(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2012 (03.05.2012)

PCT

(10) International Publication Number
WO 2012/055087 A1

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/CN2010/078085

(22) International Filing Date:
25 October 2010 (25.10.2010)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants *(for all designated States except US)*: **ZTE CORPORATION** [CN/CN]; ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan, Shenzhen, Guangdong 518057 (CN). **ZTE U.S.A., INC.** [US/US]; 10105 Pacific Heights Blvd., Suite 250, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LUO, Wen** [CN/CN]; No.68 Zijinhua RD, Yuhuatai District, Nanjing, Jiangsu 210000 (CN). **TU, Yangwei** [CN/CN]; No.68 Zijinhua RD, Yuhuatai District, Nanjing, Jiangsu 210000 (CN). **SO, Tricci** [US/US]; 6096 Blue Dawn Trail, San Diego, California 92130 (US).

(74) Agent: **AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE**; Suite B 1601A, 8 Xue Qing Rd., Haidian, Beijing 100192 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

WO 2012/055087 A1

(54) **Title**: METHOD FOR WIMAX VOICE SERVICES (WVS) REGISTRATION WITH HTTP-DIGEST

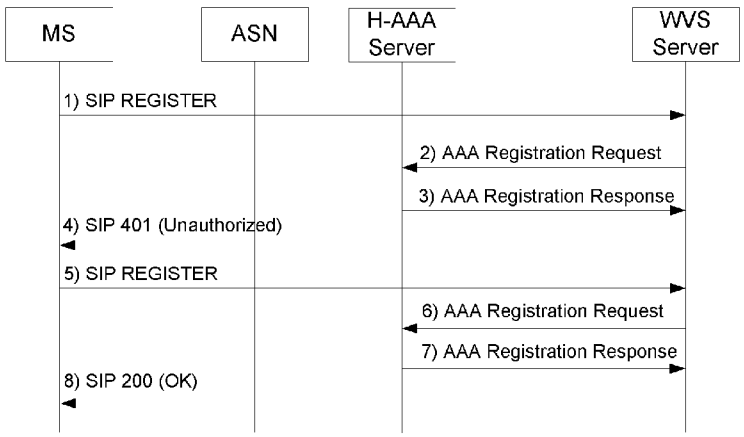

FIG. 2

(57) **Abstract**: A method for supporting a mobile station to perform SIP registration and re-registration with Wi MAX Voice Services (WVS) Server using HTTP-Digest is provided, and the specific high-level technical details including the step-by-step procedures to explain how the existing HTTP-Digest method can be integrated into the WVS feature are described.

METHOD FOR WIMAX VOICE SERVICES (WVS) REGISTRATION WITH HTTP-DIGEST

Technical Field

This invention relates to the WiMAX technology, and in particular, relates to a method for supporting a mobile station to perform SIP registration and re-registration with WiMAX Voice Services (WVS) Server using HTTP-Digest.

Background of the Invention

WiMAX is 4th generation broadband wireless technology that enables the next generation of high capacity mobile multi-media services. WiMAX Forum is currently developing the generic WiMAX Voice Service features to support SIP-based VoIP services over the WiMAX infrastructure to support WiMAX generic VoIP services and to interwork with legacy voice (i.e. PSTN) and other existing VoIP infrastructure services. The WiMAX Voice Services (WVS) architecture is shown in Figure 1.

The HTTP-Digest (RFC 2617) is already chosen by WiMAX Forum to be the method for the SIP registration and re-registration to provide some authentication service. However, the exact technical details on how to incorporate the HTTP-Digest into the WVS have not been proposed nor have been disclosed.

Summary of the Invention

The intent of this invention is to provide a method for supporting a mobile station to perform SIP registration and re-registration with WiMAX Voice Services (WVS) Server using HTTP-Digest. Accordingly, this invention provides the specific high-level technical details including the step-by-step procedures to explain how the existing HTTP-Digest method can be integrated into the WVS feature.

This invention provides a method for WiMAX Voice Services (WVS) Registration with HTTP-Digest, comprising steps of:

a terminal sending a register request for registration to a WVS server;

a Home Authentication Authorization Accounting (H-AAA) server transmitting security context information to the WVS server in response to a request from the WVS server; and

the WVS server authenticating the terminal by the HTTP-Digest approach and completing the initial registration of the terminal.

Preferably, the security context information includes a user password for using the WVS.

Preferably, the WVS server authenticates the terminal by using an algorithm of the HTTP-Digest that is negotiated between the WVS server and the terminal.

Preferably, the method further comprises:

the H-AAA server also sending realm information to the WVS server in the case when the WVS server is not aware of the realm information.

Preferably, the realm information is configured by an operator in the H-AAA.

Preferably, the method further comprises:

the H-AAA using an algorithm of the HTTP-Digest to process the security context information before transmitting the security context information to the WVS server.

Preferably, the algorithm of the HTTP-Digest is an MD5 algorithm.

Preferably, the method further comprises:

the H-AAA indicating to the WVS server the algorithm of the HTTP-Digest used.

Preferably, the method further comprises:

the WVS server storing the security context information transmitted by the H-AAA server.

Preferably, the method further comprises:

the terminal sending a register request for re-registration to the WVS server prior to the expiry of a registration timer set in the initial registration; and

the WVS server authenticates the terminal again by the HTTP-Digest approach.

Preferably, the method further comprises:

updating the security context information in the WVS server when a user password for using the WVS is changed.

Preferably, when the user password is changed, the terminal and the H-AAA are informed of a new user password.

Preferably, the updating process includes:

the terminal initiating an initial registration procedure to the WVS server; and

the H-AAA server providing the WVS server with new security context information.

Preferably, the updating process includes:

the H-AAA server transmitting new security context information to the WVS server via a security context update message; and

the WVS server storing the new security context information and replying to the H-AAA server with a security context update acknowledgement message.

Preferably, the updating process includes:

the H-AAA server triggering a WVS de-registration procedure to de-register the registered terminal if the terminal is currently not in an active WVS session; and

the terminal initiating an initial registration procedure to the WVS server using new security context information.

With the above technical schemes provided in this invention, the HTTP-Digest can be successfully incorporated into the WVS.

Brief Description of the Drawings

Figure 1 illustrates the WVS architecture;

Figure 2 illustrates the flow of WVS initial registration;

Figure 3 illustrates the flow of WVS Re-registration; and

Figure 4 illustrates a method for security context update.

Preferred Embodiments of the Invention

The design of this invention is to explain:

a. H-AAA provides security context to WVS Server for supporting WVS Server to perform authentication and authorization of WVS subscriber.

b. The security context includes the password for subscriber using WVS

c. For the purpose of the password security, H-AAA runs a checksum algorithm to generate a checksum of the combination of the password and other related parameters according to RFC2617. Then H-AAA provides WVS Server with the checksum.

d. The WVS Server uses the checksum to validate the subscriber.

Preferred embodiments of this invention are described in detail below in conjunction with the drawings.

1. WVS Managed Procedure

As described in the background, the HTTP-Digest method is used during the SIP registration and re-registration to provide authentication and authorization.

This section describes the WVS registration authentication and authorization that is performed by the WVS Server. The subscriber's subscription information for WVS, such as user-name and user-password is expected to be available for both the MS itself and H-AAA Server.

1.1 WVS Initial Registration

The flow of WVS initial registration is shown in figure 2, which includes steps of:

1) After obtaining the IP connectivity and getting the IP address of the WVS Server, the MS performs the WVS Initial Registration procedure by sending a SIP REGISTER request without

Authorization Header to the WVS Server. The SIP Expire time (non-zero value in seconds) in the message-header is included in this SIP message.

2) When receiving the SIP REGISTER request, the WVS Server will know this is an initial registration by detecting that the Authorization Header is missing. Then the WVS server will contact MS's H-AAA.

The OUI (i.e. Outer User Identity) and/or the IUI (i.e. Inner User Identity) contained in the SIP REGISTER message provides the domain information of which operator this subscriber belongs. Based on this domain information, the WVS Server can find an appropriate H-AAA server, and send an AAA Registration Request to this H-AAA Server.

This message can carry an indication which indicates this is an initial authentication request of a WVS session.

This message also can carry realm information, e.g. wvs-operator-name@operaor-domain-name.com, and the WVS server is one of the servers in this realm.

3) When receiving the AAA Registration Request with initial authentication request of a WVS session, the H-AAA Server will verify the subscription of the registered user.

If the subscription exists, there are at least two possible implementations to authenticate/validate the user which are described as the following:

Implementation A:

H-AAA Server will retrieve related security context (e.g. user password for this subscriber using WVS) for this subscriber. H-AAA Server sends this security context to WVS Server via the AAA Registration Response message. In this scenario, the H-AAA and the WVS server may have been established their security association (SA) and there may be privacy protection enabled for this interface.

Note that the user-name could be the OUI and/or the IUI mentioned above.

In the case when the WVS server is not aware of the realm information as described above, the H-AAA shall be aware of this information (e.g. via the configuration by the operator in H-AAA)

and the H-AAA is required to provide the realm information to WVS server via the AAA Registration Response message.

Implementation B:

Based on the configuration, H-AAA will apply the HTTP-Digest as the protocol to be used for the WVS registration authentication and the authorization.

If the communication between the H-AAA and the WVS server was not protected, the password which is part of the security context and is transferred in clear text could be intercepted by an intruder easily. Another possibility is that, the operator may prefer the WVS Server not to have the access of the user password information, hence, the H-AAA will not provide WVS server with the security context as mentioned in implementation A above.

Instead, the H-AAA will use an algorithm as defined in HTTP-Digest (i.e. RF2617) to process the security context first before transmitting it to the WVS server via the AAA Registration Response message. For example, the H-AAA runs MD5 algorithm (which is chosen as default algorithm in RFC2617) with input parameters user-name, realm and password. The output of this algorithm can be described as following:

Output(WVS) = MD5(unq(user-name) ":" unq(realm) ":" password)

Note: Notation unq(X) means the value of the quoted-string X without the surrounding quotes (refer to RFC 2617).

Based on this method, the security context will not be exposed to the possible intruder over the unprotected communication between the H-AAA and WVS server, and also allows the home operator to control the awareness of the WVS user's password information in the WVS server.

Note that some other algorithms which are chosen by RFC2617 can also be used instead of this MD5 algorithm.

Same consideration as for the Implementation A above, if the WVS server can not provide the realm information, the H-AAA is required to be aware of this information (e.g. configured by the

operator in H-AAA). And the H-AAA should provide this realm information to WVS server via the AAA Registration Response message

4) The WVS Server sends a SIP 401 (Unauthorized) with a WWW-Authenticate Header as defined in HTTP-Digest to MS to indicate the authentication and authorization information should be provided by the MS.

In this step, a nonce value which is uniquely generated each time a 401 response is made by the WVS Server shall be included in this WWW-Authenticate Header, and be sent to the MS.

The WVS Server can also provide some other security information. This security information is included in this SIP request message for the WVS subscriber to authenticate the WVS Server.

5) As to the response for the SIP 401 (Unauthorized), the MS sends a SIP REGISTER request with Authorization Header to the WVS Server.

Note that, the MS can also authenticate the WVS Server first, and if successfully, it will send the SIP REGISTER request mentioned above to the WVS Server.

In this step, an important parameter called "response" is generated by MS and is included in the Authorization Header, and sent to the WVS Server.

MS uses a previously negotiated algorithm between itself and the WVS Server to calculate this "response". In the case when MD5 is used, the MS calculates the "Output(MS) " first as shown below:

Output(MS) = MD5(unq(user-name) ":" unq(realm) ":" password)

MS knows the user-name and the password, and the realm information is provided by WVS Server in WWW-Authenticate Header as described in step 4 above.

By combining Output(MS) value with the nonce value (provided by WVS Server) and with other required parameters, the MS uses MD5 again to generate this "response" parameter.

The "response" together with other related parameters shall be included in the Authorization Header and be sent to the WVS Server with the SIP REGISTER request. These parameters together with this "response" parameter are called as "related security information" here.

As a result, the "related security information" together with SIP Expire time (the same value as carried in the SIP REGISTER request in step 1) are included in this SIP request message for the WVS Server to authenticate the WVS subscriber.

6) When receiving the SIP REGISTER request with Authorization Header, the WVS Server authenticates the WVS subscriber by itself.

In case the implementation A is adopted, WVS Server shall first calculate the "Output(WVS)" by itself using a negotiated algorithm between itself and the MS. In the case when the negotiated algorithm is MD5, the WVS Server calculates the "Output(WVS)" as following:

Output(WVS) = MD5(unq(user-name) ":" unq(realm) ":" password)

For this implementation, the parameters needed (e.g. the parameter password) has already been provided by the H-AAA in step3.

Then combining this Output(WVS) value with the nonce value (generated by WVS Server itself) and some other related parameters, WVS Server uses MD5 again to generate a so called parameter "validation".

In case the implementation B is adopted, WVS Server combines the Output(WVS) value which is provided by the H-AAA in step3 with the nonce value (generated by WVS Server itself) and some other related parameters, then uses MD5 to generate a so called parameter "validation" directly.

For this implementation, in the beginning, H-AAA chooses an algorithm to generate the "Output(WVS)" (refer to step 3). So, the H-AAA should indicate to the WVS Server which algorithm is used.

Note that, in the case when the WVS Server and the H-AAA Server are belonged to a same operator (i.e. Network Service Provider), because the MD5 algorithm is chosen as the default by HTTP-Digest (RFC2617), MD5 algorithm can be set as the default if decided by the operator. If H-AAA doesn't indicate to the WVS Server for which the security algorithm is applied, the WVS Server should assume the MD5 to be applied.

For both implementation A & B, if the value of the parameter "validation" equals to the value of the parameter "response" which is provided by MS in Authorization Header, then the authentication is successful.

If the authentication is successful, the WVS Server will then forward the AAA Registration Request to the H-AAA Server. The successful authentication indication and the SIP Expire time retrieved from the SIP REGISTER request shall be included in this message.

7) When receiving the AAA Registration Request with successful authentication indication, the H-AAA Server will retrieve the SIP Expire time and set the registration timer for this subscriber on this WVS Server. H-AAA may shorten the registration timer e.g. based on the operator's policy, and in this case the H-AAA shall send this new registration time to the WVS Server with an AAA Registration Response message.

8) When receiving the AAA Registration Response with a registration timer set by the H-AAA, the WVS Server will update the timer for this WVS registration according to this registration timer and reply to the MS with a SIP 200 (OK) response. The SIP Expire time in its message-header is set according to the registration timer received from the H-AAA.

1.1.1 Message Construction for Implementation A

The message between the WVS Server and the H-AAA Server could be RADIUS Based or Diameter Based or SOAP Based etc. In this context, the RADIUS based messages are present. The principle will be the same if using Diameter or SOAP to construct the message.

Table 1.1.1-1 Message mapping

Message used in this disclosure	Corresponding RADIUS
AAA Registration Request	Access-Request
AAA Registration Response	Access-Accept

Table 1.1.1-2 Message construction method 1

Attribute	**Description**	**Access Request**	**Access Accept**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber.	0-1	0-1

	If WVS Server can parse the INI, then this parameter could be present in Access Request. If WVS Server can not parse the INI, then this parameter shall be present in Access Accept.		
WVS-User-Password	The password of the subscriber for using WVS	0	1
WVS-Expire-time	The Expire time. If the H-AAA shortens the expire time provided by the WVS Server, then this parameter shall be present in Access Accept.	1	0-1
WVS-Authentication-State-Indication	In step 2, this parameter shall be set to a value which can indicate the state is "initial authentication". In step 6, this parameter shall be set to a value which can indicate the state is "authentication successful" if the authentication is successfully performed by the WVS server.	1	0
WVS- realm-name	The information of the realm to which the WVS server belongs. If the WVS Server knows the realm information, then this parameter should be present in Access Request. If the WVS Server doesn't know, then the H-AAA shall know the realm information, and the parameter shall present in Access Accept.	0-1	0-1

Table 1.1.1-3 Message construction method 2

Attribute	**Description**	**Access Request**	**Access Accept**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber. If WVS Server can parse the INI, then this parameter could be present in Access Request.	0-1	0-1
WVS-Security-Context	This parameter contains user-name, user-password and realm information explicitly (i.e. in clear text), which are useful for WVS authentication. The format is as following: unq(user-name) ":" unq(realm) ":" password	0	1
WVS-Expire-time	The Expire time	1	0-1
WVS-Authentication-State-Indication	In step 2, this parameter shall be set to a value which can indicate the state is "initial authentication". In step 6, this parameter shall be set to a value which can indicate the state is "authentication successful" if the authentication is successfully performed by the WVS server.	1	0
WVS- realm-name	The information of the realm to which the WVS server belongs.	0-1	0-1

	If H-AAA doesn't have the realm information, the WVS Server shall provide this information.		

Using either of these two message construction methods, WVS Server can get enough information for executing HTTP-Digest based authentication algorithm.

1.1.2 Message Construction for Implementation B

The message between the WVS Server and the H-AAA Server could be RADIUS Based or Diameter Based or SOAP Based etc. Here, we discuss the RADIUS based message construction. The principle will be the same if using Diameter or SOAP to construct the message.

Table 1.1.2-1 Message mapping

Message used in this disclosure	Corresponding RADIUS
AAA Registration Request	Access-Request
AAA Registration Response	Access-Accept

Table 1.1.2-2 Message construction method

Attribute	**Description**	**Access Request**	**Access Accept**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber. If WVS Server can parse the INI, then this parameter could be present in Access Request. If WVS Server can not parse the INI, then this parameter shall be present in Access Accept.	0-1	0-1
WVS-Security-Context	This parameter contains user-name, user-password and realm information implicitly which are useful for WVS authentication. The format is as following: H(unq(user-name) ":" unq(realm) ":" password) Note: Notation H(Y) means to apply a checksum algorithm to the parameter Y.	0	1
WVS-Expire-time	The Expire time. If the H-AAA shortens the expire time provided by the WVS Server, then this parameter shall be present in Access Accept.	1	0-1
WVS-Authentication-State-Indication	In step 2, this parameter shall be set to a value which can indicate the state is "initial authentication". In step 6, this parameter shall be set to a value which can indicate the state is "authentication successful" if	1	0

	the authentication is successfully performed by the WVS server.		
WVS- realm-name	The information of the realm to which the WVS server belongs. If the WVS Server knows the realm information, then this parameter should be present in Access Request. If the WVS Server doesn't know, then the H-AAA shall know the realm information, and the parameter shall present in Access Accept.	0-1	0-1
WVS-Checksum-Algorithm	To indicate the checksum algorithm used for generate parameter WVS-Security-Context. The WVS Server may use this parameter to indicate H-AAA the checksum algorithms it supports. If this parameter is missing in Access Accept, then it indicates the MD5 algorithm is used by H-AAA.	0-1	0-1

Using this message construction method, WVS Server can get enough information for executing HTTP-Digest based authentication algorithm. Meanwhile, the password is not exposed to the WVS Server.

Additionally, for the purpose of distinguishing the parameter "WVS-Security-Context" is a clear text or a checksum value, an indication can be introduced into the Access Accept in implantation A & B .

1.2 WVS Re-registration

The flow of WVS Re-registration is shown in figure 3, which includes steps of:

1) For periodic registration, the MS initiates a re-registration prior to expiry of the registration timer that was set previously. To re-register, the MS sends a new SIP REGISTER request including a new SIP Expire time to the WVS Server.

During WVS initial registration phase, when the authentication of the MS is successful, WVS Server will respond to MS with a SIP 200 (OK) message containing an Authentication-Info Header (step 8, figure 2). A parameter called "next-nonce" could be generated by the WVS Server and be contained in this Authentication-Info Header and be sent to the MS.

If the MS got this "next-nonce" parameter, then in this step, the MS will re-calculate the "response" mentioned in step 5 above. And the step 5 in figure 2 shall be modified to be based on

this "next-nonce" parameter instead of the "nonce" parameter in the context of WVS re-registration. MS will put this re-calculated "response" together with other parameters in the Authorization Header and sent this header to the WVS Server with the SIP REGISTER request.

2) When receiving the SIP REGISTER request for re-registration, the WVS Server will verify the security information included in the Authorization Header.

The security information validation method used here is similar to the method used in step 6 of figure 2. The only difference is that the WVS Server should use the "next-nonce" to calculate the "validation" value.

If the security information is valid (i.e. the value of the "validation" equals to the value of the "response"), the WVS Server will send AAA Re-registration Request including the SIP Expire time to the H-AAA Server.

3) When receiving the AAA Re-registration Request, the H-AAA Server will retrieve the SIP Expire time and set the registration timer for this subscriber on this WVS Server. H-AAA may shorten the registration timer e.g. based on the operator's policy, and in this case the H-AAA shall send this new timer to the WVS Server in the AAA Re-registration Response message.

4) When receiving AAA Re-registration Response with a registration timer set by the H-AAA, the WVS Server will update the timer for this WVS registration according to this registration timer and reply to the MS with a SIP 200 (OK) response. The SIP Expire time in its message-header is set according to the registration timer received from the H-AAA.

In this step, WVS Server could generate another "next-nonce" parameter and send this "next-nonce" parameter to the MS with the SIP 200 (OK) response. This newly generated "next-nonce" could be used by the MS to perform WVS re-registration next time.

1.3 WVS Password Changed

After MS performs WVS Registration successfully, the MS may initiate the WVS session, e.g. make a phone call, etc.

According to the WVS Initial Registration method as described in section 1.1, in the initial WVS registration procedure, the WVS Server is provided with security context of the MS, and the WVS Server will hold this security context locally for the future use (e.g. WVS re-registration).

Note that, the security context described here could be the subscriber's password for the WVS (Implementation A), and could also be the "Output(WVS)" as described in step 3 of figure 2 (Implementation B).

If the subscriber's password for using WVS is changed, then the security context hold by the WVS Server will become invalid. There should be some solution to deal with this scenario.

Note that, when the password is changed, both MS and H-AAA will be informed with the new password (e.g. via management plane).

First possible solution is to depend on the behavior of the MS. More specifically, when the password is changed, the MS will initiate a WVS Initial Registration procedure even if this MS has already registered with the WVS Server.

In this case, when receiving the SIP REGISTER message without an Authentication Header, WVS Server will approach this SIP REGISTER message using the method described in section 1.1. In this way, the WVS Server will be provided with the new security context.

Second possible solution is to depend on the behavior of the network as following, which is shown in figure 4.

1) When the password is changed, H-AAA will be informed. The H-AAA should update the security context hold by the WVS if the MS has already performed the WVS initial registration.

As described in step 3 of figure 2, H-AAA could use either Implementation A method or Implementation B method to transfer the MS's security context to the WVS Server with AAA Security Context Update message.

2) WVS Server stores the new security context of the MS for the future use, and responds to the H-AAA with an AAA Security Context Update Ack message.

For example, when the MS performs re-registration next time, the MS will use the new security context to generate the Authentication Header as described in step 1 of figure 3, and the WVS Server will also use this new security context to authenticate/validate the MS.

Third possible solution which is depended on the behavior of both MS and network is as following.

1) When the password is changed, H-AAA will be informed. H-AAA trigger to perform AAA Server Initiated WVS De-registration procedure to de-register current registered MS if there is no active WVS call session.

2) After some time or immediately, MS triggers to perform a WVS initial registration procedure as described in section 1.1 using the new security context.

1.3.1 Message Construction for second solution Implementation A

The message between the WVS Server and the H-AAA Server could be RADIUS Based or Diameter Based or SOAP Based etc. Here, we discuss the RADIUS based message construction. The principle will be the same if using Diameter or SOAP to construct the message.

Table 1.3.1-1 Message mapping

Message used in this disclosure	Corresponding RADIUS
AAA Security Context Update	CoA
AAA Security Context Update Ack	CoA Ack

Table 1.3.1-2 Message construction method 1

Attribute	**Description**	**CoA**	**CoA Ack**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber	0-1	0
WVS-User-Password	The password of the subscriber for using WVS	1	0
WVS- realm-name	The information of the realm to which the WVS server belongs.	0-1	0

Table 1.3.1-3 Message construction method 2

Attribute	**Description**	**CoA**	**CoA Ack**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber	0-1	0

WVS-Security-Context	This parameter contains user-name, user-password and realm information explicitly (i.e. in clear text), which are useful for WVS authentication. The format is as following: unq(user-name) ":" unq(realm) ":" password	1	0
WVS- realm-name	The information of the realm to which the WVS server belongs.	0-1	0

1.3.2 Message Construction for second solution Implementation B

The message between the WVS Server and the H-AAA Server could be RADIUS Based or Diameter Based or SOAP Based etc. Here, we discuss the RADIUS based message construction. The principle will be the same if using Diameter or SOAP to construct the message.

Table 1.3.2-1 Message mapping

Message used in this disclosure	Corresponding RADIUS
AAA Security Context Update	CoA
AAA Security Context Update Ack	CoA Ack

Table 1.3.2-2 Message construction method

Attribute	**Description**	**CoA**	**CoA Ack**
WVS-Outer-User-Identity	The OUI of the WVS subscriber	1	0-1
WVS-Inner-User-Identity	The INI of the WVS subscriber	0-1	0
WVS- realm-name	The information of the realm to which the WVS server belongs.	0-1	0
WVS-Security-Context	This parameter contains user-name, user-password and realm information implicitly which are useful for WVS authentication. The format is as following: H(unq(user-name) ":" unq(realm) ":" password)	1	0
WVS-Checksum-Algorithm	To indicate the checksum algorithm used for generate parameter WVS-Security-Context. The WVS Server may use this parameter to indicate H-AAA the checksum algorithms it supports. If this parameter is missing in Access Accept, then it indicates the MD5 algorithm is used by H-AAA.	0-1	0

Additionally, for the purpose of distinguishing the parameter "WVS-Security-Context" as a clear text or a checksum value, an indication can be introduced into the CoA for both implementation A & B.

Note: for all the tables above, "0" stands for the corresponding parameter in the same line shall not be present in the corresponding message; "1" stands for shall present and "0-1" stands for may or may not present.

2. H-AAA Managed Procedure

As described in the background, the HTTP-Digest method is used during the SIP registration and re-registration to provide authentication and authorization.

This section assumes that the authentication and authorization is performed by the H-AAA Server. The subscriber's subscription information for WVS, such as user-name and user-password is available to both MS itself and H-AAA Server.

In this scenario, the WVS server will act as a proxy defined in the HTTP-Digest. Between the H-AAA and WVS Server, all necessary parameters needed for running HTTP-Digest will be interacted via AAA interface.

All other approaches will obey the HTTP-Digest (i.e. RFC2617).

Other variations and enhancements are possible based on the preferred embodiments described above. It shall be understood that the above detailed description of the preferred embodiments of the present invention is not limitation to the protection scope of the present invention, which is defined by the claims.

Industrial Applicability

This invention provides a method for supporting a mobile station to perform SIP registration and re-registration with WiMAX Voice Services (WVS) Server using HTTP-Digest, and describes the specific high-level technical details including the step-by-step procedures to explain how the

existing HTTP-Digest method can be integrated into the WVS feature. This invention is applicable to a WiMAX system supporting the WiMAX Voice Service features.

Claims

1. A method for WiMAX Voice Services (WVS) Registration with HTTP-Digest, comprising steps of:

a terminal sending a register request for registration to a WVS server;

a Home Authentication Authorization Accounting (H-AAA) server transmitting security context information to the WVS server in response to a request from the WVS server; and

the WVS server authenticating the terminal by the HTTP-Digest approach and completing the initial registration of the terminal.

2. The method as claimed in claim 1, wherein the security context information includes a user password for using the WVS.

3. The method as claimed in claim 2, wherein the WVS server authenticates the terminal by using an algorithm of the HTTP-Digest that is negotiated between the WVS server and the terminal.

4. The method as claimed in claim 1, further comprising:

the H-AAA server also sending realm information to the WVS server in the case when the WVS server is not aware of the realm information.

5. The method as claimed in claim 4, wherein the realm information is configured by an operator in the H-AAA.

6. The method as claimed in claim 1, further comprising:

the H-AAA using an algorithm of the HTTP-Digest to process the security context information before transmitting the security context information to the WVS server.

7. The method as claimed in claim 3 or 6, wherein the algorithm of the HTTP-Digest is an MD5 algorithm.

8. The method as claimed in claim 6, further comprising:

the H-AAA indicating to the WVS server the algorithm of the HTTP-Digest used.

9. The method as claimed in claim 1, further comprising:

the WVS server storing the security context information transmitted by the H-AAA server.

10. The method as claimed in claim 1, further comprising:

the terminal sending a register request for re-registration to the WVS server prior to the expiry of a registration timer set in the initial registration; and

the WVS server authenticates the terminal again by the HTTP-Digest approach.

11. The method as claimed in claim 1, further comprising:

updating the security context information in the WVS server when a user password for using the WVS is changed.

12. The method as claimed in claim 11, wherein when the user password is changed, the terminal and the H-AAA are informed of a new user password.

13. The method as claimed in claim 11, wherein the updating process includes:

the terminal initiating an initial registration procedure to the WVS server; and

the H-AAA server providing the WVS server with new security context information.

14. The method as claimed in claim 11, wherein the updating process includes:

the H-AAA server transmitting new security context information to the WVS server via a security context update message; and

the WVS server storing the new security context information and replying to the H-AAA server with a security context update acknowledgement message.

15. The method as claimed in claim 11, wherein the updating process includes:

the H-AAA server triggering a WVS de-registration procedure to de-register the registered terminal if the terminal is currently not in an active WVS session; and

the terminal initiating an initial registration procedure to the WVS server using new security context information.

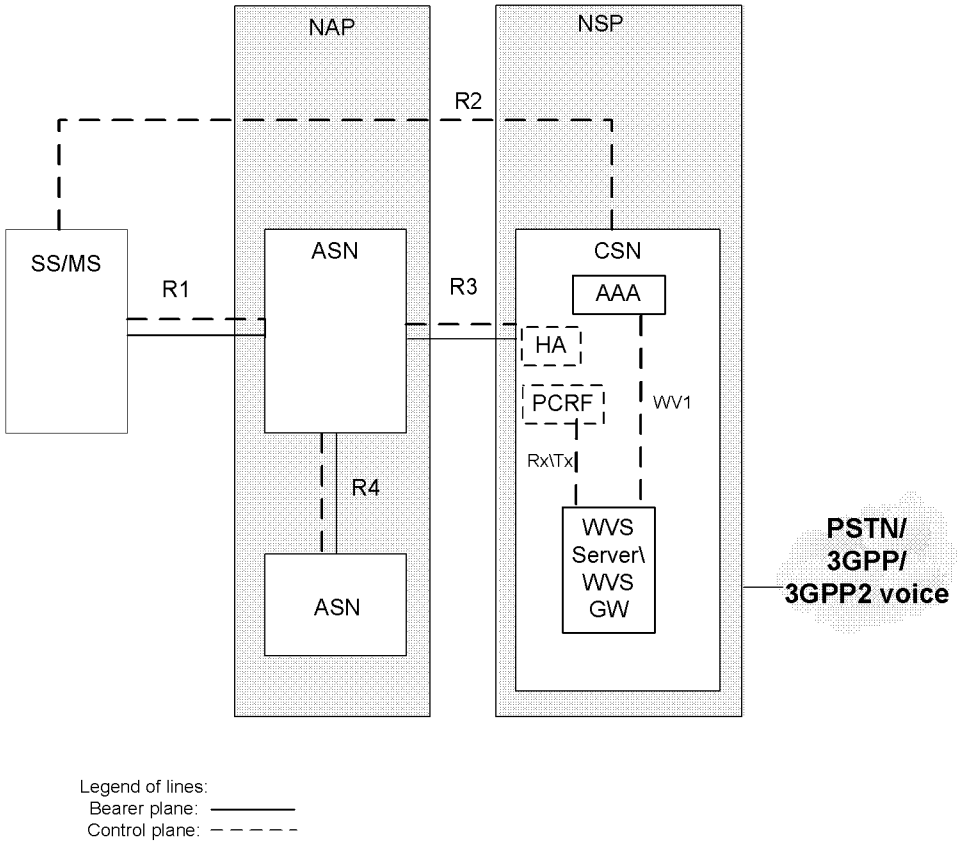
NAP
NSP
R2
SS/MS
R1
ASN
R3
CSN
AAA
HA
PCRF
WV1
Rx\Tx
R4
WVS Server\ WVS GW
ASN
PSTN/ 3GPP/ 3GPP2 voice
Legend of lines:
Bearer plane:
Control plane:

FIG. 1

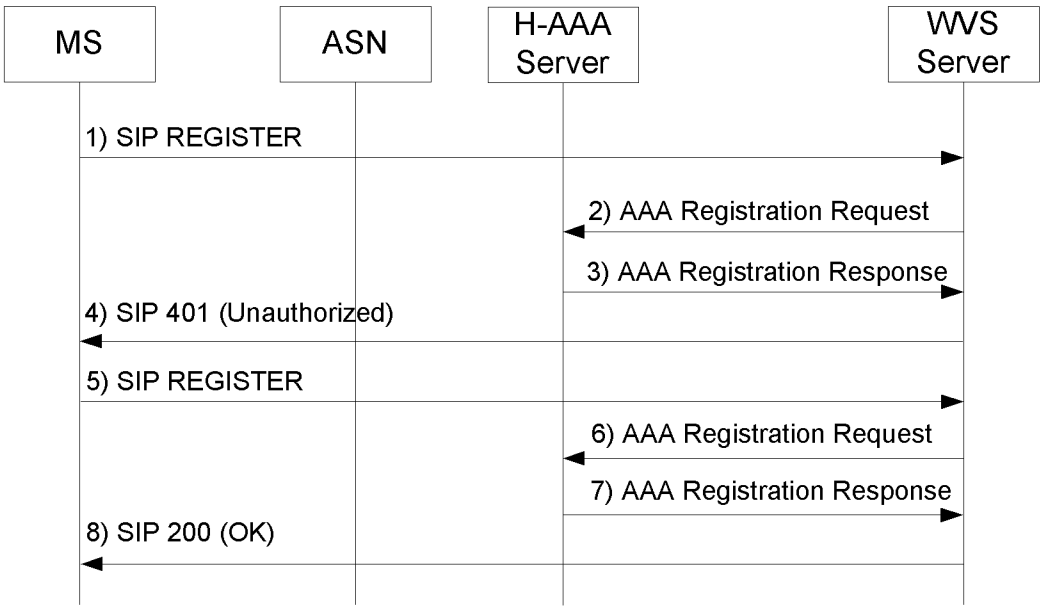
MS
ASN
H-AAA Server
WVS Server
1) SIP REGISTER
2) AAA Registration Request
3) AAA Registration Response
4) SIP 401 (Unauthorized)
5) SIP REGISTER
6) AAA Registration Request
7) AAA Registration Response
8) SIP 200 (OK)

FIG. 2

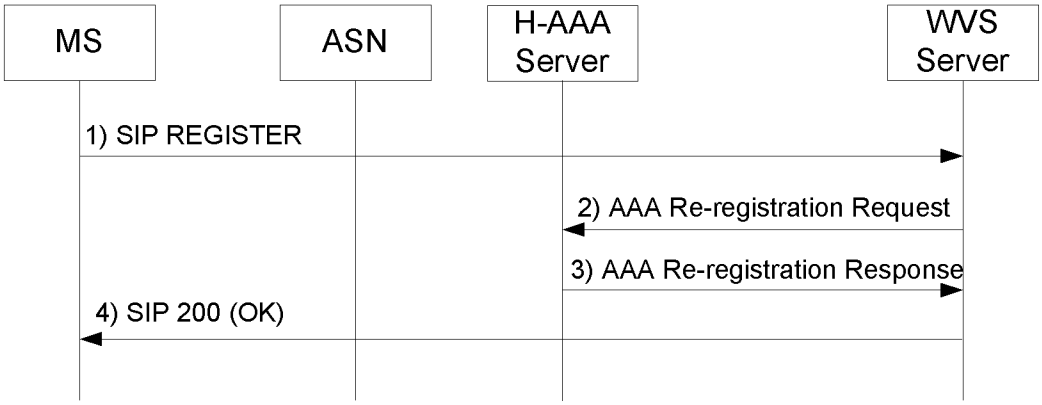
MS
ASN
H-AAA Server
WVS Server
1) SIP REGISTER
2) AAA Re-registration Request
3) AAA Re-registration Response
4) SIP 200 (OK)

FIG. 3

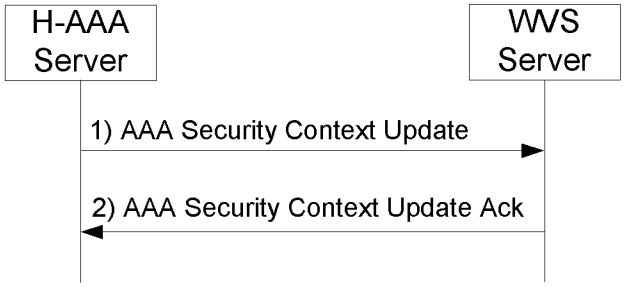
H-AAA Server
WVS Server
1) AAA Security Context Update
2) AAA Security Context Update Ack

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/078085

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W; H04Q; H04L; H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNKI; IEEE; CNPAT; GOOGLE: WiMAX voice call service HTTP digest registration re-registration AAA expiry SIP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WiMAX Forum White Paper, "WiMAX VoIP Solutions for 4G Networks", 30 Aug. 2010 (30.08.2010), sections 6.1-6.2, retrieved from the Internet: <URL: http:// www.wimaxforum.org/ sites/wimaxforum.org/files/document_library/WMF-M14-v01_WiMAX-VoIP-Solutions.pdf	1-15
A	RFC 2617, FRANKS, J. et al., "HTTP Authentication: Basic and Digest Access Authentication", Jun. 1999(06.1999), the whole document, retrieved from the Internet: <URL: http:// tools.ietf.org/ html/rfc2617	1-15
A	US2008130531A1 (CHOU, Joey) 05 Jun. 2008 (05.06.2008) the whole document	1-15
A	US2008273505A1 (HOLLINGSWORTH, Robert Lee et al.) 06 Nov. 2008 (06.11.2008) the whole	1-15

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 May 2011 (09.05.2011)	**23 Jun. 2011 (23.06.2011)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer MA, Mingyue Telephone No. (86-10) 62413398

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/078085

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	document	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/078085

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2008130531A1	05.06.2008	None	
US2008273505A1	06.11.2008	None	