

Method for providing a wireless user station for access to a telecommunication network through a network wireless access point, associated network wireless access point and wireless user station

5 The present invention generally relates to telecommunication network including wireless access points and implementing authenticating scheme between wireless access points and wireless user stations before providing telecommunication services to the wireless user stations through the wireless access points.

10 The invention relates more particularly to a method for providing a wireless user station for access to a telecommunication network through a network wireless access point, including the steps of :

- deriving, by each of the wireless user station and the wireless network access point, a second key from at least a first key shared by the wireless user station and the network access point;
 - 15 - performing, through wireless communication, an authenticating step between wireless user station and the network wireless access point as a function of the respective second keys derived by the wireless user station and the network wireless access point ;
 - providing access of the wireless user station to the telecommunication network through the network wireless access point as a function of the result of the authenticating step.
- 20

For example, the IEEE 802.11 standard defines two types of access methods to a network:

- access method based on Extensible Authentication protocol,
- access method based on Pre-Shared Keys (PSK).

25 Each access method includes an authentication and an establishment of pairwise group keys. These access methods differ by the authentication protocol.

30 The access method based on the Extensible Authentication protocol requires the exchange of information between three entities: the IEEE802.11 radio user station (the supplicant), the access point (the authenticator) and an authentication server. The authentication server is used to certify to the access point that the user station is allowed to associate and to certify to the user station that the selected access point is part of the network. This approach provides a mutual authentication. The authentication server is also use for key management.

The access method based on Pre-Shared Keys requires the exchange of information between two entities only: the IEEE802.11 radio user station (the supplicant) and the access point (the authenticator). The authentication phase is simplified and performed by the access point. The authentication and establishment of pairwise group key are merged and relies on the knowledge by both entities of a pre-shared key. The security of authentication and of communication relies on the confidentiality of the pre-shared key.

If the access method based on the Extensible Authentication protocol provides the highest level of security because of the mutual authentication of user station and access point and also the key management performed by the Authentication server, an access method based on Pre-Shared Key is much faster because it requires a limited exchange of information between only two entities, and is also simple to implement because it does not require an authentication server. The total duration of an access operation between the issue of an association request and the success of operation is above 1 second for the access method based on the Extensible Authentication protocol and a few milliseconds (ms) for the access method based on Pre-Shared Key.

There is a balance to be considered between the security level and the complexity and performance of a radio System, especially in cases wherein frequent handovers occur such as considering a user station inside a running train and communicating with a network including fixed access points.

The invention proposes a method for providing access to a telecommunication network of a wireless transceiving user station through a network wireless access point, a network wireless access point and a wireless user station according to the appended claims.

The invention enables thus to enhance the security level of access methods based on Pre-Shared Keys.

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

- Figure 1 shows diagrammatically a telecommunication network implementing an embodiment of the invention;

- Figure 2 is a flow chart illustrating steps of a method according to an embodiment of the invention;

- Figure 3 is a flow chart representing steps of a method according to an embodiment of the invention.

Figure 1 shows diagrammatically a telecommunication system 1 implementing an embodiment of the invention.

5 The telecommunication system 1 includes:

- a backbone network 3 from which telecommunication services can be provided, such as Internet services;
- one or several wireless user station(s) 6;
- several wireless access points 2 including the wireless access points 2 called AP₁, AP₂, AP₃, each connected to the backbone network 3.

10

A network manager server (NMS) 4 is also connected to the backbone network 3.

In the considered embodiment, a user station 6 is a radio user station 6, including a radio interface, a radiofrequency antenna, a microcomputer and a memory (not shown in the figures).

15

The memory of a user station 6 includes software instructions that once executed on the microcomputer of the user station 6, implement the steps described hereafter, including the steps referring to Figures 2 and 3 and performed by the user station 6.

20

In the considered embodiment, each of the access point AP₁, AP₂, AP₃ includes a radio interface, a radiofrequency antenna, a microcomputer and a memory (not shown in the Figures). Each of the access point AP₁, AP₂, AP₃ corresponds to a respective radio coverage area and is adapted to deliver the telecommunication services provided by the backstage network 3 to the radio user stations located inside the radio coverage area of said access point.

25

The memory of each of the access point AP₁, AP₂, AP₃ includes software instructions that once executed on the microcomputer of the access point, implement the steps described hereafter, including the steps referring to figures 2 and 3 and performed by the access point.

30

The radio interface of a user station 6 is adapted to communicate with the radio interface of the access point 2. In the considered embodiment of the invention, the respective radio interfaces are adapted to communicate according to IEEE 802.11 (amendment 802.11i) standard completed as disclosed hereafter regarding the generation of the Pairwise Transient Key (PTK) that is generated from the Pre-Shared Key (PSK) as

known, and also is generated according to the invention, in addition according to a regularly modified parameter.

In the specific embodiment considered in reference to figure 1, a radio user station 6, considered hereafter is for example a user station of a communication base train control radio system, and is inside a train 5. Whereas the train 5 goes along its railway line, the user station 6 successively goes through the radio coverage area of the access point AP_3 , then through the radio coverage area of the access point AP_2 and finally through the radio coverage area of the access point AP_1 . Several handoffs of the user station 6 with these successive access points 2 therefore occur.

The use of IEEE 802.11i provides for protection against intentional or unintentional interception by an authentication mechanism and encryption of all packets with payload data. The authentication mechanism avoids that an unauthorised user sets up a radio connection and the encryption of packets with payload data avoids that these ones be intercepted by any unauthorised user.

In accordance to IEEE 802.11i, the user stations 6 of the telecommunication system 1 and the access points 2 of the telecommunication system 1 have in memory a same stored pre-shared key PSK.

The pre-shared key PSK is used, as shown hereafter referring to figures 2 and 3, to generate a common pairwise transient key PTK in a user station 6 and in parallel in the access point implementing the authentication step, such PTK being used in authentication and used also in encryption/decryption of all packets including payload data.

A new PTK is generated in a user station 6 during an authentication step with an access point, after each handoff and after each power up and initialization stage of the user station 6.

According to the invention, referring to the set 100 of steps represented by the flow chart in Figure 2, in a step 101, a modified value of a parameter, called hereafter seed number, for example a random value, is generated by the NMS 4, and is transmitted to the access points 2 by the NMS 4 through the backbone network 3, for example in accordance with the Simple Network Management Protocol (SNMP).

The step 101 is repeated according to a determined seed number actualization pattern, for example a new value is randomly given to the seed number on a cyclic basis (one renewed seed number per week, per day, or per hour for example).

In a step 102, the last new value of the seed number is regularly transmitted by the radio interface of any access point 2.

In an embodiment of this step 102, each time a new value of the seed number is received from the NMS 4 by an access point 2, the access point 2 replaces, in a given field of its beacon message, the previously received seed number value by the newly received seed number value. As known, the beacon message further includes identification data of the access point 2 that are used by the user stations 6, in addition to the beacon reception level measurement when attempting to connect to the telecommunication system 1 through the access point in order to use telecommunication services provided by the telecommunication system. The beacon message of an access point 2 is transmitted repeatedly by the radio interface of the access point, for example every 30 ms.

The transmitted beacon messages are in the considered embodiment in compliance with the beacon messages of IEEE 802.11 standard, the seed number value being inserted in the field of the beacon message dedicated to proprietary information.

In addition, in an embodiment of this step 102, each time a new value of the seed number is received by an access point 2 from the NMS 4, the access point 2 replaces, in a given field of its probe response frames, the previously received seed number value by the newly received seed number value.

As known, the probe response frames of IEEE 802.11, including identification data of an access point, are transmitted by the radio interface of the access point 2 in response to any probe request sent by a user station 6 and received by the access point.

The transmitted probe response frames according the considered embodiment of the invention are in compliance with the IEEE 802.11 standard, the seed number value being inserted in the field dedicated to proprietary information.

In a step 103, the new value of the seed number transmitted by an access point 2 in step 102 is received by the radio interface of a user station 6 located inside the radio coverage area of the access point 2 and is stored in its memory. The user station 6 generates a PTK key as a function of the PSK key stored in the user station memory and of this lastly stored value of the seed number.

Said PTK key is generated each time the on-board user station 6 performs a handoff or is powered up, during an authentication step between the user station and the access point, and is also used for subsequent encryption/decryption.

The invention enables to increase the security of the telecommunication system 1 with a very limited impact on the telecommunication system performances (for example on handoff duration) and complexity.

Such advantages are valuable for example in trains running at speed up to 100 km/h, wherein on-board user stations perform frequent handovers between access points and handover duration shall be as short as possible with a value lower than 100 ms in 90 percent of the handovers.

In an embodiment of step 103, each time the on-board user station 6 performs an handoff or is powered up, the user station 6 searches for a new suitable access point 2 by listening beacons transmitted by surrounding access points 2, according to IEEE 802.11. To speed up suitable access point research, optionally the user station 6 sends a probe request, according to IEEE 802.11.

Then the user station 6 analyses listened beacons and/or probe response frames, selects a suitable access point 2 according to IEEE 802.11, for example the access point AP_3 (as known, the access point AP_3 is selected based upon at least the reception level, by the user station 6, of the radio signal transmitted by the access point AP_3). The user station 6 stores, in its memory, information contained inside the beacon and/or probe response transmitted by the selected access point AP_3 including security parameters such as the type of authentication according to IEEE 802.11 and the new seed number. Then the user station 6 transmits, via its radio interface, to the selected access point AP_3 , an association request according to IEEE 802.11 requiring association with the selected access point AP_3 . Once the association step exchanges between the user station 6 are successfully completed and the selected access point AP_3 is associated with the user station 6, the authentication step then starts. No telecommunication of payload data is possible until the completion of the authentication step between the access point AP_3 and the user station 6.

Figure 3 represents a flow chart representing steps of the authenticating stage 200 between a user station 6 and the associated access point the selected access point AP_3 , such as performed in an embodiment of step 103.

In step 201, the user station 6 generates an operational shared key OPSK, as a result of a function (function F1) of the pre-shared key PSK stored in its memory and of the new seed number that was lastly stored in its memory: $OPSK = F1(PSK, \text{seed number})$.

In an embodiment, the function F1 is based on PBKDF2 function defined in the IETF RFC2898.

In step 202, the user station 6 generates a SNonce value, that can be a random number generated on the basis of PBKDF2 defined in the RFC2898 with the main inputs being OPSK and a random number or a Random generated directly generated according to IETF RFC 4086.

In parallel to steps 201 and 202, in step 301, the access point AP3 generates also an operational shared key OPSK, as a result of a function (function F1) of the pre-shared key PSK stored in its memory and of the seed number that was lastly stored in its memory (OPSK = F1(PSK, seed number) and in step 302, the access point AP3 generates a ANonce. that can be a Random number generated on the basis of PBKDF2 defined in the RFC2898 with the main inputs being OPSK and a random number or a Random generated according to IETF RFC 4086

In a step 303, the access point AP₃ transmits to the user station 6, through the respective radio interfaces, a first authentication message including the generated ANonce value.

In a step 304, the user station 6 receives the first authentication message transmitted by the access point AP3 and derives a pairwise transient key PTK from the ANonce value included in the received first authentication message and from the SNonce and the operational shared key OPSK generated in step 201: PTK = F3(ANonce, SNonce, OPSK), wherein F3 is a function of the ANonce value and of the OPSK value and also the SNonce value.

In an embodiment, the function F3 is the PRF-n function defined by the IEEE802.11 standard.

In a step 305, the user station 6 transmits to the access point AP₃, through the respective radio interfaces, a second authentication message including the generated SNonce value and a Message Integrity Code (MIC) based on CBTC-MAC as defined in the four ways handshake mechanism specified by the IEEE802.11 standard. In a step 306, the access point AP₃ receives the second authentication message transmitted by the user station 6. The access point AP₃ checks that the MIC in the received second authentication message is valid (for example, it is considered as valid if and only if the MIC calculated on its own by the access point is equal to the MIC which is in the received second authentication message and was calculated by the user station based on SNonce and the header in the message), and only in case the MIC is checked as valid

(else the authentication fails), the access point AP₃ derives a pairwise transient key PTK from the SNONCE value included in the received second authentication message and from the operational shared key OPSK generated in step 201 and also the ANONCE: $PTK = F4(ANONCE, SNONCE, OPSK)$, wherein F4 is a function of the ANONCE value, SNONCE value and of the OPSK value. The F4 function is the F3 Function that is the PRF-n function defined by the IEEE802.11 standard.

In a step 307, the access point AP₃ transmits to the user station 6, through the respective radio interfaces, a third authentication message including a notification of installing PTK certified with a MIC calculated from the header of the third authentication message and from ANONCE.

In a step 308, the user station 6 receives the third authentication message transmitted by the access point AP₃ as defined in the IEEE802.11 four way handshake mechanism. The user station 6 checks if the MIC in the received third authentication message is valid (similarly to step 306, the user station computes the MIC on the content of the third authentication message and compare with the MIC inside the message ; if and only if they are the same, the message is considered as valid), and only in case the MIC is checked as valid (else the authentication fails), the user station 6 transmits a forth authentication message to the access point AP₃ including a MIC calculated from the header of the forth authentication message and from SNONCE.

Then in a step 309, the user station 6 installs in its memory the key PTK generated in step 304.

In a step 310, the access point AP₃ receives the forth authentication message transmitted by the user station 6 and then the access point AP₃ installs in its memory the key PTK generated in step 306.

The authentication is then completed and the communication of payload data can then occurs (step 311), these payload data being encrypted/decrypted by the user station 6 using encryption/decryption key(s) based upon the PTK key stored in its memory (and similarly the payload data being encrypted/decrypted by the access point AP₃ using the PTK key stored in its memory).

In standard prior art IEEE 802.11, considering Figure 3, the steps 201 and 301 did not exist and in the steps 202, 302-311, the pre-shared key PSK was used instead of the key OPSK, to generate the pairwise transient key PTK. The invention enables to transform a static key (the PSK key) into a dynamic one (the OPSK key).

Hereabove the steps 202, 302, 303, 304, 305, 306, 307, 308, 309, 310 are the steps defined in IEEE 802.11 for authentication stage when considering the dynamic OPSK instead of the static PSK.

5 The invention enables to increase the level of security without significantly increasing the complexity of the system architecture or the handover duration.

10 An embodiment of the invention has been here above described referring to the figures in the case of IEEE 802.11 radio communications between the user stations and the network access points. Of course, the use of a static key shared by the access points and the user stations and of a random number regularly modified according to the invention in authenticating step and/or encryption/decryption step can be implemented using radio protocols for communicating that are different from IEEE 802.11, and more generally in embodiments of the invention, other wireless interfaces for communicating can be used instead of radio interfaces.

CLAIMS

1.- Method for providing access to a telecommunication network (3) of a wireless user station (6) through a network wireless access point (2), characterized in that it including
5 successively the steps of:

- obtaining by the network access point an updated value of a parameter;
- wirelessly transmitting by the network wireless access point the updated value of the parameter;
- wirelessly receiving by the wireless user station the updated value of the
10 parameter transmitted by the network wireless access point;
- deriving, by each of the wireless user station and the wireless network access point, a second key from at least a first key and further from the received updated value of the parameter, the first key being a static pre-shared key, shared by the wireless user station and the network access point and stored in the memory of
15 the wireless user station and the network access point, respectively;
- performing, through wireless communication, an authenticating step between the wireless user station and the network wireless access point based on the second keys derived by the wireless user station and the network wireless access point;
- providing access of the wireless user station to the telecommunication network
20 through the network wireless access point as a result of the authenticating step.

2.- Method according to claim 1, wherein, at each updating time of an updating pattern including several updating times, the network wireless access point obtains an updated value of the parameter and transmits wirelessly the updated value of the parameter thus
25 obtained; and wherein any future authentication step relative to the wireless user station having received the updated value of the parameter is performed as a function of the second key derived by the wireless user station from at least the first key and further from the transmitted updated value of the parameter.

30 3.- Method according to claim 1 or 2, wherein a server provides several access points, through the telecommunication network (3), with said updated value of the parameter and any of these several access points wirelessly transmits the updated value of the parameter.

4.- Method according to any one of claims 1 to 4, wherein the authenticating step between wireless user station and the network wireless access point is performed in accordance to the IEEE 802.11 standard.

5 5.- Method according to claim 4, wherein the authenticating step is a four-way handshake mechanism.

6.- Method according to any one of claims 1 to 6, wherein the updated value of the parameter is wirelessly transmitted by the wireless access point as included in the beacon
10 messages of the wireless access point further including wireless access point identification information and cyclically broadcasted.

7.- Network wireless access point (2), configured to provide a wireless user station (2) with access to a telecommunication network, said network wireless access point being
15 characterized in being adapted:

- for obtaining an updated value of a parameter,
- for wirelessly transmitting by the network wireless access point the updated value of the parameter,
- for deriving a second key from at least a first key, and further from the transmitted
20 updated value of the parameter, the first key being a static pre-shared key, shared by the wireless user station and the network access point and stored in the memory of the wireless user station and the network access point, respectively;
- for performing, through wireless communication, an authenticating step with the wireless user station as a function of the derived second key, and
- 25 - for providing access of the wireless user station to the telecommunication network as a function of the result of the authenticating step.

8.- Network wireless access point (2) according to claim 7, adapted for, at each
30 updating time of an updating pattern including several updating times, obtaining an updated value of the parameter and transmitting wirelessly the updated value of the parameter thus obtained.

9.- Network wireless access point (2) according to claim 7 or 8, adapted for
35 performing the authenticating step with the wireless user station in accordance to the IEEE 802.11 standard.

10.- Network wireless access point (2) according to claim 9, adapted so that the authenticating step is a four-way handshake mechanism.

11.- Network wireless access point (2) according to any one of claim 7 to 10, adapted for wirelessly transmitting the updated value of the parameter as included in the beacon messages of the wireless access point further including wireless access point identification information and cyclically broadcasted.

12.- Wireless user station (6) configured to get access to a telecommunication network through a network wireless access point (2), said wireless user station being adapted for deriving a second key (OPSK) from at least a first key (PSK), for performing, through wireless communication, an authenticating step with the network wireless access point as a function of the derived second key (OPSK), and for accessing to the telecommunication network through the network wireless access point as a function of the result of the authenticating step;
said wireless user station being characterized in that it is adapted for wirelessly receiving an updated value of a parameter transmitted by the network wireless access point and for deriving the second key (OPSK) from at least the first shared key and further from the received updated value of the parameter.

13.- Wireless user station (6) according to claim 12, adapted for performing any future authentication step as a function of the second key (OPSK) derived by the wireless user station from at least the first key and further from the updated value of the parameter received at the last occurred updating time of an updating pattern including several updating times,

14.- Wireless user station (6) according to claim 12 or 13, adapted for performing the authenticating step with the network wireless access point in accordance to the IEEE 802.11 standard.

15.- Wireless user station (6) according to any one of claims 12 to 14, adapted for receiving the updated value of the parameter as included in the beacon messages cyclically broadcasted by the wireless access point and further including wireless access point identification information.