METHOD FOR AUTHENTICATING DATA PACKETS RECEIVED BY A STATION OF A DIGITAL TELECOMMUNICATIONS SYSTEM

Background

The present invention belongs to the field of digital telecommunications, and more specifically relates to the authentication of data packets transmitted by terminals and received by a station.

State of the art

The authentication of data packets received by a station aims at verifying the identity of the terminal having transmitted the data packets.

Many authentication methods are known, which are generally applicable to deterministic tuned telecommunications systems. Such systems are:

- either based on bidirectional exchanges between a terminal and a station, by which the terminal and the station synchronize and mutually authenticate;
- or based on one-way exchanges between a terminal and a receiver station and on a deterministic time and/or frequency organization known beforehand, enabling to obtain the synchronization of the terminal and of the station.

Further, in this type of deterministic tuned system, the acceptable frequency error should be lower than or in the order of the system bandwidth.

Now, in a tuned telecommunications system, such as that discussed in document US 2001/004375, the terminals and the station consider a same predefined list of frequency bands in which the data packets can be transmitted. Thereby, in this type of system, it is possible to verify whether the predefined sequence of frequency hops has been respected by directly comparing the measured frequency band with the expected frequency band among the frequency bands of the predefined list.

This type of verification is no longer possible in non-tuned telecommunications systems since there is an incompatibility between the frequency bands used by the terminals and the theoretical frequency bands expected by the receiver station. This is all the

truer when the frequency synthesis means of the terminals have a significant frequency drift. Such non-deterministic systems comprise one-way components where communications are only possible from the terminal to the station. Such a telecommunications system where the drift of the frequency synthesis means of the terminals is greater than the instantaneous spectral width of the data packets transmitted by said terminals is disclosed in document WO 2011/154466.

It should thus be understood that the authentication methods developed for deterministic and tuned telecommunications systems cannot be applied to non-deterministic, non-synchronized, and non-tuned telecommunications systems, where the time and frequency organization of communications between the terminal and the station complies with no predetermination, synchronization, or tuning imperative. Further, in such non-tuned systems, the frequency error may be larger than the system bandwidth.

Further, conventional authentication methods generally rely on the inclusion in the data packets, in addition to a terminal identification code, of additional control data dedicated to authenticating said terminal having transmitted said data packets.

Adding such control data dedicated to the terminal authentication contributes to decreasing the ratio between the quantity of useful data and the quantity of control data present in each data packet. This ratio will be all the smaller as the quantity of useful data present in each data packet is small, as for example in the case of low-speed telecommunications systems.

Summary

The present invention aims at overcoming all or part of the limitations of prior art solutions, particularly those discussed hereabove, in the case of digital one-way non-deterministic telecommunications systems. In such systems, each terminal successively transmits data packets in a plurality of different frequency bands which are not predetermined, and according to a predefined frequency hop sequence specific to the terminal. Further, each data packet incorporates an identification code of the terminal having transmitted it.

For this purpose, and according to a first aspect, the invention relates to an authentication method comprising, for each data packet received by a receiver system comprising at least one station:

- the measurement, by the station having received the considered data packet, of the frequency band in which the considered data packet has been received,
- extracting the identification code contained in the considered data packet,
- calculating a frequency hop, based on the measured frequency band of the considered packet and on a frequency band measured by the receiver system for a previous received data packet incorporating an identification code identical to the extracted identification code,
- determining, according to the predetermined frequency hop sequence associated with the identification code extracted from the considered data packet, a theoretical frequency hop applied from the previous received data packet, and
- calculating a frequency hop deviation according to the theoretical frequency hop and to the calculated frequency hop.

Further, the authentication method comprises a step of determining whether the data packets successively received with a same identification code have been transmitted by the terminal associated with the extracted identification code according to at least one frequency hop deviation calculated for one of the data packets.

As a summary, for each data packet, a frequency hop deviation is calculated according to the theoretical frequency hop, to the frequency band measured for the considered data packet, and to the frequency band measured for the previous data packet received with the same identification code. The authentication method is thus robust to the possible absence of tuning between the terminals and the station.

The receiver system according to the invention may be formed either of an assembly formed of one or a plurality of stations, or of an assembly formed of one or a plurality of stations in cooperation with a processing server.

Thus, the transmit frequency band of the considered data packet is measured in the reference frame of the station having received the considered data packet. Thereby, in the

case where the receiver system particularly comprises a plurality of stations, each station will measure the frequency bands of the packets that it receives. Such frequency band measurements are thus obtained independently from the conditions of transmission by the terminal and from the differences in receive conditions between stations.

Further, in certain extreme receive conditions, a frequency variation in the receive reference frame can be observed during the reception of a same packet. This results in an ambiguity in the calculation of the frequency hop deviation. In such conditions, the authentication decision may be based on the accumulation of the deviations of a plurality of successively-calculated frequency hops, or any other statistical operation applied to a series of successively-calculated frequency hop deviation values.

In a variation, it is also possible to develop a training system based on the history of the calculated deviations, and to dynamically adjust the threshold criterion relative to the maximum acceptable difference between deviations.

Such provisions enable to discard data packets transmitted by a malicious terminal pretending to be an authorized terminal. It should indeed be understood that if a malicious terminal pretends to be an authorized terminal by using the identification code of said authorized terminal, without however knowing the predefined frequency hop sequence associated with said authorized terminal, the calculated frequency hop deviation(s) will be important and will enable to determine that all or part of these data packets have been transmitted by a malicious terminal.

The authentication method forming the object of the invention is particularly adapted to non-tuned telecommunications systems, that is, systems where the terminal and the station are not frequency-synchronized. Further, such an authentication requires no manifest prerequisite as to the telecommunications system, and can thus be applied by extension to any telecommunications system, be it one-way or not, tuned or not, synchronized or not.

It should further be noted that such an authentication method is particularly adapted to low-speed telecommunications systems.

As an illustrative example, a terminal systematically transmitting with a frequency bias δF relative to the receiver station is considered, that is, said terminal transmits in a frequency band F1+δF when it is intended to transmit in a frequency band F1, and then in a frequency band F2+δF instead of F2 (F2 being equal to F1+ΔF, ΔF being the theoretical frequency hop), etc. In this case, the frequency band deviation, that is, the deviation between the frequency band in which the terminal transmits and the theoretical frequency band expected by the station, is always substantially equal to δF (to within measurement errors when the environmental conditions are equivalent, in terms of temperature and voltage). The frequency hop deviation is substantially zero (to within measurement errors) since the frequency hop between frequency band F1+δF and frequency band F2+δF is equal to theoretical frequency hop ΔF.

In specific embodiments, the authentication method comprises one or a plurality of the following characteristics, taken separately or according to all technically possible combinations.

In a specific embodiment, the frequency band of a data packet is measured a plurality of times during each data packet, and the frequency hop deviation is calculated by considering the final measured frequency band of the considered data packet and the final measured frequency band of the previous data packet incorporating the same identification code as the considered data packet.

Such provisions enable to avoid certain cases of authentication failures, particularly in the case of terminals with a significant frequency drift of its frequency synthesis means (such as for example disclosed in document WO 2011/154466), and with a frequency band used by a terminal which may non-negligibly vary within a same data packet.

In this case, the frequency drift behavior on turning-on of an oscillator of a transmit terminal provides a specific unique pattern, which is perfectly repeatable, and which can be modeled in time. This specific pattern forms a sort of "signature" which depends on the unique assembly of the electronic components in the transmit terminal. In practice, advantage may advantageously be taken from this signature by considering the frequency band measured at the end of the considered data packet and the frequency band measured

at the end of the previous data packet incorporating the same identification code, and thus having the same frequency drift pattern (any other environmental parameter being considered as constant). It should be understood that the frequency band variations on two frames, successive or not, of same length, will be identical if they are measured at the same time with respect to the turning-on of the circuits of the transmit terminal.

Thereby, to reinforce the authentication method forming the object of the invention, it is possible to implement complementary steps by using the frequency drift of the oscillator of the transmit terminal. Thus, advantageously, the authentication method may further comprise, for each data packet received by the receiver system:

- the measurement, by the receiver system, of a frequency drift pattern of an oscillator having been used to generate the considered data packet, and
- comparing the measured frequency drift pattern with a predefined frequency drift pattern associated with said identification code extracted from said considered data packet.

In particular, in a context where the battery of the transmit terminal is desired to be saved, it is not desirable to turn on the oscillator long before the sending of a frame, to leave time for the oscillator to stabilize. Thereby, in such a context of economy, the oscillator is generally activated just at the time of the sending of the frame and the frame thus necessarily contains the "signature" representative of the frequency drift of the oscillator.

For example, the frequency band of a data packet may be measured a plurality of times during each data packet. Such multiple measurements may thus be used to create the model of the specific unique frequency drift behavior pattern of the transmit terminal, that is, its "signature", on the given packet. This model may then be compared with a unique reference pattern known by the transmit terminal having transmitted the packet and recorded for example on manufacturing thereof or on putting into service thereof.

In practice, to be able to determine the theoretical frequency hop corresponding to two sequentially-received packets, it is advantageous to make sure that these two packets having been transmitted sequentially. When lost frames are detected, it is advantageous to

recalculate the theoretical frequency hop deviation according to the number of lost frames.

Thus, in a specific embodiment, the authentication method comprises, after the step of extracting the identification code from the considered data packet, a step of estimating a number of lost data packets, said lost data packets corresponding to data packets which have been transmitted by the terminal associated with said identification code since the previous data packet incorporating said identification code has been received, but which have not been received by the receiver system, and particularly by the station. The theoretical frequency hop for the considered data packet is then determined according to the number of lost data packets and to the sequence of frequency hops associated with said identification code.

Such provisions also enable to avoid certain cases of authentication failures. Indeed, the frequency hop between two data packets received by the station may correspond to the sum of a plurality of consecutive frequency hops, if data packets have been transmitted between said two data packets but have not been received by the station. The estimation of the number of lost packets then enables to determine the number of frequency hops performed, and accordingly to estimate the theoretical frequency hop as being the sum of said performed frequency hops.

In a specific embodiment, wherein said data packets incorporate a counter incremented by the terminal for each new transmission, the number of lost packets is estimated according to the counter of the considered data packet and to the counter of the previous received data packet incorporating the same identification code as said considered data packet.

In a specific embodiment, wherein said data packets comprise a portion ciphered by means of a rolling code incremented by the terminal for each new transmission, the number of lost packets is estimated according to the rolling code used for the considered data packet and to the rolling code used for the previous received data packet incorporating the same identification code as said considered data packet.

In a specific embodiment, wherein the data packets are transmitted by a terminal with a predefined period, the number of lost packets is estimated according to said period and to a time interval between the reception of the considered data packet and the reception of the previous data packet incorporating the same identification code as said considered data packet.

In a specific embodiment, the data packets successively received with a same identification code are only considered as having been transmitted by the terminal associated with said identification code if each frequency hop deviation considered for the authentication has an absolute value smaller than a threshold value.

Preferably, the threshold value to be used for the considered data packet is determined according to a time interval between the reception of the considered data packet and the reception of the previous data packet incorporating the same identification code as said considered data packet.

In a specific embodiment wherein a plurality of frequency hop deviations are considered for the authentication, the data packets successively received with a same identification code are only considered as having been transmitted by the terminal associated with said identification code if a predefined authentication criterion is verified by all the frequency hop deviations considered for the authentication.

In other words, the packet validity diagnosis may be delayed until a general validation criterion is achieved, this statistical criterion validating in retrospect all the packets waiting to be validated. In such conditions, the system is sometimes waiting for a validation of a sub-set of packets.

In a specific embodiment, the authentication criterion is verified if the accumulation of the frequency hop deviations considered for the authentication is smaller than a predefined threshold value.

Advantageously, the verification of the authentication criterion may also be based on the expectation, the variance, or any other statistical property on the frequency hop deviations considered for the authentication.

In a specific embodiment, the receiver system may comprise a backbone cooperating with one or a plurality of station(s). In this case, the operations of the authentication method are preferably distributed between the backbone and the station(s).

Preferably, the station measures the frequency band of the data packets that it receives, and the backbone collects all the data packets received by each station and the frequency bands measured by each station, and carries out at least the remaining operations of the above-discussed authentication method.

According to a second aspect, the invention relates to a computer program product comprising a set of program code instructions which, when they are executed by a processor, implement an authentication method according to the invention.

According to a third aspect, the present invention relates to a receiver system comprising at least one station of a digital telecommunications system, capable of receiving data packets transmitted by terminals, each data packet incorporating an identification code of the terminal having transmitted said data packet, each terminal successively transmitting data packets in a plurality of different frequency bands according to a predefined frequency hop sequence specific to said terminal. The receiver system further comprises means configured to authenticate the received data packets in accordance with a method according to the invention.

In an alternative implementation allowing a scalable deployment, the receiver system may comprise stations capable of receiving the packets transmitted by the terminals and a backbone. Each station preferably comprises means of communication with the backbone and means for performing part of the authentication method according to the invention. The backbone preferably comprises means for performing the other part of the method of authenticating received data packets according to the invention.

According to a fourth aspect, the present invention relates to a telecommunications system comprising:

- terminals, each terminal being capable of successively transmitting data packets in a plurality of different frequency bands according to a predefined frequency hop sequence specific to said terminal (10) having transmitted said data packet,
- stations cooperating with a backbone to carry out the authentication method according to the invention,
    - each station being capable of measuring the frequency bands of the data packets that it receives; and
    - the backbone being capable of collecting all the data packets received by each station and the frequency bands measured by each station, and being capable of carrying out at least the remaining operations of the authentication method according to the invention which are not carried out by the station.

Description of the drawings

The invention will be better understood on reading of the following description, given as a non-limiting example, in relation with the drawings, which show:

- Figure 1: a simplified representation of a digital telecommunications system, and
- Figure 2: a diagram illustrating the steps of an embodiment of an authentication method according to the invention.

Detailed discussion of a specific embodiment

Figure 1 very schematically shows a telecommunications system comprising one or a plurality of transmitters such as terminals **10** and one or a plurality of stations **20** (a single station has been shown in Figure 1 for clarity). In the context of the invention, "station" generally means any device capable of receiving data packets in the form of radioelectric signals. Station **20** is for example a specific device such as an access point of a wired or wireless telecommunications network.

"Radioelectric signal" means an electromagnetic wave propagating via wireless means having frequencies in the conventional spectrum of radioelectric waves (from a few hertz to several hundreds of gigahertz) or in neighboring frequency bands.

It should be noted that the case of a data packet transmission from terminals **10** to station **20** is mainly considered. The possible transmission of data packets by station **20** to terminals **10** is not comprised within the scope of the invention.

Terminals **10** transmit data packets to station **20** in a shared frequency resource, called "macrochannel" (or signal multiplexing band corresponding to the receive band of the station) in telecommunications networks, having a spectral width ΔM.

The data packets are transmitted by terminals **10** in frequency bands of predefined spectral width ΔB smaller than ΔM. Preferably, spectral width ΔM of the macrochannel is significantly greater than spectral width ΔB, to be able to multiplex a large number of terminals **10**. For example, spectral width ΔM is at least one hundred times greater than spectral width ΔB.

Each terminal **10** recurrently transmits data packets to station **20**. Data packets successively transmitted by a same terminal **10** are transmitted in different frequency bands according to a predefined frequency hop sequence specific to said terminal **10**. Further, each data packet incorporates an identification code of the terminal **10** having transmitted said data packet.

In a variation, a backbone **40** may be associated with stations **20** as illustrated in Figure 1.

Thereby, hereafter, term "transmitter" will relate to a terminal **10**, and term "receiver system" will indifferently relate to a station or to an assembly formed of at least one station in cooperation with a backbone.

Further, in the following description, the terminals are designated with the same reference **10**. When it is necessary to distinguish a terminal from another terminal, an alphabetic index specific to the considered terminal is appended to the corresponding reference numeral. For example, a generally-considered terminal will be designated by **10**, while terminals **10a**, **10b**, **10c**, etc. will correspond to specific terminals.

According to a non-limiting example, a terminal **10a** is configured to transmit in successive frequency bands defined by a base frequency band Fa and a sequence Sa comprising (N-1) successive frequency hops Sa = $\{\Delta Fa_1, \Delta Fa_2, \ldots, \Delta Fa_{N-1}\}$. Thus, terminal **10a** first transmits a data packet in frequency band Fa, then in frequency band $(Fa+\Delta Fa_1)$, and then in frequency band $(Fa+\Delta Fa_1+\Delta Fa_2)$, etc. The set of frequency hops of sequence Sa is for example selected to be such that:

$$\sum_{n=1}^{N-1} \Delta Fa_n = 0$$

so that, after having applied all the frequency hops of sequence Sa, terminal **10a** transmits again, theoretically, in base frequency band Fa.

Similarly, terminal **10b** is associated a base frequency band Fb and a specific sequence Sb of (M-1) successive frequency hops Sb = $\{\Delta Fb_1, \Delta Fb_2, \ldots, \Delta Fb_{M-1}\}$, a terminal 10c is associated a base frequency band Fc and a specific sequence Sc of (P-1) successive frequency hops Sc = $\{\Delta Fc_1, \Delta Fc_2, \ldots, \Delta Fc_{P-1}\}$, etc.

Lengths M, N, P, and generally any sequence length may be selected independently and arbitrarily. In particular, they may be selected to be arbitrarily large, so that the sequence does not exhibit such an apparent repetitive cycle.

The frequency hop sequence of terminal **10** (that is, sequence Sa of terminal **10a**, sequence Sb of terminal **10b**, sequence Sc of terminal **10c**, etc.) may be obtained either by station **20**, or by server **40** (backbone). For example, station **20** may comprise an electronic memory **30** having a look-up table associating, with each possible identification, the corresponding frequency hop sequence stored therein. Of course, this look-up table may be stored in server **40**.

A preferred implementation is that where each station **20** receives and measures the frequency band, and server **40** collects all the packets and the frequency measurements measured by the station(s) **20**, and carries out the authentication operation by comparatively using all the results to consolidate and reliabilize the diagnosis.

In the above example, the frequency hop sequences are cyclic, apparently or not. Nothing precludes, according to other examples, having non-cyclic frequency hop sequences, for example, generated by means of a linear feedback shift register or LFSR with predefined generating polynomial(s) which may be obtained by station **20**.

The following description relates, without this being a limitation, to a digital telecommunications system such as described in international application WO 2011/154466, where the data packets have a narrow band (spectral width ΔB in the range from a few hertz to a few hundreds of hertz) and the frequency drift of the frequency synthesis means of the terminals is greater than spectral width ΔB.

Accordingly, terminal **10a**, when it theoretically transmits in base frequency band Fa, practically transmits in a frequency band F'a which may be separated from base frequency band Fa by a spectral width greater than ΔB. Similarly, frequency hops $\{\Delta F'a_1, \Delta F'a_2, \ldots, \Delta F'a_{N-1}\}$ may differ from frequency hops $\{\Delta Fa_1, \Delta Fa_2, \ldots, \Delta Fa_{N-1}\}$. However, the error in the frequency hop is much lesser than that in the frequency band. Indeed, in a non-tuned system where the station performing the frequency band measurements has a frequency accuracy of 10 ppm, for example, neither corrected nor compensated for by a synchronization mechanism, the frequency error induced for base frequency band Fa around 1 GHz is 10 kHz, while the frequency error on a 10-kHz hop is 0.1 Hz only. Accordingly, the value of the frequency hop is perfectly discriminating, while frequency Fa itself is not.

It should thus be understood that an advantage of the authentication method of the present invention is that neither station **20** nor server **40** (backbone), although they have access to the frequency hop sequences of each terminal **10**, neither can nor need to directly discriminate the frequency band in which a terminal **10** has transmitted a packet for authentication purposes. This authentication method fundamentally differs from deterministic methods such as described in document US2001/0004375, which are based on frequency measurement and discrimination to authenticate the packets.

In a specific embodiment, station **20** comprises an analog receiver unit and a digital receiver unit.

The analog receiver unit is capable of receiving a general signal corresponding to all the radioelectric signals received in the macrochannel. For this purpose, it comprises a set of means, considered as known by those skilled in the art (antennas, analog filters, amplifiers, local oscillators, mixers, etc.), capable of shifting the frequency of the general signal.

The analog receiver unit outputs an analog signal corresponding to the general signal shifted around an intermediate frequency lower than the central frequency of the multiplexing band, and which may be zero.

The digital receiver unit conventionally comprises one or a plurality of analog-to-digital converters (A/D) capable of sampling the analog signals delivered by the analog receiver unit to obtain a digital signal.

The digital receiver unit further comprises a unit for processing the digital signal at the output of the A/D converters. The processing unit detects, from the digital signal, data packets transmitted by terminals **10** and present in the general signal. The processing unit also executes the steps of a method **50** of authenticating the detected data packets, described in further detail hereafter.

In a preferred variation, authentication method **50** may be distributed between a calculation unit allocated by server **40** and a calculation unit of station **20**.

The processing unit for example comprises a processor and an electronic memory having a computer program product stored therein, in the form of a set of program code instructions which, when they are executed by the processor, implement all or part of the steps of an authentication method **50**. In a variation, the processing unit comprises programmable logic circuits, of FPGA, PLD, etc., type and/or application-specific integrated circuits (ASICs), capable of implementing all or part of the steps of an authentication method **50**.

Figure 2 shows a preferred embodiment of a method **50** of authenticating data packets received by station **20**.

Authentication method **50** comprises steps which are executed by the receiver system for each received data packet, the main steps being:

- **51** measuring the frequency band where the considered data packet has been received,
- **52** extracting the identification code from said considered data packet,
- **55** determining a theoretical frequency hop according to the frequency hop sequence associated with said identification code extracted from the considered data packet,
- **56** calculating a frequency hop difference according to the theoretical frequency hop, to the frequency band measured for the considered data packet, and to the frequency band measured for the previous received data packet incorporating the same identification code as said considered data packet.

During measurement step **51**, station **20** measures the frequency band of the considered data packet, called "Fe" hereafter, and then extracts the identification code during extraction step **52**, called "Ce" hereafter.

For the description of the embodiment illustrated in Figure 2, the case where identification code Ce extracted from the considered data packet corresponds to the identification code associated with terminal **10a** is considered, without this being a limitation.

Based on identification code Ce, the calculation unit, located either in station **20** or in server **40** (backbone), obtains the frequency hop sequence associated with said identification code Ce, previously stored in electronic memory **30**, and obtains sequence Sa of frequency hops associated with terminal **10a**.

The calculation unit also obtains data relative to the previous data packet received with identification code Ce, that is, in the present case, received from terminal **10a**. These data have been previously stored in the database of the network, as a result of the execution of the steps of authentication method **50** for a previous data packet received from terminal **10a**.

Particularly, the calculation unit obtains the frequency band measured for the previous data packet during measurement step **51** and stored in electronic memory **30**, called "Fep" hereafter.

In the specific embodiment illustrated in Figure 2, the case where each terminal **10** incorporates in a transmitted data packet a counter which is incremented for each new transmission by said terminal is considered, without this being a limitation. For example, when terminal **10a** transmits a data packet in base frequency band Fa, the counter is equal to 0, when it transmits the next data packet (in frequency band Fa+ΔF1a), the counter is equal to 1, etc. In this case, authentication method **50** may comprise a step **53** of extracting the counter from the considered data packet, called "sn" hereafter.

In this case, the data, obtained by station **20** from identification code Ce in electronic memory **30**, also comprise the counter of the previous data packet received with identification code Ce, called "snp" hereafter.

In the specific embodiment illustrated in Figure 2, authentication method **50** further comprises a step **54** of estimating the number of lost packets, called "δsn" hereafter. The lost data packets correspond, in the present case, to data packets which have been transmitted by terminal **10a** since the previous data packet received from terminal **10a** has been received, but which have not been received by station **20**.

Number δsn of lost data packets may be estimated according to counter sn extracted from the considered data packet and to counter snp extracted from the previous data packet received with the same identification code Ce. For example, if counter sn is equal to n (modulo N) and if counter snp is equal to (n-d) (modulo N, $d \geq 1$), then number δsn of lost packets is equal to (d-1) and may be equal to zero.

During step **55**, station **20** calculates a theoretical frequency hop, called "ΔFt" hereafter, according to sequence Sa of frequency hops obtained from identification code Ce extracted from the considered data packet. Theoretical frequency hop ΔFt corresponds to

the frequency hop theoretically applied since the transmission of the previous data packet received with the same identification code Ce.

Theoretical frequency hop ΔFt, in the example illustrated in Figure 2, is also calculated according to counters sn (equal to n) and snp (equal to (n-d)). In the considered case of data packets received from terminal **10a**, theoretical frequency hop ΔFt is for example calculated according to the following expression:

$$\Delta Ft = \sum_{k=sn-\delta sn}^{sn} \Delta Fa_k$$

For example, if sn = 4 and (sn-δsn) = 4 (that is, no data packet has been lost), theoretical frequency hop ΔFt is equal to ΔFa_4. If sn = 4 and (sn-δsn) = 3 (that is, no data packet has been lost), theoretical frequency hop ΔFt is equal to (ΔFa_3+ΔFa_4), etc.

During step **56**, station **20** calculates a frequency hop deviation, called "δe" hereafter.

In the specific embodiment illustrated in Figure 2, authentication method **50** further comprises a step **57** of calculating a real frequency hop, called "ΔFe" hereafter. Real frequency hop ΔFe is calculated according to measured frequency band Fe and to measured frequency band Fep, for example, according to expression ΔFe = Fe – Fep. In this case, frequency hop deviation δe is calculated as being a distance between theoretical frequency hop ΔFt and real frequency hop ΔFe, for example, according to expression δe = ΔFe – ΔFt.

Nothing precludes, according to other examples, calculating frequency hop deviation δe differently. In a variation, not shown in drawings, authentication method **50** comprises a step of calculating a theoretical frequency band where the considered data packet should have been received, called "Ft" hereafter. Theoretical frequency band Ft is calculated according to theoretical frequency hop ΔFt and to measured frequency band Fep, for example, according to expression Ft = Fep + ΔFt. In this case, frequency hop deviation δe is calculated as being a distance between measured frequency band Fe and theoretical frequency band Ft, for example, according to expression δe = Fe – Ft.

Preferably, in particular when the frequency drift of the frequency synthesis means of terminals **10** is large, the frequency band of the considered data packet is measured a plurality of times during said considered data packet. For example, during measurement step **51**, the frequency band is measured L times, to obtain respectively measured frequency bands Fe_1 (first measurement), Fe_2, …, Fe_L (last measurement). Similarly, for the previous data packet, a plurality of measurements are performed to obtain respectively measured frequency bands Fep_1 (first measurement), Fep_2, …, Fep_L (last measurement). In this case, frequency hop deviation δe is advantageously calculated by considering measured frequency band Fe_L of the considered data packet and measured frequency band Fep_L of the previous data packet incorporating the same identification code as said considered data packet. In the case illustrated in Figure 2, this amounts to calculating real frequency hop ΔFe according to expression $\Delta Fe = Fe_L - Fep_L$.

Nothing however precludes, when the frequency band of the considered data packet is measured a plurality of times during a same data packet, considering according to other examples equivalent times of the considered data packet and of the previous data packet. For example, real frequency hop ΔFe may be calculated by considering the first measurements (according to expression $\Delta Fe = Fe_1 - Fep_1$) or any other measurement (according to expression $\Delta Fe = Fe_i - Fep_i$).

When the frequency drift of the frequency synthesis means of terminals **10** is significant, it is possible to identify the terminal from the signature of its frequency drift at the turning-on. Indeed, as known by those skilled in the art, the frequency drift behavior at the turning-on of an electronic device synthesizing a radioelectric frequency exhibits a unique pattern which depends on the unique assembly of the electronic components forming it. Based on measurements Fe_i, this single pattern may be restored by a mathematical operation, for example, an interpolation, and it may be compared with the theoretical drift pattern stored in a database for this device.

Authentication method **50** further comprises a step **58** of determining whether the data packets successively received with a same identification code have been transmitted by terminal **10** associated with said identification code according to at least one frequency hop deviation δe calculated for one of said data packets.

Preferably, a plurality of frequency hop deviations, calculated for different data packets received with a same identification code, are considered during determination step **58** to improve the robustness of the authentication. In the following description, the case where M frequency hop deviations (respectively δe_1, δe_2, …, δe_M) are considered during determination step **58** is considered.

In a specific embodiment of determination step **58**, the data packets successively received with a same identification code are only considered as having been transmitted by the terminal **10** associated with said identification code if each frequency hop deviation δe_1, δe_2, …, δe_M has an absolute value smaller than a threshold value. The threshold value is for example predefined according to the maximum frequency drifts observed according to the environmental conditions (temperature) for the frequency synthesis means of terminals **10**.

As a numerical example, the above-discussed example is considered, that is, a non-tuned system wherein:

- the receiver station has an initial frequency accuracy of 10 ppm ("parts per million"), which is not compensated for by a synchronization mechanism, the frequency error induced for Fa = 1 GHz is 10 kHz,
- the terminal transmits packets of spectrum occupancy ΔB = 100 Hz, and
- the temperature variation is typically 10 ppm in the authorized range or 0.1 ppm per degree.

In this case, from one packet to the other, a typical variation of 10°C of the temperature conditions around the work temperature will induce between two packets a hop deviation of 0.1 Hz + 1 kHz. The threshold value to be applied in this case is around 1 kHz. In specific conditions of implementation, an extreme variation of the temperature conditions will induce between two packets a hop deviation of 0.1 Hz + 10 kHz. The hop deviation is then no longer discriminating per se, it is thus preferable to adapt the authentication system and to apply a general analysis over a large set of packets successively received by the network. In this case, the analysis may be carried out on the statistical behavior of the received data packets, in particular over all the hop deviations, having an expectation and a variance, when they have realistic statistical values, which will validate

all the packets received until the statistic criterion is achieved. However, if a deviation or if a series of deviations of frequency hops δe_1, δe_2, …, δe_M is too large, the data packets successively received with the same identification code will not be considered as having been transmitted by the terminal **10** associated with said identification code and the authentication will fail.

In another specific embodiment of determination step **58**, capable of being combined with the previous one, the data packets successively received with the same identification code are only considered as having been transmitted by the terminal **10** associated with said identification code if a predefined authentication criterion is verified by all said frequency hop deviations δe_1, δe_2, …, δe_M considered for the authentication.

For example, the authentication criterion is verified if the accumulation (sum in absolute or relative value) of the frequency hop deviations δe_1, δe_2, …, δe_M considered for the authentication is smaller than a predefined threshold value.

In addition to the previously-described operations, it is possible to independently implement a step **59** taking into account the frequency drift pattern of the oscillator which has been used to generate the considered data packet, to reinforce the authentication method. Step **59** may particularly comprise:

- measuring the frequency drift pattern of the oscillator which has been used to generate the considered data packet, and then
- comparing this measured frequency drift pattern with a predefined frequency drift pattern associated with said identification code extracted from said considered data packet.

More generally, it should be noted that the embodiments considered hereabove have been described as non-limiting examples, and that variations may accordingly be envisaged.

It should in particular be noted that authentication method **50** may be considered alone or in combination with other authentication methods, to reinforce the robustness of the authentication. For example, the data packets may comprise a portion ciphered by

means of a rolling code. A conventional authentication based on the use of rolling codes may be combined with an authentication based on the verification, according to the invention, of the frequency hop sequence.

Further, an estimation of the number of lost packets according to a counter incorporated in the data packets has been described hereabove.

Nothing precludes, according to other examples, estimating the number of lost packets in another way. According to a non-limiting example, if a portion of the data packets is ciphered with a rolling key incremented by the terminal for each new transmission, station **20** may increment the rolling key that it uses to attempt to decipher the considered data packet until a rolling key enabling to successfully decipher said considered data packet is obtained. The number of lost data packets is then estimated according to the rolling key enabling to decipher the considered data packet and according to the rolling key which has enabled to decipher the previous received data packet incorporating the same identification code as said considered data packet.

CLAIMS

1. A method (50) of authenticating data packets transmitted by terminals (10) and received by a receiver system (20) comprising at least one station, each data packet incorporating an identification code of the terminal (10) having transmitted said data packet, each terminal (10) successively transmitting data packets in a plurality of different frequency bands according to a predefined frequency hop sequence specific to said terminal,

characterized in that it comprises, for each data packet received by said receiver system (20):

- (51) the measurement, by said station, of the frequency band in which the considered data packet has been received,
- (52) extracting the identification code contained in said considered data packet,
- calculating a frequency hop, based on said measured frequency band of the considered packet and on a frequency band measured by the receiver system for a previous received data packet incorporating said extracted identification code,
- (55) determining, according to the predetermined frequency hop sequence associated with said identification code extracted from the considered data packet, a theoretical frequency hop applied from said previous received data packet,
- (56) calculating a frequency hop difference according to said theoretical frequency hop and to said calculated frequency hop,

and in that the authentication method (50) further comprises a step (58) of determining whether the data packets successively received with a same identification code have been transmitted by the terminal (10) associated with said identification code according to at least one frequency hop deviation calculated for one of said data packets.

2. The method (50) of claim 1, characterized in that the frequency band of a data packet is measured a plurality of times during said considered data packet, the frequency hop deviation being calculated by considering the final measured frequency band of the considered data packet and the final measured frequency band of the previous data packet incorporating the same identification code as said considered data packet.

3. The method (50) of any of the foregoing claims, characterized in that it comprises, after the step (52) of extracting the identification code from the considered data packet, a

step (54) of estimating a number of lost data packets, said lost data packets corresponding to data packets which have been transmitted by the terminal (10) associated with said identification code since the previous data packet incorporating said identification code has been received, but which have not been received by the receiver system (20), the theoretical frequency hop for the considered data packet being determined according to the number of lost data packets and to the frequency hop sequence associated with said identification code.

4. The method (50) of claim 3, characterized in that the data packets incorporating a counter incremented by the terminal (10) for each new transmission, the number of lost packets is estimated according to the counter of the considered data packet and to the counter of the previous received data packet incorporating the same identification code as said considered data packet.

5. The method (50) of claim 3, characterized in that the data packets comprising a portion ciphered by means of a rolling code incremented by the terminal (10) for each new transmission, the number of lost packets is estimated according to the rolling code used for the considered data packet and to the rolling code used for the previous received data packet incorporating the same identification code as said considered data packet.

6. The method (50) of claim 3, characterized in that the data packets being transmitted by a terminal (10) with a predefined period, the number of lost packets is estimated according to said period and to a time interval between the reception of the considered data packet and the reception of the previous data packet incorporating the same identification code as said considered data packet.

7. The method (50) of any of the foregoing claims, characterized in that the data packets successively received with a same identification code are only considered as having been transmitted by the terminal (10) associated with said identification code if each frequency hop deviation considered for the authentication has an absolute value smaller than a threshold value.

8. The method (50) of claim 7, characterized in that the threshold value to be used for the considered data packet is determined according to a time interval between the reception of said considered data packet and the reception of the previous data packet incorporating the same identification code as said considered data packet.

9. The method (50) of any of the foregoing claims, characterized in that a plurality of frequency hop deviations being considered for the authentication, the data packets successively received with a same identification code are only considered as having been transmitted by the terminal (10) associated with said identification code if a predefined authentication criterion is verified by all of said frequency hop deviations considered for the authentication.

10. The method (50) of claim 9, characterized in that the authentication criterion is verified if the accumulation of the frequency hop deviations considered for the authentication is smaller than a predefined threshold value.

11. The method (50) of any of the foregoing claims, characterized in that it further comprises, for each data packet received by said receiver system:

- the measurement, by the receiver system, of a frequency drift pattern of an oscillator having been used to generate the considered data packet, and
- comparing the measured frequency drift pattern with a predefined frequency drift pattern associated with said identification code extracted from said considered data packet.

12. The method (50) of any of the foregoing claims,

characterized in that the receiver system comprises a backbone cooperating with at least one station,

and in that the operations of the authentication method are distributed between said station and said backbone.

13. The method (50) of claim 12, characterized in that:

- the station measures the frequency bands of the data packets that it receives;

- the backbone collects all the data packets received by each station and the frequency bands measured by each station, and carries out at least the remaining operations of the authentication method.

14. A computer program product, characterized in that it comprises a set of program code instructions which, when they are executed by a processor, implement the authentication method (50) of any of the foregoing claims.

15. A receiver system of a digital telecommunications system, capable of receiving data packets transmitted by terminals (10), said receiver system comprising at least one station, each data packet incorporating an identification code of the terminal (10) having transmitted said data packet, each terminal (10) successively transmitting data packets in a plurality of different frequency bands according to a predefined frequency hop sequence specific to said terminal, characterized in that it comprises means configured to authenticate the received data packets according to the method of any of claims 1 to 13.

16. A telecommunications system comprising:

- terminals, each terminal being capable of successively transmitting data packets in a plurality of different frequency bands according to a predefined frequency hop sequence specific to said terminal, each data packet incorporating an identification code of the terminal (10) having transmitted said data packet,
- stations cooperating with a backbone to carry out the authentication method of any of claims 1 to 13,
    - each station being capable of measuring the frequency bands of the data packets that it receives; and
    - the server being capable of collecting all the data packets received by each station and the frequency bands measured by each station, and being capable of carrying out at least the remaining operations of said authentication method.