US 20090170476A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2009/0170476 A1**

(43) **Pub. Date: Jul. 2, 2009**

**Lin et al.**

(54) **APPARATUS AND METHOD FOR EXECUTING THE HANDOFF PROCESS IN WIRELESS NETWORKS**

(76) Inventors: **Yi-Bing Lin**, Hsinchu (TW); **Shih-Feng Hsu**, Tainan (TW)

Correspondence Address:
**LIN & ASSOCIATES INTELLECTUAL PROPERTY, INC.**
**P.O. BOX 2339**
**SARATOGA, CA 95070-0339 (US)**

(21) Appl. No.: **12/114,818**

(22) Filed: **May 5, 2008**

(30) **Foreign Application Priority Data**

Dec. 26, 2007 (TW) ..... 096150292

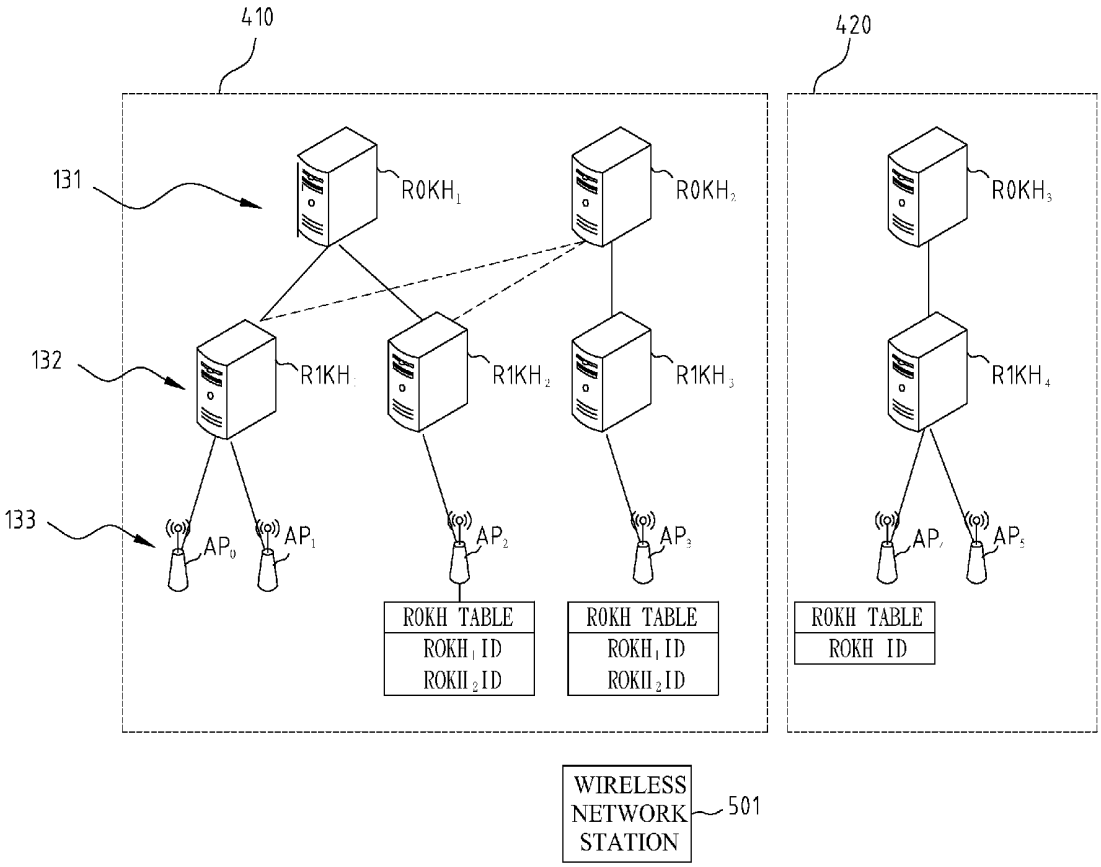
**Publication Classification**

(51) **Int. Cl.**
*H04M 1/66* (2006.01)

(52) **U.S. Cl.** ..... **455/411**

(57) **ABSTRACT**

Disclosed is an apparatus and method for executing the handoff process in the wireless networks. The apparatus comprises a processor to execute an identity checking mechanism. When a wireless network station wants to move from a source AP to a destination AP, the wireless network station sends an authentication request message to the destination AP. The identity checking mechanism searches a R0KH table of the destination AP for the R0KH ID contained in the authentication request message, and determines a setting parameter for executing a handoff process. Thereby, the wireless network station may execute the handoff process. A R0KH table of an AP consists of all IDs of R0KHs that can be accessed by the AP.



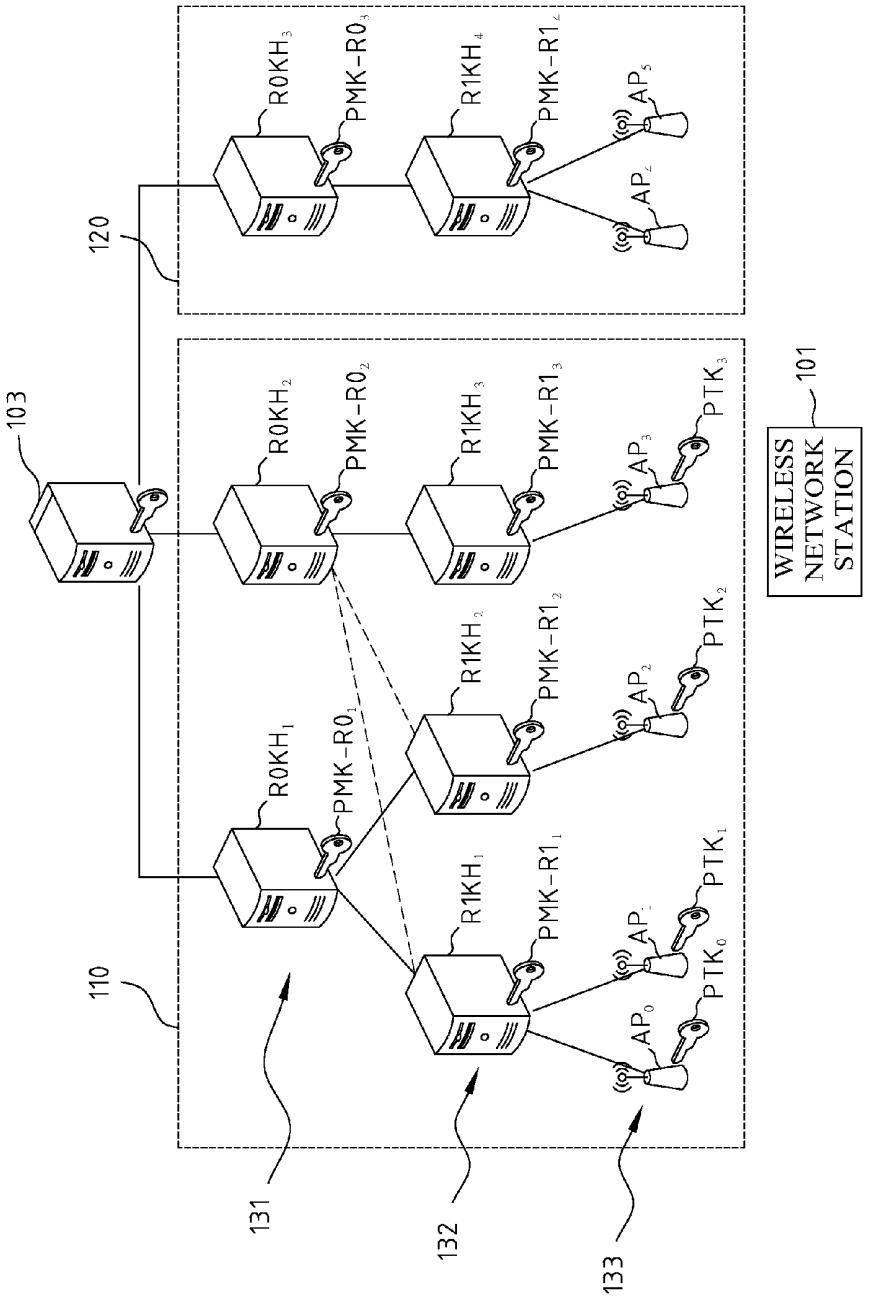



FIG. 1
(PRIOR ART)

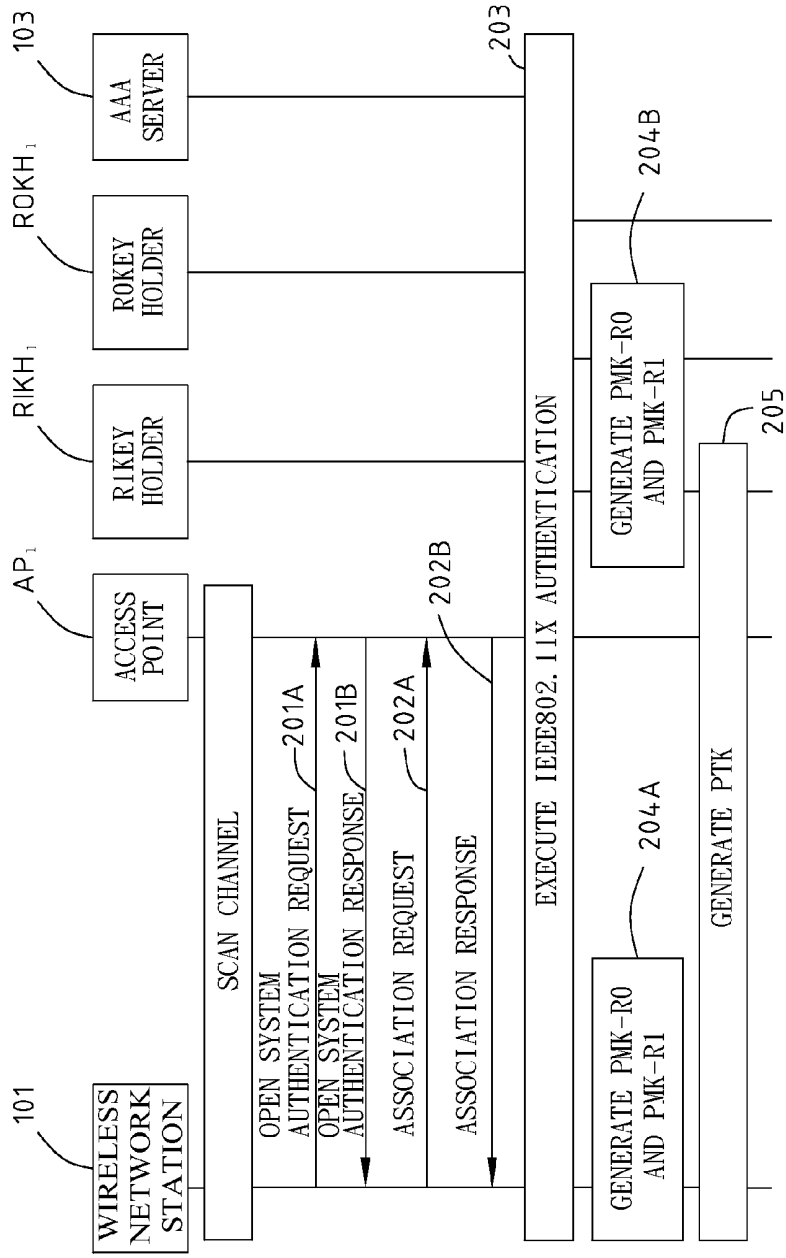



FIG. 2
(PRIOR ART)

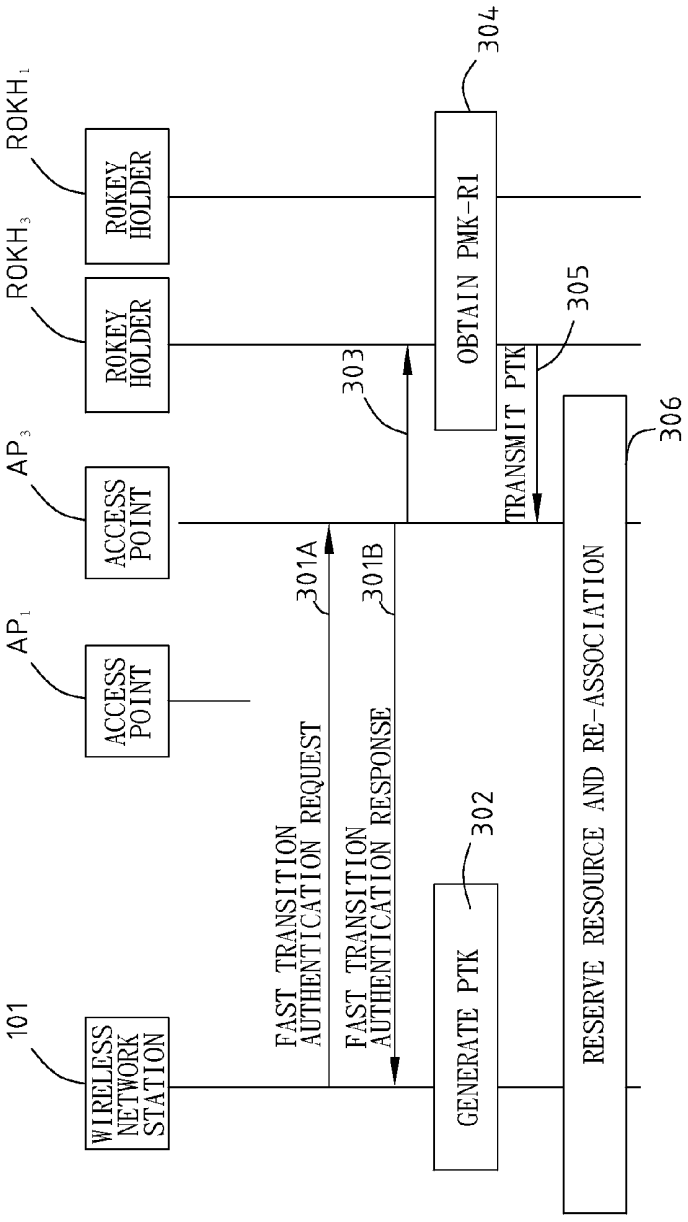



FIG. 3
(PRIOR ART)

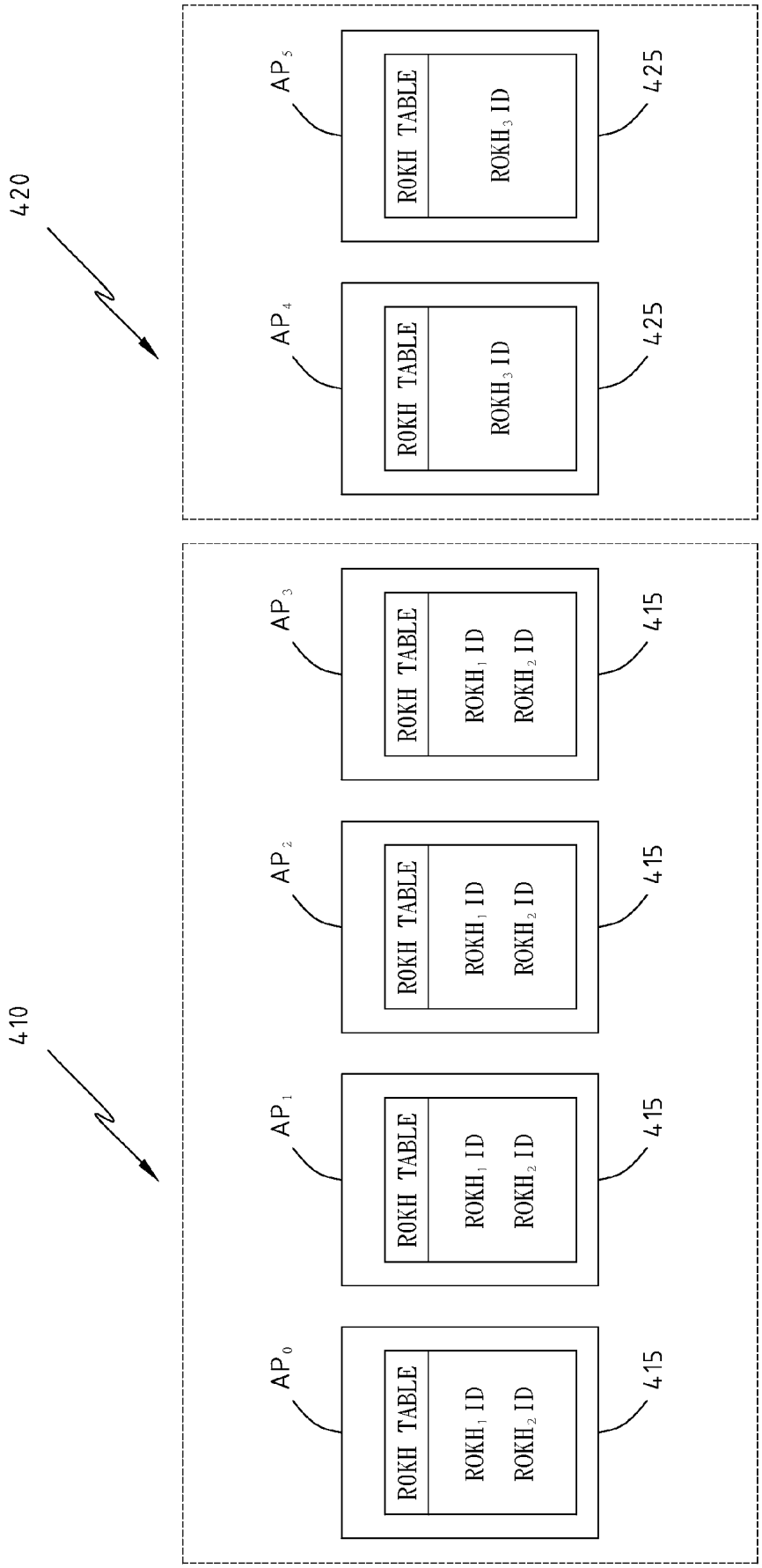

410
420
AP0
AP1
AP2
AP3
AP4
AP5
ROKH TABLE
ROKH1 ID
ROKH2 ID
ROKH3 ID
415
425

FIG. 4

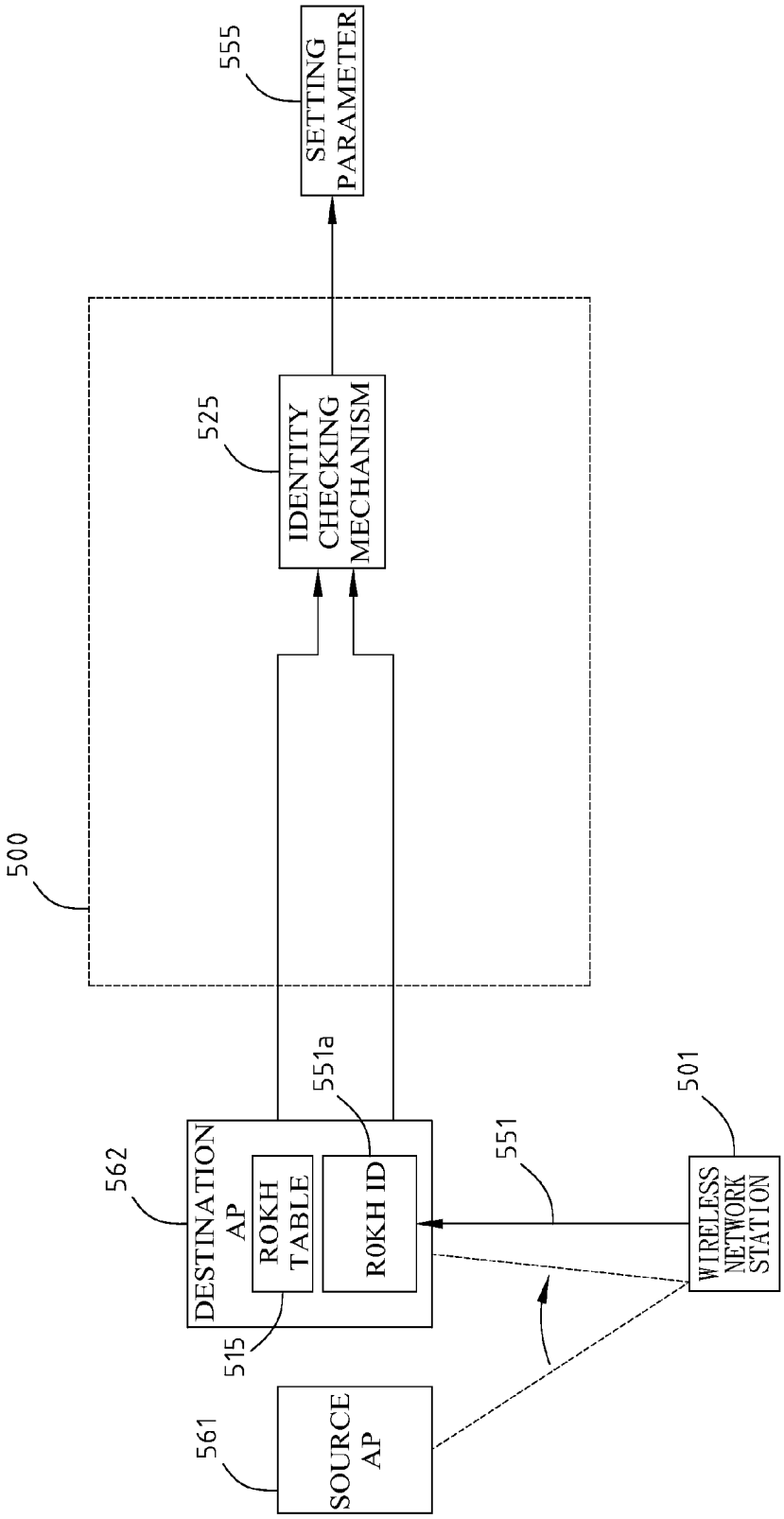

555
SETTING PARAMETER
525
IDENTITY CHECKING MECHANISM
500
551a
501
562
DESTINATION AP
ROKH TABLE
R0KH ID
551
WIRELESS NETWORK STATION
515
561
SOURCE AP

FIG. 5

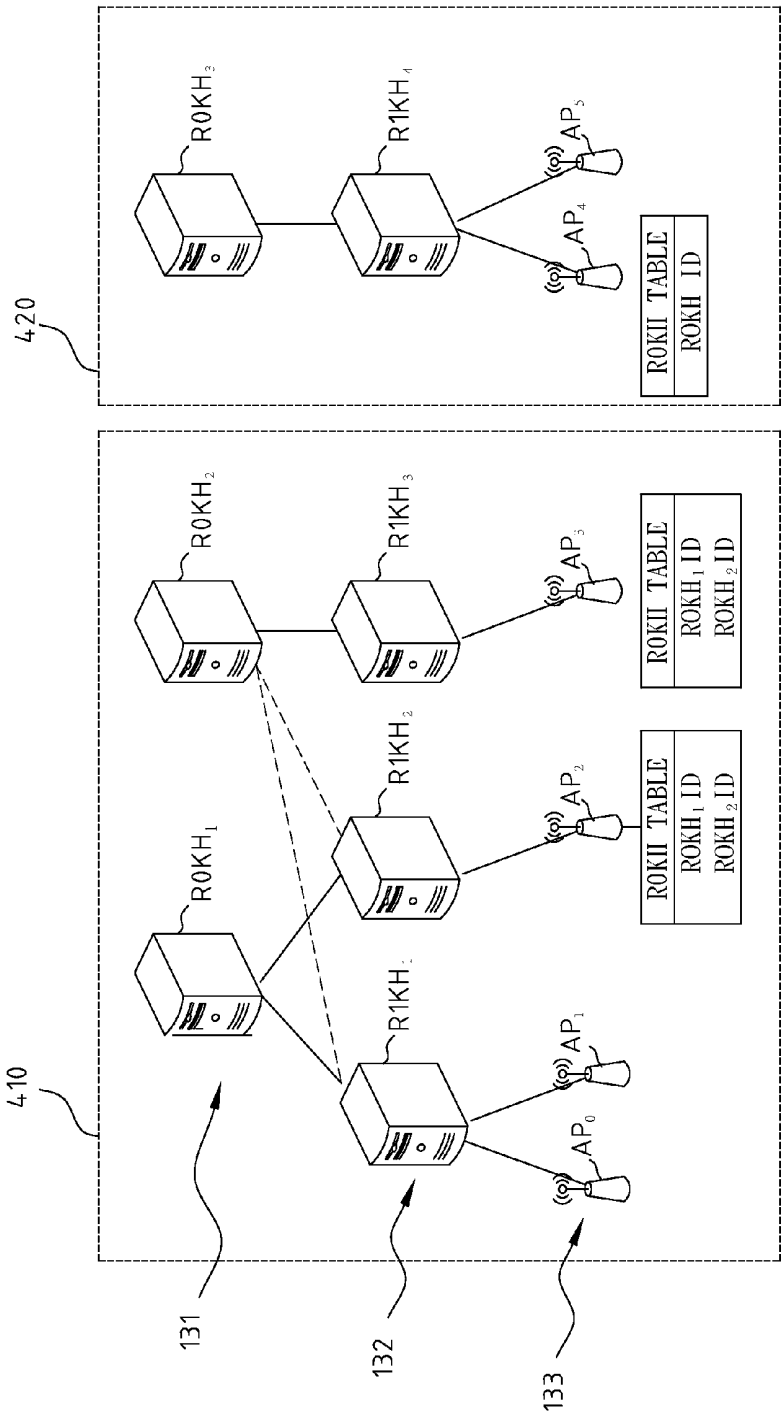

410
420
R0KH1
R0KH2
R0KH3
R1KH2
R1KH3
R1KH4
AP0
AP1
AP2
AP3
AP4
AP5
131
132
133
R0KII TABLE
ROKH1 ID
ROKH2 ID
R0KII TABLE
ROKH ID
WIRELESS NETWORK STATION
501

FIG. 6

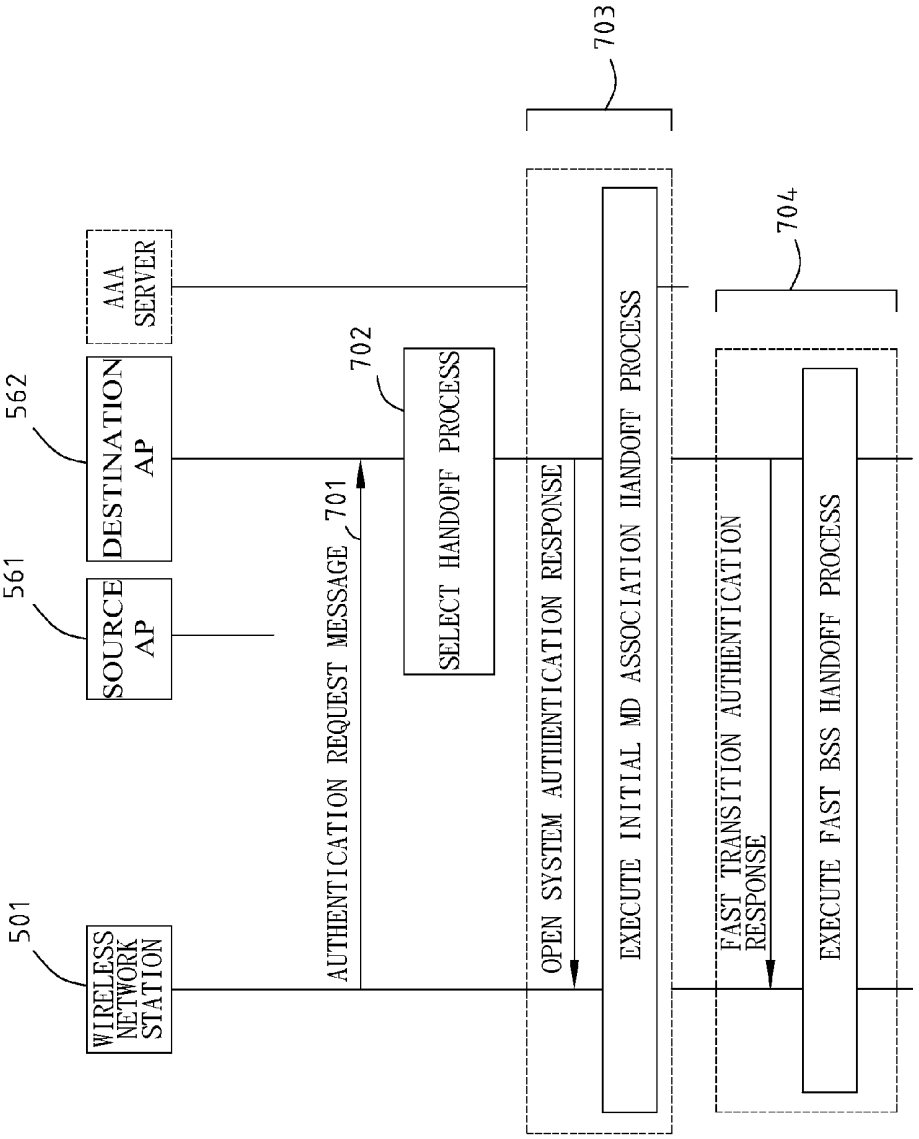

501
WIRELESS NETWORK STATION
561
SOURCE AP
562
DESTINATION AP
AAA SERVER
AUTHENTICATION REQUEST MESSAGE
701
702
SELECT HANDOFF PROCESS
703
OPEN SYSTEM AUTHENTICATION RESPONSE
EXECUTE INITIAL MD ASSOCIATION HANDOFF PROCESS
704
FAST TRANSITION AUTHENTICATION RESPONSE
EXECUTE FAST BSS HANDOFF PROCESS

FIG. 7

# APPARATUS AND METHOD FOR EXECUTING THE HANDOFF PROCESS IN WIRELESS NETWORKS

## FIELD OF THE INVENTION

**[0001]** The present invention generally relates to an apparatus and method for executing the handoff process in the wireless networks.

## BACKGROUND OF THE INVENTION

**[0002]** The wireless networks are an important medium for connecting to Internet. The wireless network is more prone to tapping and theft in comparison with the wired network. Between an access point (AP) and a wireless network station, the use of security key for authentication and encryption is an important issue for wireless networks. If the AP and the wireless network station do not save the security key in advance, the key will cause the execution of a handoff process when the wireless network station connected to an AP.

**[0003]** Because the handoff process takes much time, the execution of the handoff process may interrupt the real-time application, such as voice over IP (VoIP). IEEE802.11r protocol defines three-level key architecture to accelerate the execution of handoff process and generate security key.

**[0004]** FIG. **1** shows a schematic view of an exemplary three-level key architecture of IEEE802.11r protocol. Referring to FIG. **1**, the first level key is Pairwise Master Key R**0**, or PMK-R**0**. PMK-R**0** is generated by the first level Master Session Key (MSK) or Authentication, Authorization and Accounting (AAA)-key, and is saved at a wireless network station **101** and a R**0** key holder (R**0**KH). MSK is generated and separately by wireless network station **101** executing the handoff process and by AAA server **103** executing IEEE802.1X authentication. R**0**KH plays the role of AAA client to receive and store the MSK from AAA server **103**.

**[0005]** The second level key PMK-R**1** is stored at wireless network station **101** and a R**1** key holder (R**1**KH). PMK-R**1** is generated by PMK-R**0**. PMK-R**1** may be used to generate the third level Pairwise Transient Key (PTK). The PTK is the key for message encryption and decryption between wireless network station **101** and the APs inside the third level.

**[0006]** The aforementioned IEEE802.11r three-level key architecture defines the mobility domain (MD) architecture. As shown in FIG. **1**, an MD includes a plurality of R**0**KHs at first level **131**. Each R**0**KH has connections to a plurality of R**0**KHs, for R**1** from all the R**0**KHs in the MD, for example, $R1KH_1$ and $R1KH_2$ may obtain PMK-R**1** directly from $R0KH_1$, or indirectly from $R0KH_2$. Second level **132** is all the R**1**KHs. Third level **133** is all the APs of an MD in the following description.

**[0007]** Based on the MD architecture defined in IEEE802.11r protocol specifications, the movement of the wireless network station may be divided into intra-MD movement and Inter-MD movement. The intra-MD movement may be further divided into intra-R**1**KH movement and inter-R**1**KH movement. For example, wireless network station **101** switching from $AP_0$ to $AP_1$ is an intra-R**1**KH movement, and switching from $AP_1$ to $AP_2$ or $AP_3$ is an inter-R**1**KH movement. These two examples are both intra-MD movements within domain **110**. On the other hand, a switching from $AP_3$ in MD **110** to $AP_4$ in MD **120** is an inter-MD movement.

**[0008]** When moving in MD, a wireless network station needs to execute a fast basic service set (Fast BSS) handoff process. For inter-MD movement, the wireless network station needs to execute initial MD association handoff process. Through the MD Identity (MDID) embedded in the periodical broadcast of probe and beacon messages by the AP, it is possible to distinguish the inter-MD movement from intra-MD movement.

**[0009]** The current MDID can be assigned by each vendor; however, there is no guarantee that the MDID assigned by different vendors will be unique. Therefore, when a wireless network station executes inter-MD movement, the inter-MD movement may be mistakenly identified as an intra-MD movement because of the same MDID, and then the Fast BSS handoff process is executed. In this scenario, during the execution of Fast BSS handoff process, the AP cannot generate PTK because the R**1**KH cannot obtain PMK-R**1** from R**0**KH used by the wireless network station. Therefore, the AP will notify the wireless network station to terminate the Fast BSS handoff process, and to execute the initial MD association handoff process.

**[0010]** FIG. **2** and FIG. **3** show the exemplary flowcharts of initial MD association handoff process and the Fast BSS handoff process, respectively.

**[0011]** In FIG. **1**, when wireless network station **101** turns on the wireless network function, wireless network station **101** can connect to the wireless network through $AP_1$ of MD **110**, or move from MD **120** to the coverage range of $AP_1$, which can be known from the probe and beacon messages broadcast by $AP_1$ to be an inter-MD movement. Wireless network station **101** executes the initial MD association handoff process in FIG. **2**.

**[0012]** In step **201**A and step **201**B, wireless network station **101** and $AP_1$ execute the open system authentication process. In step **201**A, wireless network station **101** transmits authentication request to $AP_1$. In step **201**B, $AP_1$ replies the authentication response to wireless network station **101**. After the open system authentication process finishes, $AP_1$ allows wireless network station **101** to transmit IEEE802.11r communication protocol messages to AAA server.

**[0013]** Steps **202**A & **202**B are association request and association response, respectively. In step **202**A, wireless network station **101** transmits association request to $AP_1$, where the field of the mobility domain information element (MDIE) of the association request message is set as "0" to indicate that wireless network station **101** supports Fast BSS handoff process. In step **202**B, $AP_1$ uses association response message to store the $R0KH_1$, $R1KH_1$ and MDID in the MDIE field, and transmits the association response message to wireless network station **101**.

**[0014]** In step **203**, wireless network station **101** executes the IEEE803.1X authentication to AAA server **103** through $AP_1$. After the authentication step is successful, wireless network station **101** and AAA server **103** generate the MSK respectively, and AAA server **103** will transmit the MSK to $R0KH_1$.

**[0015]** Steps **204**A & **204**B are to generate PMK-R**0** and PMK-R**1**, respectively. In step **204**A, wireless network station **101** and $R0KH_1$ execute the key derivation function (KDF) algorithm, respectively, to use $R0KH_1$ with MSK, and the MAC address of wireless network station **101** to generate PMK-R**0**. In step **204**B, PMK-R**1** may be generated by using PMK-R**0**, MAC address of wireless network station **101**, and ID of $R1KH_1$.

**[0016]** In step **205**, wireless network station **101** and $AP_1$ execute the 4-way handshake of IEEE802.11i to generate

PTK. In this step, wireless network station **101** and $AP_1$ generate a random number "SNonce" and a random number "ANonce", respectively, and exchange. $AP_1$ transmit the two random numbers "SNonce" and "ANonce", ID of $R0KH_1$, MAC address of wireless network station **101** and MAC address of $AP_1$ to $R1KH_1$. Then, wireless network station **101** and $R1KH_1$ execute KDF algorithm, respectively, and use the above parameters, ID of $R1KH_1$ and PMK-R1 to generate PTK. After generating PTK, $R1KH_1$ transmits the PTK to $AP_1$.

**[0017]** After executing the above initial MD association handoff process, wireless network station **101** is successfully connected to $AP_1$, and $R0KH_1$ and $R1KH_1$ will store PMK-R0 and PMK-R1, respectively. PMK-R0 and PMK-R1 may be used to generate a new PTK. Therefore, the time-consuming IEEE802.1X authentication process may be saved to reduce the handoff process time.

**[0018]** When the wireless network station moves within $MD_1$, for example, from $AP_1$ to $AP_3$, the wireless network station may execute the Fast BSS handoff process of FIG. **3**.

**[0019]** Because $AP_1$ and $AP_3$ are both in $MD_1$, in step **301**A, wireless network station **101** notifies $AP_3$ through the fast transition (FT) authentication request message to execute FT authentication. The authentication request message includes a random number SNonce for generating PTK, and an MDIE field. The MDIE field includes the IDs of $R0KH_1$, $R1KH_1$, and MDID of $MD_1$.

**[0020]** $AP_3$ knows of the occurrence of the inter-R1KH switch from the authentication request message, and replies an authentication response message to wireless network station **101**, as shown in step **301**B. The authentication response message includes a random number ANonce for generating PTK, and an MDIE field. The MDIE field at least includes the IDs of $R0KH_2$, $R1KH_3$, and MDID of MD **110**.

**[0021]** After receiving the FT authentication response message from $AP_3$, wireless network station **101** uses random number ANonce and MDIE, and with ID of $R1KH_3$, MAC address of wireless network station **101** and PMK-R0 to generate PMK-R1. The PMK-R1 will be stored in wireless network station **101** and $R1KH_3$. Then, step **302** is to generate PTK according to MAC address of wireless network station **101**, MAC address of $AP_3$, SNonce, ANonce, and IDs of $R0KH_1$ and $R1KH_3$. If wireless network station **101** moves from $AP_1$ to $AP_0$, the old PMK-R1 may be used directly to generate PTK because $AP_1$ and $AP_0$ are connected to the same R1KH.

**[0022]** As shown in step **303**, $AP_3$ transmits MAC address of wireless network station **101**, MAC address of AP, SNonce, ANonce, ID of $R0KH_1$ to $R1KH_3$ for generating new PTK.

**[0023]** In step **304**, according to the ID of $R0KH_1$, $R1KH_3$ requests PMK-R1 from $R0KH_1$. However, if wireless network station **101** moves from $AP_1$ to $AP_0$, this step may be omitted.

**[0024]** After obtaining new PMK-R1, $R1KH_3$ executes KDF algorithm to generate network station **101** and $AP_3$ both have the same PTK.

**[0025]** Wireless network station **101** and $AP_3$ then execute step **306** for resource from $AP_1$ to $AP_3$. In this manner, wireless network station **101** may start to use $AP_3$ service.

**[0026]** In the Fast BSS handoff process, the PMK-R0 is re-used to generate new PTK to accelerate the handoff process. Because the AP will broadcast the probe and beacon response frame with the IDs of R0KH and R1KH used by the AP and the ID of MD embedded in the frame, the appropriate handoff process may be selected after the wireless network station selects the AP, and whether the movement is an Inter-MD movement or an intra-MD movement is determined. Especially, the MAC address may be used to identify R0KH and R1KH, and MDID is managed by the vendors.

## SUMMARY OF THE INVENTION

**[0027]** In accordance with the exemplary embodiments of the present invention, the disclosed is directed to an apparatus and method for executing the handoff process in wireless networks. Without MDID for executing handoff process, the uncertainty of MDID may be ruled out. In the present disclosure, each AP stores a R0KH table, and the R0KH table records the IDs of all the R0KHs at the AP.

**[0028]** In an exemplary embodiment of the present invention, the disclosed is directed to an apparatus for executing handoff process in wireless network. The apparatus comprises a processor to execute an identity checking mechanism. The R0KH table of a destination AP consists of the IDs of all the R0KHs accessible within the coverage of the destination AP. When a wireless network station wants to move from a source AP to a destination AP, the wireless network station sends an authentication request message to the destination AP. The identity checking mechanism searches the R0KH table of the destination AP for the R0KH ID contained in the authentication request message, and determines a setting parameter for executing a handoff process. Thereby, the wireless network station may execute the handoff process.

**[0029]** In another exemplary embodiment of the present invention, the disclosed is directed to a method for executing handoff process in wireless networks, applicable to the movement of a wireless network station. When a wireless network station wants to move from a source AP to a destination AP, the method comprises: a wireless network station transmitting an authentication request message to the destination AP, the authentication request message including an R0KH ID; using the R0KH ID to search the R0KH table of the destination AP for selecting a transition process, the R0KH table of destination AP including the IDs of all the R0KHs accessible to the destination AP; when the R0KH ID not in the R0KH table, executing an initial MD association handoff process; and when the R0KH ID in the R0KH table, executing a Fast BSS handoff process.

**[0030]** The foregoing and other features, aspects and advantages of the present invention will become better understood from a careful reading of a detailed description provided herein below with appropriate reference to the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0031]** FIG. **1** shows a schematic view of an exemplary 3-level key architecture of IEEE802.11r communication protocol.

**[0032]** FIG. **2** shows a schematic view of an exemplary flowchart of a wireless network station executing initial MD association handoff protocol.

**[0033]** FIG. **3** shows a schematic view of an exemplary flowchart of a wireless network station executing Fast BSS handoff protocol.

**[0034]** FIG. **4** shows a schematic view of an exemplary R0KH table, consistent with certain disclosed embodiments of the present invention.

**[0035]** FIG. **5** shows a schematic view of an exemplary apparatus for executing handoff process in a wireless network, consistent with certain disclosed embodiments of the present invention.

**[0036]** FIG. **6** shows an exemplary schematic view of the R0KH tables stored at source AP and destination AP for a wireless network station to execute an inter-MD or an Intra-MD movement, consistent with certain disclosed embodiments of the present invention.

**[0037]** FIG. **7** shows a schematic view of an exemplary flowchart of the method for executing handoff process in wireless networks, consistent with certain disclosed embodiments of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

**[0038]** The disclosed embodiments in accordance with f the present invention may provide an apparatus and a method for the AP to select the suitable handoff process for the wireless network station without using the MDID to avoid the MDID collision. In the disclosed embodiments, each AP stores a R0KH table with all the R0KH IDs. When the wireless network station moves from an AP to another AP, the present invention may help the wireless network station to select a suitable handoff process by searching the R0KH table. The movement of the wireless network station may be either inter-MD movement or intra-MD movement.

**[0039]** Take the 3-level key architecture of IEEE802.11r communication protocol in FIG. **1** as an example. The R0KH table of the present invention may be described as in FIG. **4**. Because in the architecture of FIG. **1**, the R0KH ID holders of MD **110** are $R0KH_1$ and $R0KH_2$ of first level **131**, therefore, each AP of MD **410** of FIG. **4**, i.e., $AP_0$, $AP_1$, $AP_2$, $AP_3$, stores a R0KH table **415** consisting of $R0KH_1$ ID and $R0KH_2$ ID. Similarly, in the architecture of FIG. **1**, the R0KH ID holder of MD **120** is $R0KH_3$, therefore, each AP of MD **420** of FIG. **4**, i.e., $AP_4$, $AP_5$, stores a R0KH table **425** consisting of $R0KH_3$ ID.

**[0040]** With the R0KH table, each AP may select the suitable handoff process for the wireless network station without MDID. FIG. **5** shows a schematic view of an exemplary apparatus for executing handoff process in a wireless network, consistent with certain disclosed embodiments of the present invention.

**[0041]** Referring to FIG. **5**, an apparatus **500** comprises a processor (not shown) for executing an identity checking mechanism **525**. When a wireless network station **501** wants to move from a source AP **561** to a destination AP **562**, wireless network station **501** transmits an authentication request message **551** to destination AP **562**. Identity checking mechanism **525** uses a R0KH ID **551***a* in authentication request message **551** to search for R0KH table **515** and determines a setting parameter **555** of a handoff process. R0KH table **515** may include the IDs of all the R0KHs in the coverage range accessible to the destination AP.

**[0042]** For example, in FIG. **6**, when wireless network station **501** wants to move from $AP_2$ to $AP_3$, identity checking mechanism **525** checks and finds that $R0KH_2$ ID is in the R0KH table at $AP_3$, it may determines that the FT authentication is a setting parameter for the handoff process. On the other hand, when wireless network station **501** wants to move from $AP_2$ to $AP_4$, identity checking mechanism **525** checks and finds that $R0KH_3$ ID is not in the R0KH table at $AP_3$, it may determines that the open system authentication is a setting parameter for the handoff process.

**[0043]** After receiving the authentication response message from the destination AP, wireless network station **501** will execute the Fast BSS handoff process if the setting parameter in the response message is FT authentication; on the other hand, wireless network station **501** will execute the initial MD association handoff process if the setting parameter is the open system authentication.

**[0044]** Therefore, in FIG. **6**, when wireless network station **501** makes an intra-MD movement, such as, from $AP_2$ to $AP_3$, the setting parameter in the response message is FT authentication. Hence, wireless network station **501** will execute the Fast BSS handoff process. If wireless network station **501** makes an inter-MD movement, such as, from $AP_2$ to $AP_4$, the setting parameter in the response message is the open system authentication. Hence, wireless network station **501** will execute initial MD association handoff process. So, regardless the movement is an inter-MD or an Intra-MD movement, the wireless network station may always execute the suitable handoff process.

**[0045]** Because the change and update of the R0KHs within the MD cover range is less frequent, the contents of R0KH table **515** may be either dynamically or statically set in AP through the AP management system. The storing of the IDs of all the R0KHs may be done through the search of R0KH table **515**, and the AP management system allows the wireless network station to select the handoff process. The exemplary structure of the disclosed embodiments in accordance with the present invention does not need to manage MDID. Therefore, the execution of unsuitable handoff process caused by the MDID collision will not occur. The present invention is also applicable to the wireless network platforms of IEEE802.11r communication protocol.

**[0046]** According to the exemplary architecture of the disclosed embodiments, when the change or update of the R0KHs of a MD occurs, the IDs of the R0KHs in the AP may be dynamically or manually updated.

**[0047]** FIG. **7** further shows a schematic view of an exemplary flowchart of the method for executing handoff process in wireless networks, consistent with certain disclosed embodiments of the present invention. Referring to FIG. **7**, after wireless network station **501** successfully executes data communication and connection with source AP **561**, and when wireless network station **501** wants to move from source AP **561** to destination AP **562**, destination AP **562** has an R0KH table. The R0KH table stores the IDs of all the R0KHs accessible to destination AP **562** within the MD cover range. The following steps **701-704** describe the execution of handoff process.

**[0048]** Step **702** is to select the handoff process. Through searching for the ID of the message to destination AP **562**. The authentication request message notifies destination AP **562** to execute FT authentication. The authentication request message at least contains the information of a R0KH ID, but the MDID information is not necessary included in the authentication request message.

**[0049]** Step **702** is to select the handoff process. Through searching for the ID of the R0KH in the R0KH table of destination AP **562**, a suitable handoff process may be determined. After destination AP **562** receives the authentication request message from wireless network station **501**, destination AP **562** reads the R0KH ID in the message, and compares with the R0KH table of destination AP to determine whether

wireless network station **501** should execute initial MD association handoff process (step **703**), or Fast BSS handoff process (step **704**).

**[0050]** When R0KH ID is not stored in the R0KH table of destination AP **562**, destination AP **562** executes the open system authentication and replies the authentication response message to wireless network station **501**, as in step **703**. In the response message, the setting parameter is set as the open system authentication. After wireless network station **501** receives the response message, wireless network station **501** executes the initial MD association handoff process. The description of the initial MD association handoff process is as in FIG. **2**, and is omitted here.

**[0051]** When R0KH ID is already stored in R0KH table of destination AP **562**, destination AP **562** executes the FT authentication and replies the authentication response message to wireless network station **501**, as in step **704**. In the response message, the setting parameter is set as the FT authentication. After wireless network station **501** receives the response message, wireless network station **501** executes the Fast BSS handoff process. The description of the fast BSS handoff process is as in FIG. **3**, and is omitted here.

**[0052]** In this manner, without the MDID for handoff process, the present invention may avoid the uncertainty of MDID. Also, through searching for the R0KH table stored at AP, the wireless network station may distinguish whether the movement is an inter-MD movement or an intra-MD movement, and selects a suitable handoff process accordingly.

**[0053]** Although the present invention has been described with reference to the exemplary embodiments, it will be understood that the invention is not limited to the details described thereof. Various substitutions and modifications have been suggested in the foregoing description, and others will occur to those of ordinary skill in the art. Therefore, all such substitutions and modifications are intended to be embraced within the scope of the invention as defined in the appended claims.

What is claimed is:

**1**. An apparatus for executing handoff process in wireless networks, applicable to the movement of a wireless network station when said wireless network station moving from a source access point (AP) to a destination AP, said apparatus comprising:

a processor, executing an identity (ID) checking mechanism, said wireless network station transmitting an authentication request message to said destination AP, said ID checking mechanism using a R0 key holder (R0KH) ID included in said authentication request message to search a R0KH table of said destination AP for determining a setting parameter for a handoff process, and said wireless network station executing said handoff process according to said setting parameter;

wherein said R0KH table of said destination AP consisting of the IDs of all said R0KHs accessible to said destination AP within the cover range of said destination AP.

**2**. The apparatus as claimed in claim **1**, wherein said handoff process is either an initial mobility domain (MD) association handoff process or a Fast Basic Service Set handoff process.

**3**. The apparatus as claimed in claim **1**, wherein each AP in said wireless network stores a R0KH table consisting of the IDs of all R0KHs accessible to said AP within the cover range of said AP.

**4**. The apparatus as claimed in claim **1**, wherein when said R0KH ID contained in said authentication request message is stored in said R0KH table, said setting parameter of said handoff process is fast transition authentication.

**5**. The apparatus as claimed in claim **1**, wherein when said R0KH ID contained in said authentication request message is not stored in said R0KH table, said setting parameter of said handoff process is open system authentication.

**6**. The apparatus as claimed in claim **1**, wherein said apparatus is applied to IEEE802.11r protocol.

**7**. The apparatus as claimed in claim **1**, wherein said movement of said wireless network station is either an inter-MD movement or an intra-MD movement.

**8**. A method for executing handoff process in wireless networks, applicable to the movement of a wireless network station when said wireless network station moving from a source access point (AP) to a destination AP, said method comprising:

said wireless network station transmitting an authentication request message to said destination AP, said authentication request message containing a R0 key holder identity (R0KH ID);

using said R0KH ID to search a R0KH table of said destination AP for determining a handoff process, said R0KH table of said destination AP consisting of the IDs of all said R0KHs accessible to said destination AP within the cover range of said destination AP;

when said R0KH ID not being stored in said R0KH table, said wireless network station executing an initial mobility domain (MD) association handoff process; and

when said R0KH ID being stored in said R0KH table, said wireless network station executing a Fast Basic Service Set (BSS) handoff process.

**9**. The method as claimed in claim **8**, wherein each AP in said wireless network stores a R0KH table consisting of the IDs of all said R0KHs accessible to said AP within the cover range of said AP.

**10**. The method as claimed in claim **8**, wherein when said R0KH ID contained is not stored in said R0KH table, said destination AP replies an authentication response message containing a setting parameter of said handoff process, and sets said setting parameter as open system authentication.

**11**. The method as claimed in claim **8**, wherein when said R0KH ID contained is stored in said R0KH table, said destination AP replies an authentication response message containing a setting parameter of said handoff process, and sets said setting parameter as fast transition (FT) authentication.

**12**. The method as claimed in claim **8**, wherein said source AP and said destination AP are both in the same MD.

**13**. The method as claimed in claim **8**, wherein said source AP and said destination AP are in different MDs.

**14**. The method as claimed in claim **10**, wherein said wireless network station executes an initial MD association handoff process.

**15**. The method as claimed in claim **11**, wherein said wireless network station executes a Fast BSS handoff process.

* * * * *