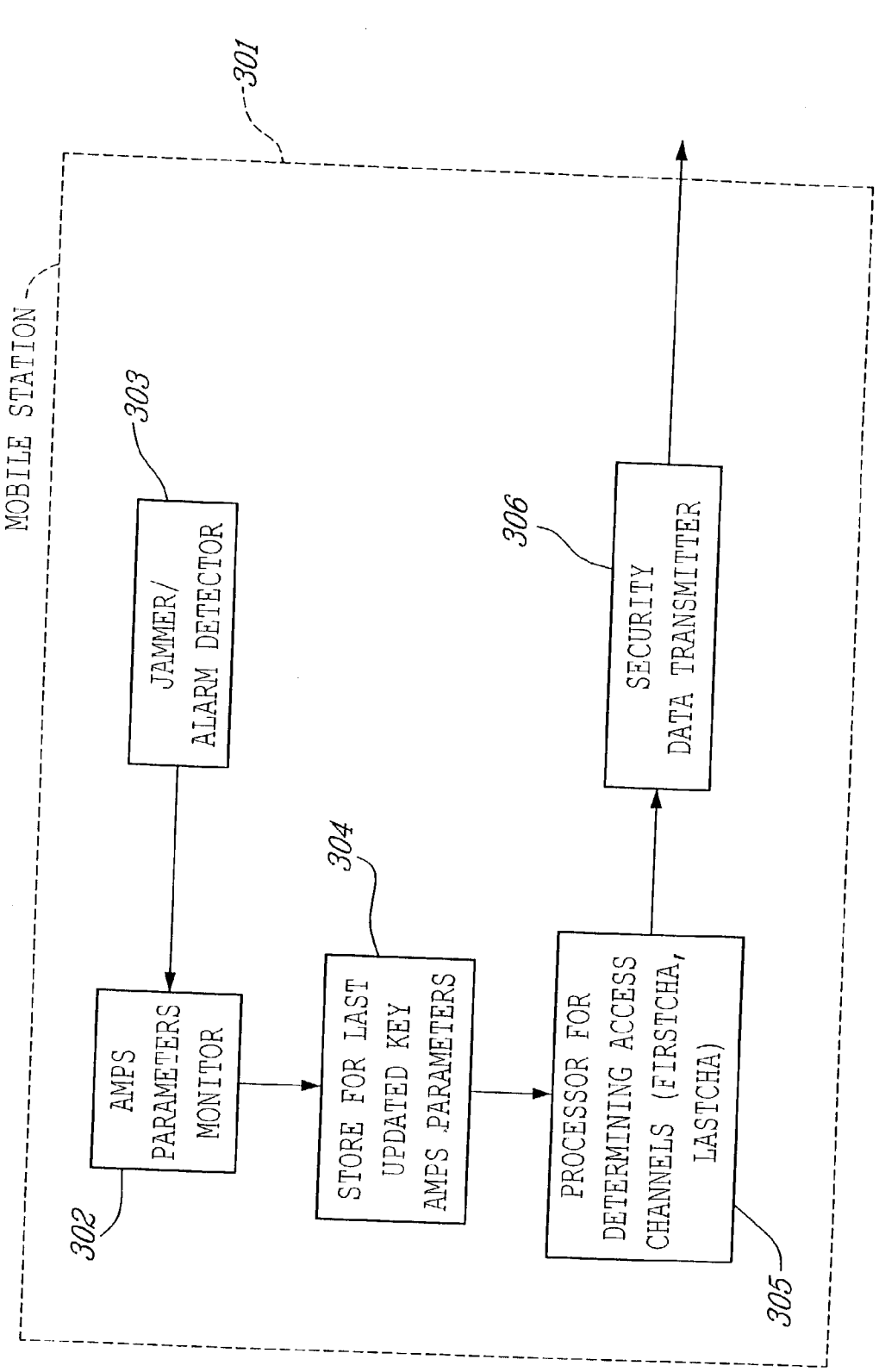

301
MOBILE STATION
303
JAMMER/
ALARM DETECTOR
306
SECURITY
DATA TRANSMITTER
304
AMPS
PARAMETERS
MONITOR
STORE FOR LAST
UPDATED KEY
AMPS PARAMETERS
PROCESSOR FOR
DETERMINING ACCESS
CHANNELS (FIRSTCHA,
LASTCHA)
302
305

FIG. 3

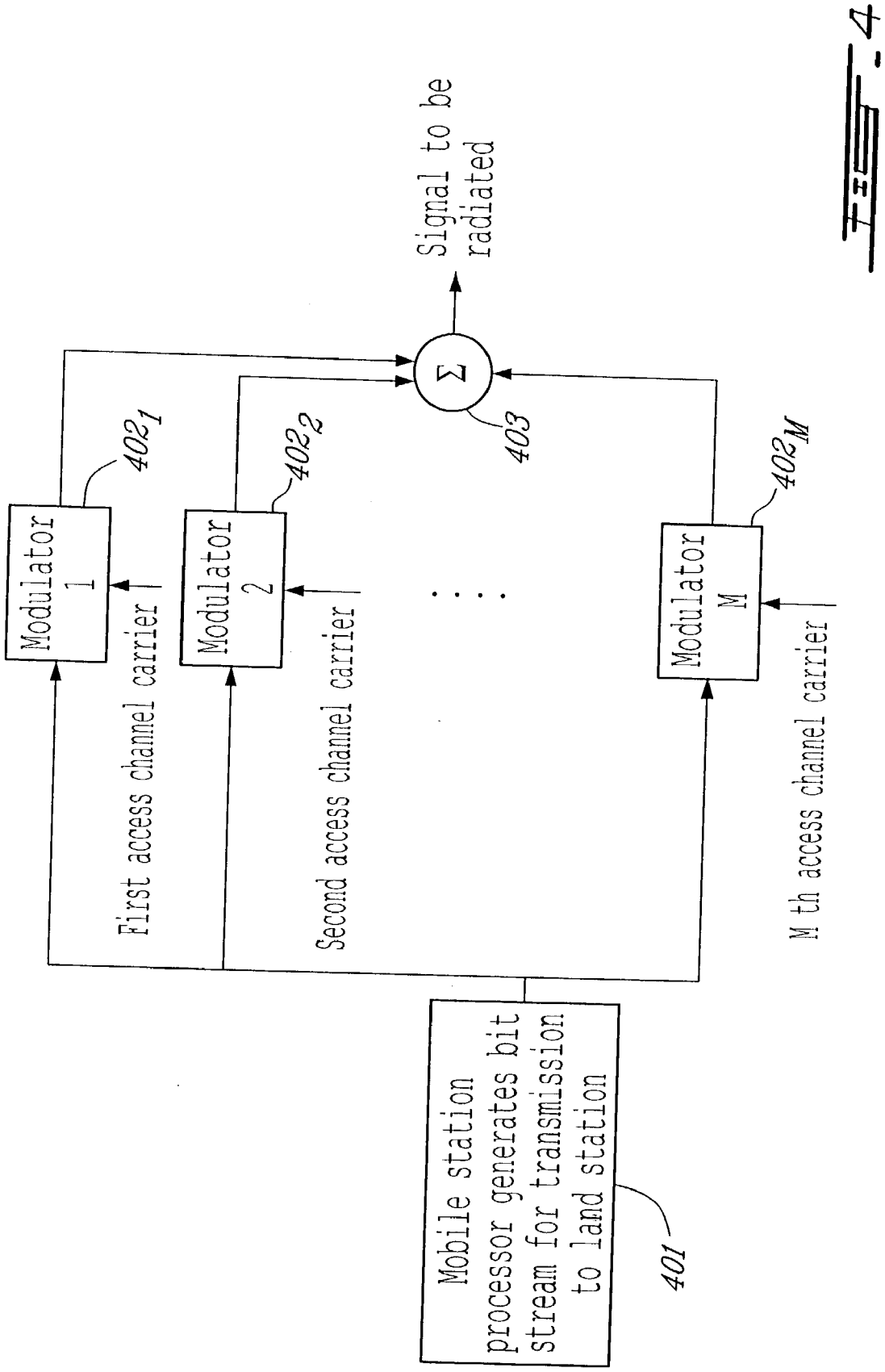

Mobile station processor generates bit stream for transmission to land station
401
Modulator 1
Modulator 2
Modulator M
402_1
402_2
402_M
First access channel carrier
Second access channel carrier
M th access channel carrier
Σ
403
Signal to be radiated

Fig. 4

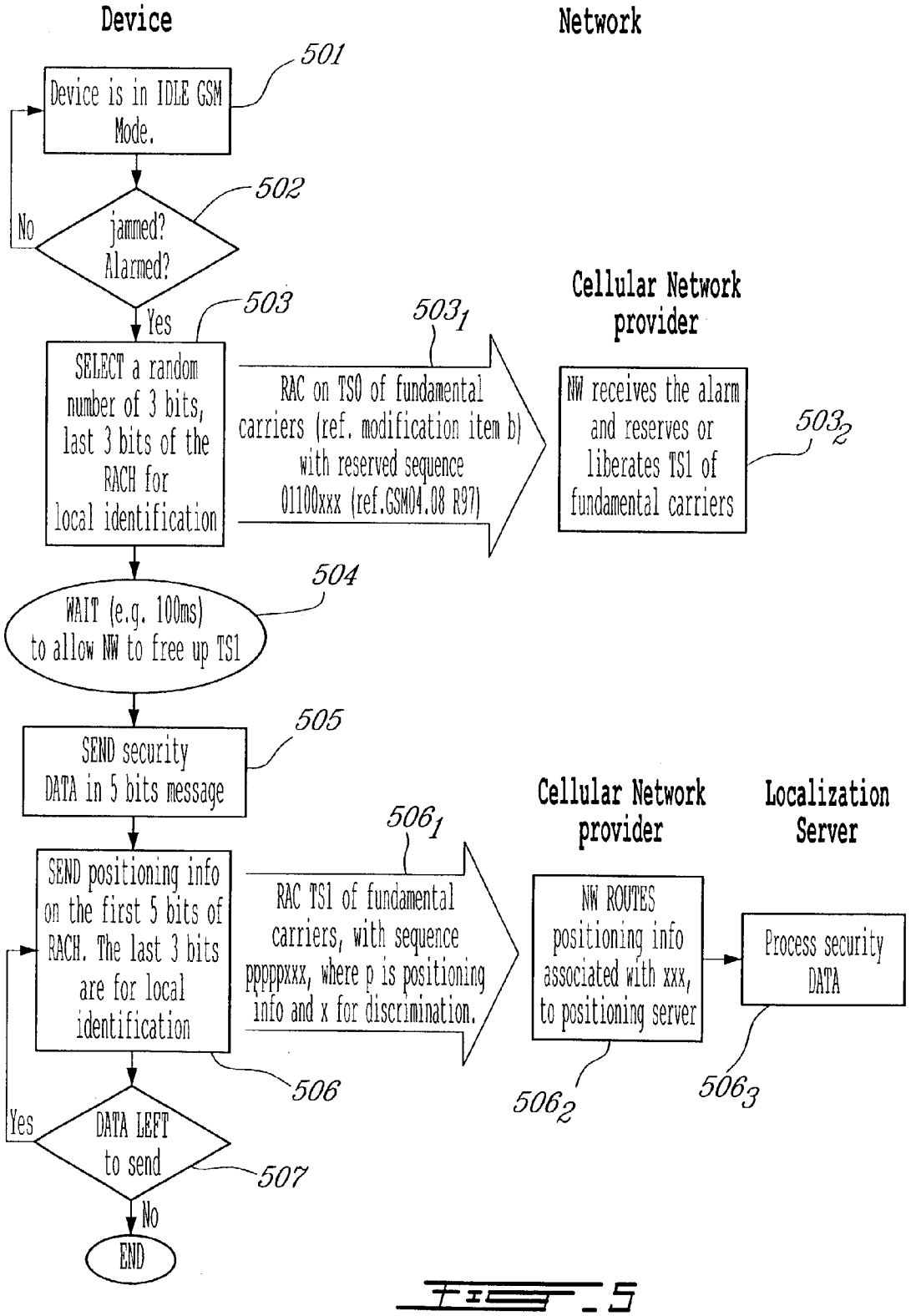

Device
Network
501
Device is in IDLE GSM Mode.
502
jammed? Alarmed?
No
Yes
503
SELECT a random number of 3 bits, last 3 bits of the RACH for local identification
503 1
RAC on TS0 of fundamental carriers (ref. modification item b) with reserved sequence 01100xxx (ref.GSM04.08 R97)
Cellular Network provider
NW receives the alarm and reserves or liberates TS1 of fundamental carriers
503 2
504
WAIT (e.g. 100ms) to allow NW to free up TS1
505
SEND security DATA in 5 bits message
506 1
SEND positioning info on the first 5 bits of RACH. The last 3 bits are for local identification
RAC TS1 of fundamental carriers, with sequence pppppxxx, where p is positioning info and x for discrimination.
Cellular Network provider
Localization Server
NW ROUTES positioning info associated with xxx, to positioning server
Process security DATA
506
506 2
506 3
Yes
DATA LEFT to send
507
No
END

Fig. 5

JAMMING-RESISTANT WIRELESS TRANSMISSION OF SECURITY DATA

FIELD OF THE INVENTION

[0001] The present invention relates to jamming-resistant method and system for transmitting through a wireless telecommunication network security data from a first station to a second station remote from the first station.

BACKGROUND OF THE INVENTION

[0002] Tracking Systems:

[0003] Tracking systems are designed and implemented to enable people to remotely determine the position or location of their assets. Tracking systems are widely used in many logistic applications such as fleet management, and in many security applications such as stolen asset recovery.

[0004] Tracking systems comprise a mobile station and usually incorporate two technologies:

[0005] 1. A positioning/navigation technology such as GPS (Global Positioning System), cellular triangulation, or dead reckoning to determine the coordinates of the mobile station being tracked; and

[0006] 2. A wireless telecommunication technology such as cellular or satellite communication to transmit the coordinates or reference signal from the mobile station to a remote, mobile and/or stationary station.

[0007] The wireless technology must work for the tracking system to operate properly.

[0008] For the application to tracking systems, the commercial wireless telecommunication networks present the drawback of being vulnerable to jammers, which can interfere with or prevent clear reception of air-borne EMW (Electro-Magnetic Wave) signals. For instance, the following Table 1 compares the commercial jammers (transmitters in the receiving band of the mobile station) and military jammers.

TABLE 1

Jammers	
Commercial	Military
Intended appiication is to create a cellular service hole in theatres, restaurants, and places of worship to eliminate cellular ring tones and phone conversations.	Intended application is warfare.
Operation constrained by regulation.	No regulation applies.
Widely distributed and large international market. Illegal in Canada and the U.S., yet easily available: one can order a jammer over the Internet and receive the unit 48 hours later.	Very limited legal market, and distribution controlled by special government agencies.
Low-power radiation blocks all commercial downlink bands by generating noise near terminal receiver. Usage affects subscribers in room (for example 10-100 meter radius area) or only immediate vicinity of truck/cargo.	High-power radiation blocks the receivers of all neighboring base stations, effectively putting several thousand subscribers out of service. This is a major civil disturbance that would mobilize public emergency services. The high power radiation makes the source easy to locate quickly so this jammer would not be an obvious choice to support a theft.
Undetectable by network operator.	Network alarms are triggered and emergency procedures could take effect to re-establish service and identify source of problem.

[0009] Therefore, individuals can today disable any commercial tracking system using a jammer purchased online through the Internet for a few hundred dollars. This is of major concern to those who use tracking systems for security purposes such as fleet owners, insurance companies, and governments keeping a close watch on the transport of hazardous materials.

[0010] Alarm Systems:

[0011] In the case of alarm systems, status and identification information must be communicated to remote monitoring stations. Normally:

[0012] 1. Mobile alarm systems use wireless telecommunications; and

[0013] 2. Fixed alarm systems today use wireline telecommunications as a first resource. High-end systems offer a wireless telecommunication service as backup in case wireline communications fail.

[0014] Again, the wireless telecommunication link used in alarm systems can be disabled by means of a jammer purchased online through the Internet for a few hundred dollars.

SUMMARY OF THE INVENTION

[0015] According to the invention, there is provided a jamming-resistant method for transmitting security data through a wireless telecommunication network from a first station to a second station remote from the first station, comprising: determining, prior to transmission, common access channels of the wireless telecommunication network; and transmitting the security data from the first station to the second station through a plurality of these common access channels of the wireless telecommunication network.

[0016] The present invention also relates to a jamming-resistant system for transmitting security data through a wireless telecommunication network from a first station to a second station remote from this first station. The wireless telecommunication network comprises common access channels, and the jamming-resistant system comprises a transmitter of the security data from the first station to the second station through a plurality of the common access channels of the wireless telecommunication network.

[0017] The foregoing and other objects, advantages and features of the present invention will become more apparent upon reading of the following non restrictive description of illustrative embodiments thereof, given for the purpose of illustration only with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] In the appended drawings:

[0019] **FIG. 1** is a schematic diagram illustrating the structure of an autonomous registration frame sent by a mobile station over an access channel of a wireless telecommunication network;

[0020] **FIG. 2** is a flow chart showing the operation of a jamming-resistant wireless transmission method according to a first illustrative embodiment of the present invention;

[0021] **FIG. 3** is a block diagram of a first version of wireless mobile station according to the first illustrative embodiment of the present invention;

[0022] **FIG. 4** is a block diagram of a second version of wireless mobile station according to the first illustrative embodiment of the present invention; and

[0023] **FIG. 5** is a flow chart showing the operation of a jamming-resistant wireless transmission method according to a second illustrative embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

[0024] Illustrative embodiments of the present invention will now be described with reference to the accompanying drawings.

[0025] All communication protocols used in wide area wireless telecommunication networks require the mobile stations to receive at least one of the following local access parameters from the wireless telecommunication network before transmitting:

[0026] the frequency channel on which the mobile station should transmit;

[0027] the time slot during which the mobile station should transmit;

[0028] the code which should be used to spread, scramble or discriminate the narrowband signal;

[0029] the transmission power; and

[0030] the synchronisation frame.

[0031] Commercial jammers disable the receivers of all mobile stations within a variable radius typically in the range of 10-100 meters. More specifically, since the mobile stations no longer receive the above listed local access parameters in the presence of a jammer, the mobile stations do not transmit.

[0032] Therefore, a jammer will prevent a mobile station from receiving information from a wireless telecommunication network. However, commercial jammers do not prevent the mobile stations from transmitting data to the same network. Accordingly, it is possible for a mobile station to transmit data to a wireless telecommunication network using current frequency plans and multiple access schemes. The transmitted data could comprise security data such as identification, alarm, position and/or displacement information, and/or any other useful data.

[0033] Cellemetry Virtual Network:

[0034] In the first illustrative embodiment, as depicted in **FIGS. 1, 2, 3** and **4**, the mobile station **301** (**FIG. 3**) transmits information to a Cellemetry virtual network.

[0035] In the following description of the first and second illustrative embodiments of the present invention, the time period before a security-breach "event" is referred to as the "pre-event" period. In the same manner, the time period after the security-breach "event" is referred to herein as the "post-event" period.

[0036] During the post-event period, the mobile station **301** (**FIG. 3**) is assumed to remain within the coverage of the wireless telecommunication network detected by the mobile station **301** just before the event.

[0037] The jamming-resistant cellular uplink of the first illustrative embodiment is based on piggybacking data on the autonomous registration frame shown in **FIG. 1**. The idea behind this first illustrative embodiment of **FIGS. 1, 2, 3** and **4** is to replace the ESN (Electric Serial Number) with 32 bits of data, to send the autonomous registration frame on all possible common access channels of the Cellemetry virtual network and, then, to route the autonomous registration frame to a remote station.

[0038] As a non-limitative example, **FIG. 1** shows a TIA-553 (AMPS (Advanced Mobile Phone Service)) autonomous registration frame sent by the mobile station **301** over the RECC (Reverse Control Channel) of a common access channel to a wireless cellular telecommunication network. The autonomous registration frame comprises a serial bit stream including a 30-bit dotting, an 11-bit word sync, a 7-bit coded DCC (Digital Colour Code), WORD A, WORD B, and WORD C. WORD A is repeated five (5) times within a first stream of 240 bits, WORD B is repeated five (5) times within a second stream of 240 bits, and WORD C is repeated five (5) times within a third stream of 240 bits.

[0039] **FIG. 1** further describes the constitution of the 30-bit dotting, 11-bit word sync, 7-bit coded DCC, WORD A, WORD B, and WORD C. As illustrated in **FIG. 1**:

[0040] the 30-bit dotting is a repetitive stream of bits such as "10101010101010101010101010101010";

[0041] the 11-bit word sync is a stream of bits such as "11100010010";

[0042] the 7-bit coded DCC is

[0043] 0000000 (for channel 00)

[0044] 0011111 (for channel 01)

[0045] 1100011 (for channel 10)

[0046] 1111100 (for channel 11)

[0047] WORD A is an abbreviated address word having a structure such as the one illustrated in **FIG. 1**, comprising a first MIN1 (Mobile Identification Number);

[0048] WORD B is an extended address word having a structure such as the one illustrated in **FIG. 1**, comprising a second MIN2 (Mobile Identification Number); and

[0049] WORD C is the third word of the called address having a structure such as the one illustrated in **FIG. 1**, comprising a 32-bit serial ESN **101** which is replaced, as indicated in the foregoing description, with 32 bits of data.

[0050] These 30-bit dotting, 11-bit word sync, 7-bit coded DCC, WORD A, WORD B, and WORD C are otherwise well known to those of ordinary skill in the art and, accordingly, will not be further described in the present specification. In particular, these 30-bit dotting, 11-bit word sync, 7-bit coded DCC, WORD A, WORD B, and WORD C are fully described in the following AMPS specifications: Mobile Station—Land Station Compatibility Specification EIA/TIA-553, September 1989, incorporated herein by reference.

[0051] Referring now to **FIG. 3**, the mobile station, generally identified by the reference **301**, comprises an AMPS parameters monitor **302**, a jammer/alarm detector **303**, a store **304** for the last updated key AMPS parameters, a processor **305** for determining the common access channels, and a security data transmitter **306**.

[0052] Step **201** (**FIG. 2**):

[0053] Referring to **FIG. 2**, in the pre-event period (step **201**), the mobile station **301** (**FIG. 3**) is in the idle AMPS mode. In this particular mode, during the pre-event period, the mobile station **301** acts as a standard Cellemetry terminal; the AMPS parameters monitor **302** of the mobile station **301** monitors, updates and keeps in memory the following key AMPS parameters or variables received from the wireless cellular telecommunication network (substep $\mathbf{201}_2$) through overhead system messages (substep $\mathbf{201}_1$) transmitted from the wireless cellular telecommunication network through dedicated control or paging channels, for example FOCCs (Forward Control Channels):

[0054] N: Number of paging channels;

[0055] CPA: Combined paging/access field;

[0056] CMAX: Number of access channels;

[0057] NEWACC: New Access Channel; and

[0058] DCC: Digital Colour Code (useful for fixed application of the mobile station).

[0059] Step **202**:

[0060] In step **202**, a jammer/alarm detector **303** detects the presence of a jammer or alarm (security breach). If no jammer or alarm is detected, the process returns to step **201**.

[0061] For example, a jammer is detected when a loss of contact between the mobile station and the telecommunication network is detected.

[0062] Step **203**:

[0063] In response to detection of a jammer (proximate the mobile station **301**) or an alarm by the detector **303**, i.e. once an event is detected the AMPS parameters monitor **302** stops updating the values of the above mentioned key AMPS parameters based on the overhead system messages (substep $\mathbf{201}_1$) received from FOCCs of the cellular network. The last updated key AMPS parameters are then stored into a store **304**.

[0064] Step **204**:

[0065] The purpose of the Cellemetry's modifications to the TIA-553 (AMPS) autonomous registration frame were to create an uplink data channel through the autonomous registration procedure. More specifically, the modifications are:

[0066] 1. Replacing the ESN (Electric Serial Number) **101** of WORD C (**FIG. 1**) of the autonomous registration frame with 32 bits of data; and

[0067] 2. Forcing the autonomous registration to occur when the mobile station **301** (application software) has data to send.

[0068] In step **204**, the first (FIRSTCHA) and last (LASTCHA) access channels are determined by a processor **305** (**FIG. 3**) using the following standard equations:

[0069] If mobile station **301** stands on an A-band system (B-band case uses a similar procedure):

[0070] if paging and access channels are combined (CPA=1), set FIRSTCHA to the first dedicated control channel on A-band System:

[0071] 834.990 MHz mobile Tx, 879.990 MHz land Tx and the last access channel (LASTCHA) to:

LAST*CHA*=FIRST*CH*−*CMAX*+1

[0072] if paging and access channels are not combined (CPA=0), set FIRSTCHA to the first dedicated control channel on A-band system minus N× channel bandwidth:

(834.990−*N*×0.030) *MHz* mobile *Tx*, (879.990−*N*× 0.030) *MHz* land *Tx*

[0073] and the last access channel (LASTCHA) to:

LAST*CHA*=FIRST*CH*+*CMAX*−1

[0074] if NEWACC specified, set

FIRSTCHA=NEWACC

LAST*CHA*=NEW*ACC*−*CMAX* +1

[0075] Step **205**:

[0076] The mobile station **301** then proceeds with sending security data in 32-bits messages through a transmitter **306** (**FIG. 3**) to the desired destination, for example a remote station (not shown) of an event-monitoring service.

[0077] Step **206**:

[0078] As indicated in the foregoing description the ESN **101** of WORD C of the autonomous registration frame is replaced by the security data to be transmitted to the remote station.

[0079] Then, when used in a mobile application (for instance telematics), the transmitter **306** of the mobile station **301** transmits the autonomous registration frame [(LASTCHA−FIRSTCHA+1)×4] times, i.e. once on each possible RECC access channel within the range between the first access channel FIRSTCHA and the last access channel LASTCHA, with all four (4) DCCs (substep $\mathbf{206}_1$).

[0080] If used in a fixed application (for instance home alarms), the transmitter **306** of the mobile station **301** transmits the autonomous registration frame on one or more RECC access channels with corresponding DCC (substep

206_1). Since the mobile station is not moving, it should always remain in the coverage of the same neighbouring base station(s).

[0081] Modifications to the first illustrative embodiment can be done to increase the rate in which information can be successfully transmitted in a jamming resistant fashion. In fact, three different modifications applicable to the first illustrative embodiment have been identified:

[0082] MIN rotation;

[0083] Multi-carriers transmission;

[0084] MIN information encoding

[0085] MIN Rotation:

[0086] Basic Cellemetry uses a single MIN (Mobile Identification Number) to make the registration request. In the first illustrative embodiment of the present invention, the MIN of the autonomous registration frame is formed by MIN1 of WORD A and MIN2 of WORD B (**FIG. 1**) and identifies the remote station of the event monitoring service to which the security data has to be transmitted. The MIN and ESN are forwarded to the Cellemetry server on an inter-cellular network (for example an IS-41 inter-cellular network), where the encapsulated 32 bits of data are received. Since the ESN has been replaced by the security data (32 bits of data), the ESN is not recognized by the Cellemetry server, and a "reject registration request" message is sent back to the host network. The host network then deletes the record from the VLR (Visitor Location Register). This loop can take as much as 1 minute to complete, and the terminal with the same MIN is unable to send an additional registration request. This system would offer a 32 bits/minute bandwidth.

[0087] To increase the bandwidth, one can use MIN rotation. For example, one can assign a large number of slave MINs to every mobile station in addition to the MIN used to uniquely identify the mobile station. After the first registration request is sent over a plurality of common access channels using the uniquely identifying MIN of the mobile station, subsequent registration requests carrying new 32-bits serial ESNs are sent over a plurality of common access channels using different MINs. The throughput of 32 bits per minute initially achieved will then be increased by the number of autonomous registration requests successfully received using a different MIN and a new ESN. For example, assuming the mobile transmits one third (⅓) of the time, RECC transmission lasts one tenth of a second, and 84 access channels/codes combinations exist, approximately 7 unique RECC transmissions will be received for a throughput of 224 bits/minute. The minimum number of slave MINs required to implement this case would be 6.

[0088] Multi-Carriers Transmission

[0089] Consider a cellular network with j access channels/code combinations. In order to ensure reception by the network of the autonomous registration request under jamming conditions, it is necessary to transmit sequentially in time j copies of the autonomous registration request, once over each access channel/code combinations.

[0090] In order to increase the bandwidth of the jamming-resistant data uplink by a factor M, multi-carriers transmission can be used to enable the mobile station to radiate on M access channels simultaneously. **FIG. 4** illustrates the first illustrative embodiment with the multi-carriers transmission modification.

[0091] As illustrated in **FIG. 4**, the mobile station comprises a processor **401** for generating a bit stream for transmission to the remote station. This bit stream is transmitted through a first modulators 402_1 operating at the frequency of a first access channel carrier, a second modulators 402_2 operating at the frequency of a second access channel carrier, . . . a M^e modulators 402_M operating at the frequency of a M^e access channel carrier. The modulated outputs from the modulators 402_1, 402_2, . . . 402_M are processed through an adder **403** prior to being radiated toward the base station(s) of the AMPS network.

[0092] MIN Information Encoding

[0093] The selection of a given slave MIN can also be used to send information and to increase the throughput. If 2^N slave MINs were temporary assigned to a mobile station, an information block of N bits can be encoded to one of the 2^N slave MINs. For example, assuming N=10, the use of this encoding scheme can increase the throughput by 31%, as 10 information bits can be appended to the 32 bits already transmitted using the ESN on a given registration message.

[0094] Since the MIN identifies the remote station of the event monitoring service to which the security data has to be transmitted, the MIN is used by the Cellemetry server to return the ESN to this remote station of the event monitoring service (substep 206_3).

[0095] The remote station of the event monitoring service finally processes the received security data (substep 206_4).

[0096] Step **207**:

[0097] When all data have been sent, the transmission process is terminated. As long as there are data left to sent, transmitter **306** keeps transmitting data to the remote destination station.

[0098] GSM (Global System for Mobile Communications) Network:

[0099] In the second illustrative embodiment, as depicted in **FIG. 5**, the mobile station transmits information to a GSM wireless cellular telecommunication network.

[0100] More specifically, the transmission relies on the use of the GSM's RACH (Random Access Channel) to transmit security data, while a security GSM based mobile station is being jammed by a commercial jammer. The RACH is the only uplink channel in GSM that does not require timing advance information. The timing advance is an estimation of the propagation delay between a mobile station and its serving base station. The timing advance is calculated and sent by the base station.

[0101] The RACH is normally used to request an immediate assignment to initiate a call or during a handoff. The RACH is sent during an access burst, which contains a long guard band (equivalent 68,25 bits) which makes it immune to varying propagation delay.

[0102] Some modifications must be made by the operator to enable implementation of the second illustrative embodiment of the present invention. The following summarizes the principal changes:

[0103] a) The operator must synchronise its base stations (GPS network) together so that all time slots TS0 are sent at the same time. This requirement must already be implemented for an operator who wants to support EDGE (Enhanced Data rates for Global Evolution) compact, which was standardised in GSM Release 99.

[0104] b) The operator must use a regular frequency pattern, (i.e. 4/12 (clusters of 4 cells /12 sectors) or 3/9 (clusters of 3 cells /9 sectors) in order to use the new concept of fundamental frequency carriers. In the case of frequency pattern 4/12, 12 fundamental frequencies (one per sector) are defined by the GSM network so that a jammed mobile station knows "a priori" on which frequencies should the device send its RACH. Time slot TS0 of a fundamental frequency must be reserved for Common Control Channels. Time slot TS1 can be used for voice traffic or in priority for traffic of security data from one or more mobile stations being jammed. Many operators use this type of frequency allocation, where the Time Slot TS0 of the first 12 frequency carriers of its spectrum allocation are used for transmitting the BCCH (Broadcast Control Channel) on the downlink and RACH on the uplink.

[0105] c) The GSM network must be modified to correctly process the sequence 01100xxx sent over the RACH on the time slot TS0 of the fundamental frequencies, to enable access to the GSM network.

[0106] d) The GSM network must be modified to correctly group and route the security data.

[0107] Referring to the flow chart of **FIG. 5**, the operation of the second illustrative embodiment of the present invention will be described.

[0108] Step **501**:

[0109] The mobile station is in the idle GSM mode until a jammer or any other alarm (security breach) is not detected by step **502**.

[0110] Step **502**:

[0111] When the presence of a jammer (proximate the mobile station) or any other alarm is detected, the mobile station goes to step **503**. Otherwise, the mobile station remains in the idle GSM mode (step **501**).

[0112] Step **503**:

[0113] In response to detection of a jammer or alarm, a random number of three (3) bits is selected. This random number forms the last three (3) bits of the RACH for local identification, i.e. identification of the mobile station. More specifically, as indicated in substep $\mathbf{503}_1$, a bit stream including a reserved RACH sequence 01100xxx (ref. GSM04.08 R97) is generated and transmitted over the time slot TS0 of the fundamental carriers of the GSM system, where the term xxx represents the random number identifying the mobile station.

[0114] As indicated in the above modification b), time slot TS0 of a fundamental frequency is reserved for Common Control Channels. Time slot TS1 can be used for voice traffic or in priority for traffic of security data from one or more mobile stations being jammed or detecting an alarm. Many operators use this type of frequency allocation, where the time slot TS0 of the first 12 frequency carriers of its spectrum allocation are used for transmitting the BCCH.

[0115] The mobile station being jammed or detecting an alarm therefore registers in the GSM network through the time slot TS0 of the fundamental carriers. The GSM network then recognizes the reserved RACH sequence 01100xxx, to reserve or liberate the time slot TS1 of the fundamental carriers. The mobile station then proceeds with generating a bit stream suitable for transmitting the security data from the mobile station to the remote station of an event-monitoring service (substep $\mathbf{503}_2$) through the time slot TS1.

[0116] Step **504**:

[0117] Following transmission of the reserved RACH sequence to the GSM network, a waiting period is provided for to allow the network to free up the time slot TS1. This waiting period can be of the order of 100 ms.

[0118] Step **505**:

[0119] Then, the security data are sent in five (5) bits messages. This transmission of the security data comprises step **506**, and substeps $\mathbf{506}_1$, $\mathbf{506}_2$ and $\mathbf{506}_3$.

[0120] Step **506**:

[0121] The security data are sent on the first five (5) bits of RACH. The last three (3) bits are for local identification of the mobile station. More specifically, as indicated in subset $\mathbf{506}_1$, the time slot TS1 of the fundamental carriers of RACH is used for transmitting sequences pppppxxx, in which the term ppppp is the security data and xxx is used for discrimination; more specifically the term xxx will represent the above mentioned random number identifying the mobile station. Thereafter, the GSM network routes the security data associated with the local identification information xxx to the remote station (substep $\mathbf{506}_2$). The identification number of the remote station will be provided by the term ppppp of the first sequences pppppxxx. The security data are processed (substep $\mathbf{506}_3$) as soon as they reach the remote station of the event-monitoring service.

[0122] Step **507**:

[0123] The security data are processed until no data are left to send.

[0124] The above described illustrative embodiments of the present invention can be implemented for a plurality of different applications such as, for example:

[0125] Jamming-resistant alarm notification;

[0126] Jamming-resistant GPS tracking;

[0127] Jamming-resistant real-time vehicle tracking; and

[0128] Jamming-resistant real-time cargo tracking.

[0129] Also, the above described first and second illustrative embodiments can be used in connection with both cellular and satellite wireless telecommunication systems.

[0130] Although the illustrative embodiments of the present invention have been described in relation to AMPS and GSM wireless cellular telecommunication networks, it

should be kept in mind that the present invention can be equally applied to other cellular telecommunications standard such as CDMA.

[0131] Although the present invention has been described hereinabove with reference to illustrative embodiments thereof, it should be kept in mind that these illustrative embodiments can be modified at will, within the scope of the appended claims, without departing from the spirit and nature of the invention.

What is claimed is:

1. A jamming-resistant method for transmitting security data through a wireless telecommunication network from a first station to a second station remote from said first station, comprising:

determining, prior to transmission, common access channels of the wireless telecommunication network; and

transmitting the security data from the first station to the second station through a plurality of said common access channels of the wireless telecommunication network.

2. A jamming-resistant method as defined in claim 1, wherein the security data are transmitted from the first station to the second station without receiving local access parameters from the wireless telecommunication network at the time of transmission.

3. A jamming-resistant method as defined in claim 1, comprising:

detecting a security-breach event; and

transmitting the security data from the first station to the second station through the plurality of common access channels in response to detection of the security-breach event.

4. A jamming-resistant method as defined in claim 1, comprising:

detecting the presence of a jammer proximate the first station, said jammer producing an emission interfering with transmission from the wireless telecommunication network to prevent said transmission from the network to reach the first station; and

transmitting the security data from the first station to the second station through the plurality of common access channels in response to detection of the presence of a jammer.

5. A jamming-resistant method as defined in claim 1, wherein transmitting the security data comprises sending from the first station an autonomous registration frame to the plurality of common access channels of the wireless telecommunication network.

6. A jamming-resistant method as defined in claim 3, wherein the wireless telecommunication network is an AMPS network, and wherein the jamming-resistant method further comprises:

prior to detection of a security-breach event:

receiving AMPS parameters from the wireless telecommunication network;

updating the received AMPS parameters; and

keeping in memory the updated AMPS parameters; and

after detection of a security breach event:

storing the last updated AMPS parameters; and

sending an autonomous registration frame to the wireless telecommunication network through the plurality of common access channels of the network selected in relation to the last updated AMPS parameters.

7. A jamming-resistant method as defined in claim 6, further comprising:

determining, in relation to the last updated AMPS parameters, a first common access channel and a last common access channel defining a range of access channels including said plurality of common access channels.

8. A jamming-resistant method as defined in claim 5, wherein transmitting the security data from the first station to the second station comprises inserting the security data in the autonomous registration frame and transmitting said autonomous registration frame to the second station through the wireless telecommunication network.

9. A jamming-resistant method as defined in claim 8, wherein the autonomous registration frame comprises a mobile identification number, and transmitting the security data through the plurality of common access channels comprises transmitting successive sets of security data respectively inserted in successive autonomous registration frames through the plurality of common access channels using a rotation of a plurality of mobile identification numbers in the successive autonomous registration frames.

10. A jamming-resistant method as defined in claim 1, wherein transmitting the security data through the plurality of common access channels comprises using a plurality of access channel carriers for transmitting said security data through the plurality of common access channels, respectively.

11. A jamming-resistant method as defined in claim 8, wherein transmitting the security data through the plurality of common access channels comprises:

assigning at least one slave mobile identification number to the first station;

encoding information by means of said at least one slave mobile identification number; and

inserting said at least one encoded, slave mobile identification number in the autonomous registration frame.

12. A jamming-resistant method as defined in claim 8, comprising:

inserting in the autonomous registration frame a station identification number corresponding to the second station, and

transmitting the autonomous registration frame to the second station through the wireless telecommunication network in response to the station identification number.

13. A jamming-resistant method as defined in claim 12, wherein transmitting the autonomous registration frame to the second station comprises transmitting the autonomous registration frame to the second station through a Cellemetry virtual network.

14. A jamming-resistant method as defined in claim 1, wherein transmitting the security data through the plurality of common access channels comprises sending from the first station a random access channel sequence to the wireless telecommunication network.

15. A jamming-resistant method as defined in claim 14, wherein the wireless telecommunication network uses a plurality of fundamental frequency carriers each having first and second time slots, and wherein sending the random access channel sequence comprises sending the random access channel sequence through the first time slot of the fundamental frequency carriers.

16. A jamming-resistant method as defined in claim 15, further comprising inserting in the random access channel sequence a random number identifying the first station.

17. A jamming-resistant method as defined in claim 15, further comprising:

liberating the second time slot of the fundamental frequency carriers of the wireless telecommunication network in response to reception of the random access channel sequence; and

transmitting from the first station to the second station a second sequence including the security data through the second time slot of the fundamental frequency carriers.

18. A jamming-resistant method as defined in claim 17, further comprising inserting in the second sequence a random number identifying the first station.

19. A jamming-resistant system for transmitting security data through a wireless telecommunication network from a first station to a second station remote from said first station, wherein the wireless telecommunication network comprises common access channels, and wherein the jamming-resistant system comprises:

a transmitter of the security data from the first station to the second station through a plurality of said common access channels of the wireless telecommunication network.

20. A jamming-resistant system as defined in claim 19, wherein the transmitter comprises means for transmitting the security data from the first station to the second station without receiving local access parameters from the network at the time of transmission.

21. A jamming-resistant system as defined in claim 19, comprising a detector of a security-breach event, wherein the transmitter is responsive to said detection of the security-breach event for transmitting the security data from the first station to the second station through the plurality of common access channels.

22. A jamming-resistant system as defined in claim 19, comprising a detector of the presence of a jammer proximate the first station, said jammer producing an emission interfering with transmission from the network to prevent said transmission from the network to reach the first station, wherein the transmitter is responsive to detection of the presence of a jammer for transmitting the security data from the first station to the second station through the plurality of common access channels.

23. A jamming-resistant system as defined in claim 19, wherein the transmitter comprises means for sending from the first station an autonomous registration frame to the plurality of common access channels of the wireless telecommunication network.

24. A jamming-resistant system as defined in claim 21, wherein the wireless telecommunication network is an AMPS network, and wherein the jamming-resistant system further comprises:

prior to detection of a security-breach event:

means for receiving AMPS parameters from the network;

means for updating the received AMPS parameters; and

a memory for storing the updated AMPS parameters; and

after detection of a security-breach event:

a memory for storing the last updated AMPS parameters; and

means for sending an autonomous registration frame to the network through the plurality of common access channels of the network selected in relation to the last updated AMPS parameters.

25. A jamming-resistant system as defined in claim 24, further comprising:

a processor for determining, in relation to the last updated AMPS parameters, a first common access channel and a last common access channel defining a range of access channels including said plurality of common access channels.

26. A jamming-resistant system as defined in claim 23, wherein the transmitter comprises means for inserting the security data in the autonomous registration frame and transmitting said autonomous registration frame to the second station through the wireless telecommunication network.

27. A jamming-resistant system as defined in claim 23, wherein the autonomous registration frame comprises a mobile identification number, and the transmitter comprises means for transmitting successive sets of security data respectively inserted in successive autonomous registration frames through the plurality of common access channels using a rotation of a plurality of mobile identification numbers in the successive autonomous registration frames.

28. A jamming-resistant system as defined in claim 19, wherein the transmitter comprises means for transmitting said security data through the plurality of common access channels using respective access channel carriers.

29. A jamming-resistant method as defined in claim 23, wherein the transmitter comprises:

means for assigning at least one slave mobile identification number to the first station;

means for encoding information by means of said at least one slave mobile identification number; and

means for inserting said at least one encoded, slave mobile identification number in the autonomous registration frame.

30. A jamming-resistant system as defined in claim 26, comprising:

means for inserting in the autonomous registration frame a station identification number corresponding to the second station, and

means for transmitting the autonomous registration frame to the second station through the wireless telecommunication network in response to the station identification number.

31. A jamming-resistant system as defined in claim 30, wherein the autonomous registration frame is transmitted to the second station through a Cellemetry virtual network.

32. A jamming-resistant system as defined in claim 19, wherein the transmitter comprises means for sending from the first station a random access channel sequence to the wireless telecommunication network.

33. A jamming-resistant system as defined in claim 32, wherein the network uses a plurality of fundamental frequency carriers each having first and second time slots, and wherein the random access channel sequence is sent through the first time slot of the fundamental frequency carriers.

34. A jamming-resistant system as defined in claim 33, further comprising means for inserting in the random access channel sequence a random number identifying the first station.

35. A jamming-resistant method as defined in claim 33, further comprising:

means for liberating the second time slot of the fundamental frequency carriers in response to reception of the random access channel sequence; and

means for transmitting from the first station to the second station a second sequence including the security data through the second time slot of the fundamental frequency carriers.

36. A jamming-resistant system as defined in claim 35, further comprising means for inserting in the second sequence a random number identifying the first station.

* * * * *