ENABLE WI-FI DEVICE IDENTITY WITH MAC RANDOMIZATION ENABLED

INVENTOR:

LUTHER E. SMITH

Description

To provide user or device identity privacy when using Wi-Fi technology, the IETF and OS vendors have introduced MAC randomization. The use of a randomized MAC address breaks various implemented functions and feature in use on Wi-Fi Local Area Networks also know as Wireless Local Area Network (WLAN). The need to have a consistent device identification enable functions as device verification, allow and deny list, parental control, device prioritization, and lawful intercept.

Since open Wi-Fi network do not afford any method to encrypt information transmitted over the air, all remaining Wi-Fi networks have some type of encryption. This encryption is established during the association phase of a device becoming enabled on the Wi-Fi network.

This idea is to establish a protocol exchange that happens after the association phase is completed and before the Wi-Fi network allows the device access to functions, features and Internet access. In this interim state the Wi-Fi Access Point(AP) and the device (Station - STA) exchange messaging to allow the AP to know the true identity of the STA. The exchange is initiated by the AP once STA association is completed requesting the STA to provide the unique manufacture MAC address. The STA then response with the unique manufacture MAC address of the STA.

The AP can use the unique MAC address in the same manner that features and functions were designed to make use of the STA MAC address. This includes but not limited to device/STA verification, allow and deny list, parental control, device prioritization, lawful intercept, and tracking acceptance of Terms and Conditions.

Since this messaging exchange is done after association, the over the air data is encryption in all cased exception open Wi-Fi networks. In the case of an open Wi-Fi network the AP would not initiate the protocol to get the STA unique manufacture MAC address. In the case where the STA MAC address offered by the STA during association is not randomized then the AP would not the protocol to get the STA unique manufacture MAC address.

This can be extended to have the requesting message from the AP to include encryption keys (public key) to be used by the STA to encrypt the STA's MAC Address. Since the AP is providing the public key, only the AP can decrypt the STA MAC Address thus keeping the STA MAC Address secure. In the case of open networks, if the same public key is used then tracking could be done by monitor for the same encrypted STA MAC Address string. This can be avoided by the AP using random key pairs.

Background

Multiple device (STA) OS vendors are attempting to address user privacy issues. Since the device MAC address is sent in the clear over the air, the user or are least the device

could be tracked by anyone that is sniffing the RF of a Wi-Fi LAN. This could be used for tracking and also implementing spoofing of another user MAC address. To combat this the OS vendors have moved to make use of randomized MAC address. In doing so functions that relied on the MAC address of device are impacted. This impact was to the scale that the OS vendors had to rethink how MAC randomization is done to ensure the same MAC address is used per SSIDs. Some services impacted are:

- Parental controls
- Lawful intercept
- Access/deny list
- Captive portal access
- Terms and conditions
-

Several standards groups are working on solutions (WBA/WFA/IETF/IEEE). There are also new technology to assist with identifying devices such as RF Finger Printing.
If there was a method that an AP can get the device real or unique MAC address that above services could continue to function while protecting the user privacy. While this is not a 100% fix, that application where this would not apply, which is an open Wi-Fi LAN, that is already not expectation by users of privacy. Thus the solution suggested as the invention idea would cover all other cases - basically covering all (100%) use cases where user privacy is an expectation.

Abstract

To provide user or device identity privacy when using Wi-Fi technology, the IETF and OS vendors have introduced MAC randomization. The use of a randomized MAC address breaks various implemented functions and feature in use on Wi-Fi Local Area Networks also know as Wireless Local Area Network (WLAN). The need to have a consistent device identification enable functions as device verification, allow and deny list, parental control, device prioritization, and lawful intercept.

Since open Wi-Fi network do not afford any method to encrypt information transmitted over the air, all remaining Wi-Fi networks have some type of encryption. This encryption is established during the association phase of a device becoming enabled on the Wi-Fi network.

This idea is to establish a protocol exchange that happens after the association phase is completed and before the Wi-Fi network allows the device access to functions, features and Internet access. In this interim state the Wi-Fi Access Point(AP) and the device (Station - STA) exchange messaging to allow the AP to know the true identity of the STA. The exchange is initiated by the AP once STA association is completed requesting the STA to provide the unique manufacture MAC address. The STA then response with the unique manufacture MAC address of the STA.

The AP can use the unique MAC address in the same manner that features and functions were designed to make use of the STA MAC address. This includes but not limited to device/STA verification, allow and deny list, parental control, device prioritization, lawful intercept, and tracking acceptance of Terms and Conditions.

Since this messaging exchange is done after association, the over the air data is encryption in all cased exception open Wi-Fi networks. In the case of an open Wi-Fi network the AP would not initiate the protocol to get the STA unique manufacture MAC address. In the case where the STA MAC address offered by the STA during association is not randomized then the AP would not the protocol to get the STA unique manufacture MAC address.

A solution that addresses all network types, including open networks, that the in the AP request for the unique STA MAC address, the AP would generate a unique key pair and provide the public key to the STA. The STA then encrypts the unique MAC address with the public key and then returns the encrypted unique MAC address. Since over an open network monitoring can see happen, the encrypted unique MAC address string is exposed and would not change if the public key remains the same. To overcome this the AP would randomly update the key pair thus resulting in a differing encrypted unique MAC address string being sent.

Protocol Exchange to Obtain STA unique MAC address

The following is the proposed defined message exchange between an Access Point (AP) and a Wi-Fi device or station (STA) to enable the AP to obtain the unique MAC address of the STA. The STA unique MAC address is the MAC address that is assigned to the STA by the manufacture. This MAC address has been used in many AP functions and features. The various AP functions and features include but are not limited to access and deny list, parental controls, device prioritization, terms and conditions, and lawful intercept.

Protocol definition

By making use of the Service Information Request ANQP Element and the Service Information Response ANQP Element, a specific Service Information attribute can be defined. The AP would send the ANQP request containing the Service Information specific to request the unique MAC address of the STA. The ANQP request would be sent post association allowing the ANQP response containing the Service Information Response to be encrypted thus keeping the unique MAC Address of the STA protected from ease droppers.

The specific of the Service Information Request attribute is not defined as that attribute would have to be coordinated through an SDO such as IEEE. The Service Information Response attribute would be defined as the Service Information Response attribute that would also contain the unique MAC address of the device.

By the AP knowing the unique MAC address functions and features such as associated white-list and black-list devices could be developed. As well knowing the associated unique MAC to the random MAC would enable the AP to put traffic on specific VLAN and routing based on implementations within the AP.

An alternate to the Service Information elements, Vendor Specific element could be employed.

Protocol Exchange to Obtain STA unique MAC address by using unique key pairs

This is an additional method of obtaining the STA unique MAC address by using unique key pairs. While following the base of the original idea, this solution covers all network types (open, WPA2-P, WPA2-E, WPA3-P, and WPA3-E).

The query by the AP and return of the STA unique manufacture unique MAC address by the STA could be done pre-association, during association, or post-association. This would allow the request to happen using current gas messaging or defined message exchange. As with the original ideas, this would enable the AP to obtain the unique MAC address of the STA. The STA unique MAC address is the MAC address that is assigned to the STA by the manufacture. This MAC address has been used in many AP functions and features. The various AP functions and features include but are not limited to access and deny list, parental controls, device prioritization, terms and conditions, and lawful intercept.

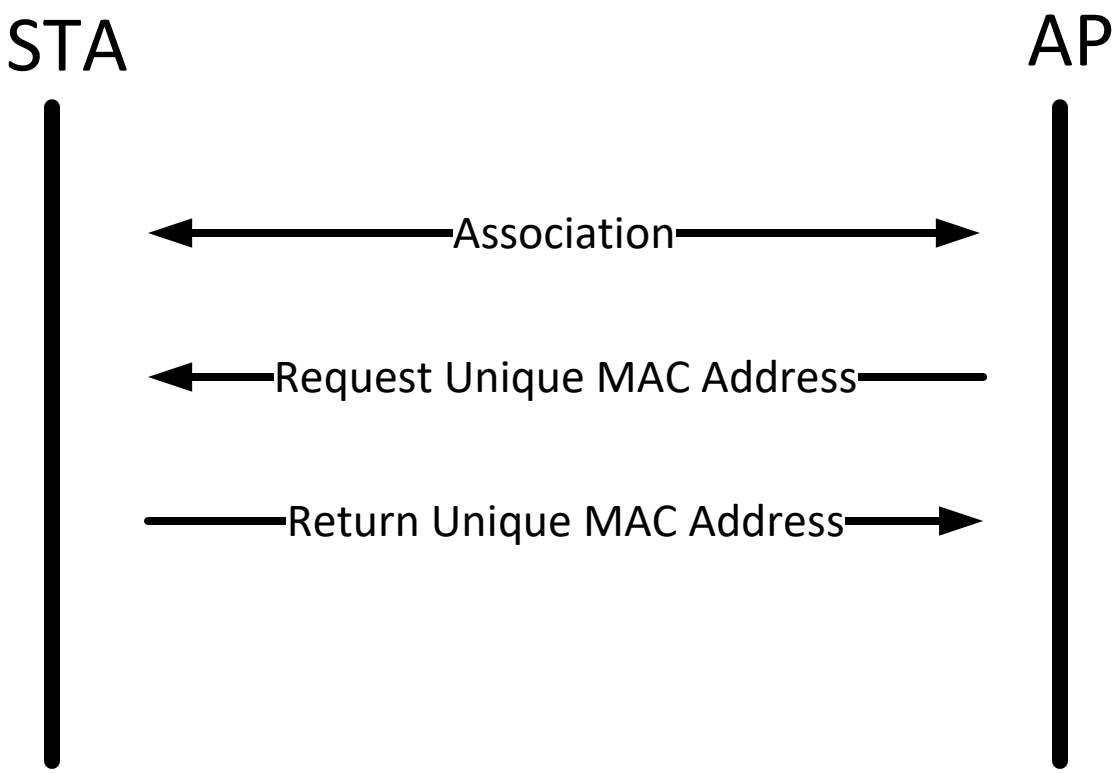
Protocol definition

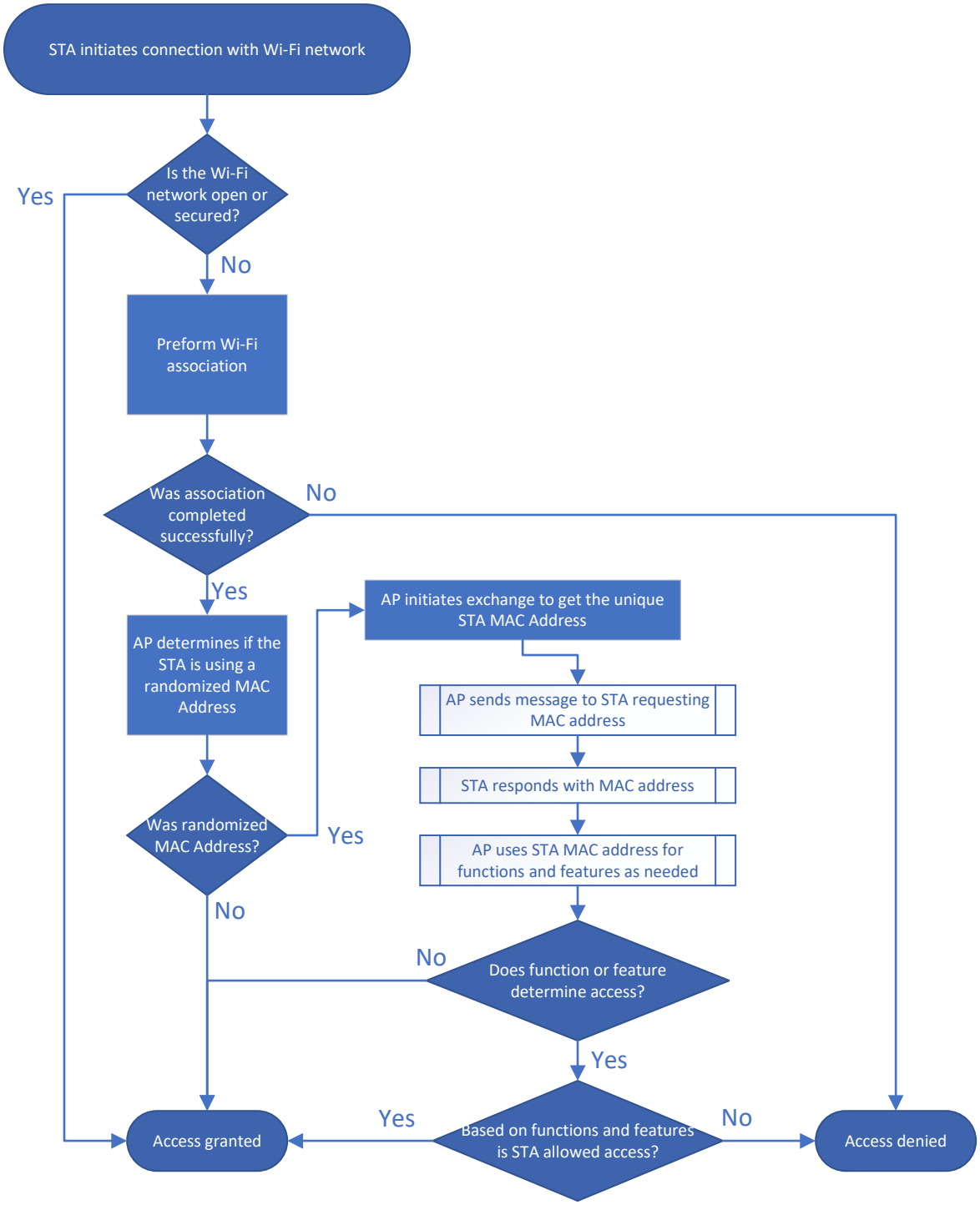
By making use of undefined fields in the current gas messages or in a new message type, the AP can request the STA to provide that STA's unique manufacture MAC address. Included in this message from the AP, the public key of an encryption certificate key pair is sent to the STA. The STA then encrypt the unique MAC address using the provided public key and returns the encrypted string to the AP. The AP then decrypts the proved encrypted STA unique MAC address with the private key of the encryption certificate key pair. This allows the AP access to the STA unique MAC address with out exposing the MAC address over the air (OTA) interface.

To farther ensure that tracking cannot be done through monitoring the RF (OTA) interface, the AP can randomly update the encryption certificate key pair. This results in different public keys used to encrypt the same unique MAC address making the encrypted string not static. This would create a randomness of the string not allowing tracking of the STA in any form.

By the AP knowing the unique MAC address functions and features such as associated white-list and black-list devices could be developed. As well knowing the associated unique MAC to the random MAC would enable the AP to put traffic on specific VLAN and routing based on implementations within the AP.

This can be shared and incorporated in future IEEE/WFA specification.


STA
AP
Association
Request Unique MAC Address
Return Unique MAC Address


STA initiates connection with Wi-Fi network
Is the Wi-Fi network open or secured?
Yes
No
Preform Wi-Fi association
Was association completed successfully?
No
Yes
AP determines if the STA is using a randomized MAC Address
Was randomized MAC Address?
Yes
No
AP initiates exchange to get the unique STA MAC Address
AP sends message to STA requesting MAC address
STA responds with MAC address
AP uses STA MAC address for functions and features as needed
Does function or feature determine access?
No
Yes
Based on functions and features is STA allowed access?
Yes
No
Access granted
Access denied