November 2022

LOCATION FINGERPRINT AS A FACTOR OF AUTHENTICATION OF ACCESS POINTS IN WIRELESS NETWORK DEPLOYMENTS

Niranjan M M

LOCATION FINGERPRINT AS A FACTOR OF AUTHENTICATION OF ACCESS POINTS IN WIRELESS NETWORK DEPLOYMENTS

AUTHOR:
Niranjan M M

ABSTRACT

Usage of Wi-Fi has gone to the next level with ever increase in the number of mobile devices, improved bandwidth and stability of Wireless LANs. There are many indoor and outdoor deployments using Wi-Fi in the form of wireless mesh networks. Administrators have little control on the APs installed in outdoor wireless mesh deployments. While AP authenticity is ensured by verifying its device certificate, but its physical location and safety is always big concern for Administrators. Being outdoor APs, they face always threats in the form of, getting stolen, misplacements, installation of rogue APs etc., Monitoring APs with the help of cameras or manually are very expensive solutions and may not be feasible in certain situations. As we know, once Access Points (APs) are deployed, they usually does not move. APs can use existing features (e.g., radio interface, NDP protocol, GPS etc.,) to detect their unique Location Fingerprint to identify with the physical location. Location Fingerprint is generated based on number of factors such as RRM neighbours, GPS co-ordinates, etc., The technique presented herein propose method, wherein APs periodically report their physical location information to the Network Management System, which generate Location Fingerprint from the collected location information of the AP and record the historical data of the Location Fingerprint of the APs. Whenever AP tries to re-join to the WLC, after completion of first factor authentication, second factor authentication is triggered, wherein WLC asks AP to provide the current location information. Upon receiving the location information from the AP, WLC forward it to the NMS. Further, NMS validate the location information of the AP with the pattern of historical data of the Location Fingerprint. If the pattern matches with the current location information of the AP, it is further allowed to proceed with the onboarding, otherwise, AP is rejected to join.

DETAILED DESCRIPTION

Usage of Wi-Fi has gone to the next level with ever increase in the number of mobile devices, improved bandwidth and stability of Wireless LANs. There are many indoor and outdoor deployments using Wi-Fi in the form of wireless mesh networks formed using hundreds or thousands of Access Points (APs). APs deployed in indoor/outdoor environment are identified as authentic by verifying the MIC (Manufacturer Installed Certificate). But in outdoor deployments, it is really difficult to monitor and control their physical presence in a given location, There is every chance that they can be stolen or moved to different location. It is always big concern to the administrator to verify not just the authenticity of the APs but also its physical location.

Administrators have little control on the APs installed in outdoor wireless mesh deployments. While AP authenticity is ensured by verifying its device certificate, but its physical location and safety is always big concern for Administrators. Being outdoor APs, they face always threats in the form of, getting stolen, misplacements, installation of rogue APs (these in-turn affect the end user experience) etc.,

Monitoring APs with the help of cameras or manually are very expensive solutions and may not be feasible in certain situations. Administrators looks for methods to check authenticity and physical location of the APs in a very cost effective manner especially in outdoor deployments. Hence there is every need for a method to identify an AP to be authentic and also validate the physical location where APs are deployed. Also, the method should not increase cost of the AP, but should improve safety requirements. Additionally, the method needs to be compatible with existing flows and functionalities. In short, Administrators wanted to have an in-built mechanism to validate its physical location along with the existing authentication mechanisms.

The technique presented herein propose a method to address this by enhancing the authenticity of the APs in an efficient and secure way. There are existing methods to provide Multi-Factor Authentication to improve authentication of the users/devices, but there are no efficient MFA aspects with respect to AP authentication and onboarding to the wireless network.

As we know, once Access Points (APs) are deployed, they usually does not move. APs can use existing features/components (e.g., Radio interface, Neighbour Discovery

Protocol, GPS etc.,) to detect their unique Location Fingerprint to identify with the physical location. Location Fingerprint is generated based on number of factors such as RRM neighbours which are identified using NDP protocol by deducing RF continuity space, GPS co-ordinates (if available) etc.,

As per this method, APs periodically report their physical (relative and/or absolute) location information to the Network Management System (NMS), which generate Location Fingerprint from the collected location information of the AP and record/store the historical data of the Location Fingerprint of the APs. Whenever AP tries to re-join to the WLC, after completion of first factor authentication (using certificate validation, or auth-token etc.,), second factor authentication is triggered, wherein WLC ask AP to provide the current location information. Upon receiving the location information from the AP, WLC forward it to the NMS. Further, NMS validate the location information of the AP with the pattern of historical data of the Location Fingerprint. If the pattern matches with the current location information of the AP, it is further allowed to proceed with the onboarding, otherwise, AP is rejected with reason "second factor authentication failure". Also, the WLC generate set of challenges for the AP to prove using request/response mechanism. The set of challenges generated are dynamic. Only if AP prove for the challenges by the WLC, then only AP is allowed to onboard to the network.

RF continuity space:

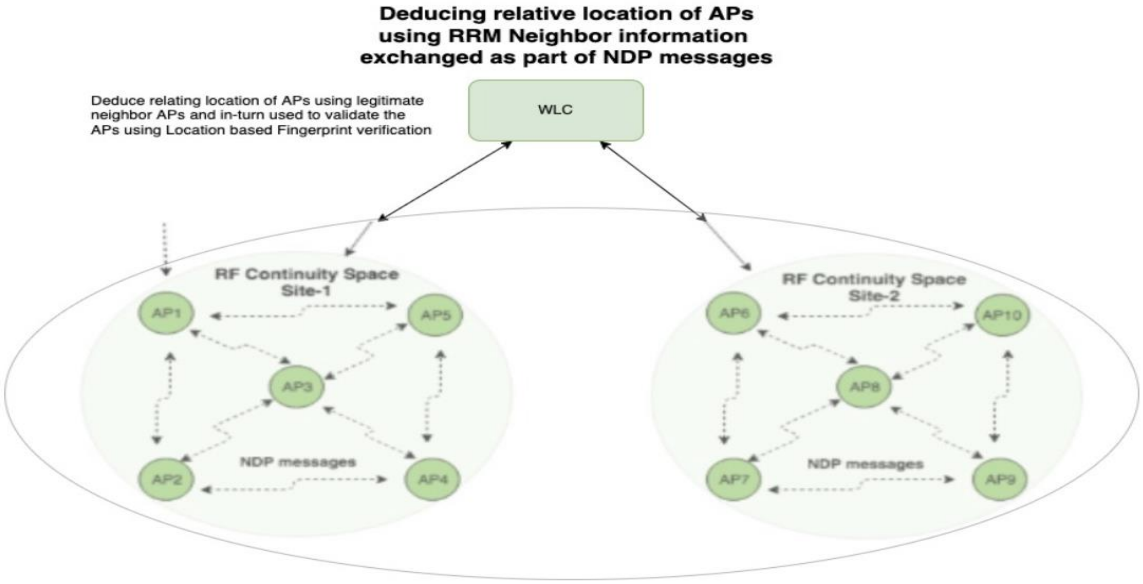

Figure-1

In the figure-1, AP1-AP5 are in one RF continuity space and joined to WLC, provisioned in Location (let us say, Site-1). And AP6-AP10 are in another RF continuity space and joined to WLC, provisioned in Location (let us say, Site-2).

RF continuity space is deduced from NDP messages (RRM neighbour information) exchanged between the APs. Deducing RF continuity space helps in identifying the relative location of the APs in the wireless network deployments, in-turn helps in generating Location Fingerprint of the APs. Also, to provide seamless handover (mobility/roaming), there will be radio signal overlap between the APs in the wireless deployment. This helps to generate Overlap Location Fingerprint of the APs in the deployment, which is very helpful in the pattern matching during AP re-join process. Both Location Fingerprint and Overlap Location Fingerprint are used to match with the pattern of the current AP location.

The technique presented herein is explained in detail as below. For simplicity, consider AP onboarding to the enterprise wireless networks but applicable to other wireless deployments/solutions, for example,

- Software Defined Wireless Mesh Networks (SDWMN), wherein AP are deployed on the outdoor public network and centralised SDN controller handles the AP onboarding.
- Private/Public cloud, wherein APs are deployed on the premises, but Wireless LAN controller (WLC) is deployed in the private/public cloud.
- Small and Medium Business (SMB) deployments, wherein APs are deployed in the shop/outlet/apartment etc. and the control plane software will be running on the cloud instance (this could be managed by vendor/company or managed by the customer).

This section is divided into multiple sub-sections, explained by considering different aspects of the proposed method.

A. Initial AP Join:

- When an AP tries to join to the WLC, certificate based authentication is done to validate the AP.

- After AP successfully join to the WLC, it periodically, collect and deduce the location information (i.e., RRM neighbours using NDP, GPS [if available]) and report it to the Network Management System (NMS).
- Upon receiving the location information of the AP, NMS generate Location Fingerprint (LF) and stores/record each Location Fingerprint data in its database. Further, NMS will extract the matrix to generate a pattern of the individual Location Fingerprint of the AP. This matrix is used later to match the location pattern send by the AP during re-joining, in particular, as part of second factor authentication.
- Similarly, all the APs update their location information to NMS, which makes NMS to have database of Location Fingerprint of all the APs in the deployment.
- Also, to provide seamless mobility/roaming, APs are deployed such a way that there will be overlapping space with the neighbouring AP. Hence there is a correlation matrix of Location Fingerprint between each AP in the deployment. NMS extracts the overlap of Location Fingerprint to generate a pattern of the "Overlap Location Fingerprint" between each AP.

B. AP Re-join:

- When the AP tries to re-join to the WLC, certificate based authentication is done to authenticate the AP. This is nothing but the first factor authentication.
    - If certificate validation fails, then WLC dis-join the AP.
    - If certificate validation is successful, then goes for the second factor authentication.
- As per the proposed method, do the second factor authentication as below:
    - WLC requests the AP to send the current (real-time) location information.
    - AP collect and deduce the location information using different methods such as
        - Using Neighbour Discovery Protocol (NDP) to detect the RRM neighbours and in-turn generate RF continuity space, which will give relative location of the AP.
        - Using GPS co-ordinates (if available), which will give absolute location of the AP.

- AP reports the location information gathered (RRM neighbours, GPS co-ordinates etc.,) to the WLC.
- In-turn WLC sends the location information of the AP to the Network Management System (NMS).
- When the NMS receives the location information of the AP, NMS uses different methods (e.g., RF continuity space, pattern recognition etc.,) to validate the location information received against the previously recorded/cached pattern of Location Fingerprint (on the NMS).
    - If location information does not match with the recorded pattern, NMS sends "second factor authentication failure" status to the WLC. Subsequently, WLC takes the action based on administrative policy (e.g., disjoin the AP, report the error of second factor authentication failure to the telemetry/network assurance server etc.,).
    - If location information match the recorded pattern, NMS sends "authentication success" to the WLC.
- Further, the WLC uses the neighbour AP information to create a set of challenges about the AP's physical location, then the WLC challenges AP to provide the requested information, for example:
    - WLC requests current AP (say AP1) whether it received the NDP (RRM information) messages from the neighbouring AP (say AP2). If AP1 can receive the signal of AP2, then WLC asks AP2 to send its neighbour information to WLC (it obviously have the information about the AP1). The information provided by the current AP and its neighbouring APs is used to validate the challenge response. Until the challenge is passed, second factor authentication is not successful. Note here, the challenge set is dynamic (i.e., WLC can ask one or more of the neighbouring APs to provide information about the current AP being onboarded).
    - In some cases, WLC may ask the previously reported good/working configuration to validate against the administrator configured values, to check whether AP configurations are modified or not.

- Once AP joins to the WLC, it periodically report location information to the NMS. Subsequently NMS generates the Location Fingerprint (in-turn populate matrix of patterns) using the location information provided by the AP.

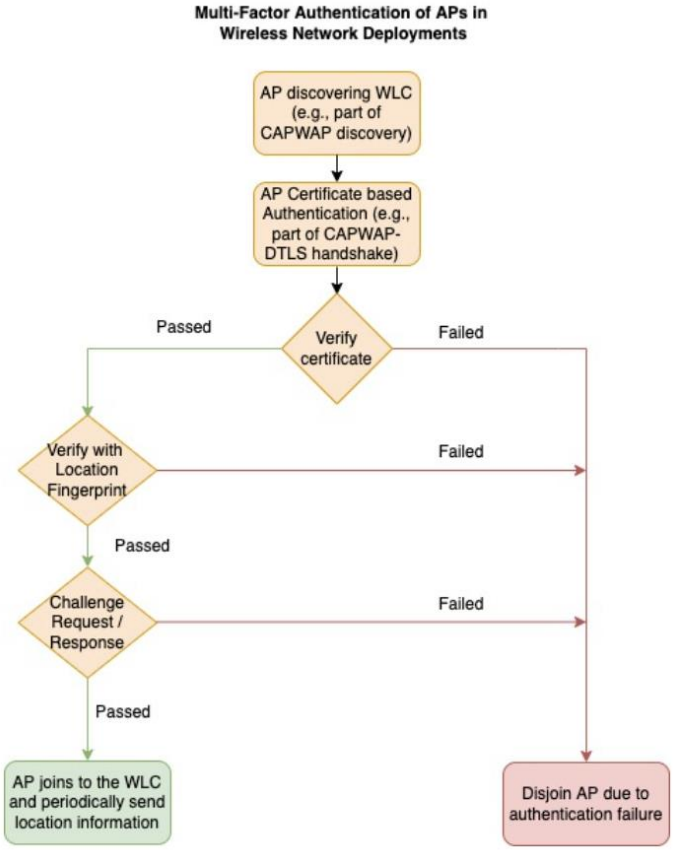

Figure-2

C. Population of Location Fingerprint and pattern generation:

Location Fingerprint includes environmental factors that can be detected by the APs.

- Neighbour information collected using Neighbour Discovery Protocol (NDP) to deduce the RRM neighbours and subsequently calculate the RF continuity space (which provides relative location of the AP in the deployment).
- The GPS co-ordinates, longitude and latitude (which provides absolute location of the AP).

- The location information of the AP deduced using above factors is updated to the NMS.
- NMS generate Location Fingerprint using the location information provided by the AP. Further NMS extract the matrix to generate a pattern of the Location Fingerprint of the AP.
- Also, every AP has an overlapping space with the neighbouring AP. Hence there is a correlation matrix of Location Fingerprint between each AP in the deployment. NMS extracts the overlap of Location Fingerprint to generate a pattern of the "Overlap Location Fingerprint" between each AP.

D. How to determine whether the Location Fingerprint and correlation matrix matches with the location information provided by the AP:

- Check whether the AP's location information matches the pattern of the Location Fingerprint matrix on the NMS. Let us say, hacker takes the legitimate AP from the original location and deploys it in other location. In this case, current AP location information does not match with the pattern of Location Fingerprint database on the NMS. Hence, second factor authentication fails.
- If above validation successful, then further check whether AP's Location Fingerprint matches the pattern of the Overlap Location Fingerprint. Let us say, hacker places the new APs near the AP being authenticated. In this case, let us say, Location Fingerprint pattern might match with the location information provided by the AP. But because of the number of APs increases in this area, the overlapping pattern of Location Fingerprint does not match with the overlap location information provided by the AP. NMS can traverse more patterns of the overlap location to find the suspicious APs added by the hacker.

E. Scenario where AP being Stolen by the Hacker:

- Let us say, somebody stolen the AP (which was connected to the SDN Cloud Controller) from the deployment especially from outdoor wireless mesh network and switched-on from the new location.

- Since it is legitimate AP (having valid SUDI certificate), first factor authentication succeeds.
- But as part of this proposed second factor authentication, SDN Cloud Controller requests AP to provide the current location information.
    - If AP running the genuine software, then it collects the location information using RRM neighbours (using NDP) and/or GPS etc., and send it to the Controller. Controller in-turn send to the NMS. Further, NMS validate the location information against the pattern of Location Fingerprint recorded earlier. Since currently AP re-joining from new location, new location pattern does not match with the Location Fingerprint on the NMS and hence second factor authentication fails.
    - Let us say, AP running the hacked software, then AP may not send the location information to the WLC. if second factor authentication is mandated by the network administrator, then AP will not be allowed to continue join to the WLC, unless second factor authentication is done.

F. Scenario where legitimate AP moved by the administrator to the new location:

- Let us say, network administrator want to move the AP from one location to the another.
- But if administrator changes the location of the AP, then proposed second factor authentication fails during re-join. Hence administrator need to clear the Location Fingerprint (or update the status as "Location Change") before changing the AP's location.
- Since Location Fingerprint information is cleared by the admin (and hence not available), initially AP re-join would happen without second factor authentication. Once it is joined from the new location, AP would periodically updates the new location information to the NMS through the WLC. Further, NMS populate Location Fingerprint records and generate the matrix for pattern matching later. Further, NMS populate correlation matrix of Location Fingerprint between each AP in the deployment.

G. Multi-Factor Authentication in different Wireless Network Deployments:

1. In Non-cluster Deployments:

The figure-3 depicts the proposed Multi-Factor Authentication in Wireless Network deployments (considering both Wireless Mesh Network and Enterprise Non-mesh Wireless Network). Here, RAPs (Root APs), MAPs (Mesh APs) and enterprise APs (Non-mesh APs) authenticate with the WLC using both first and second factor authentication before AP onboarding.

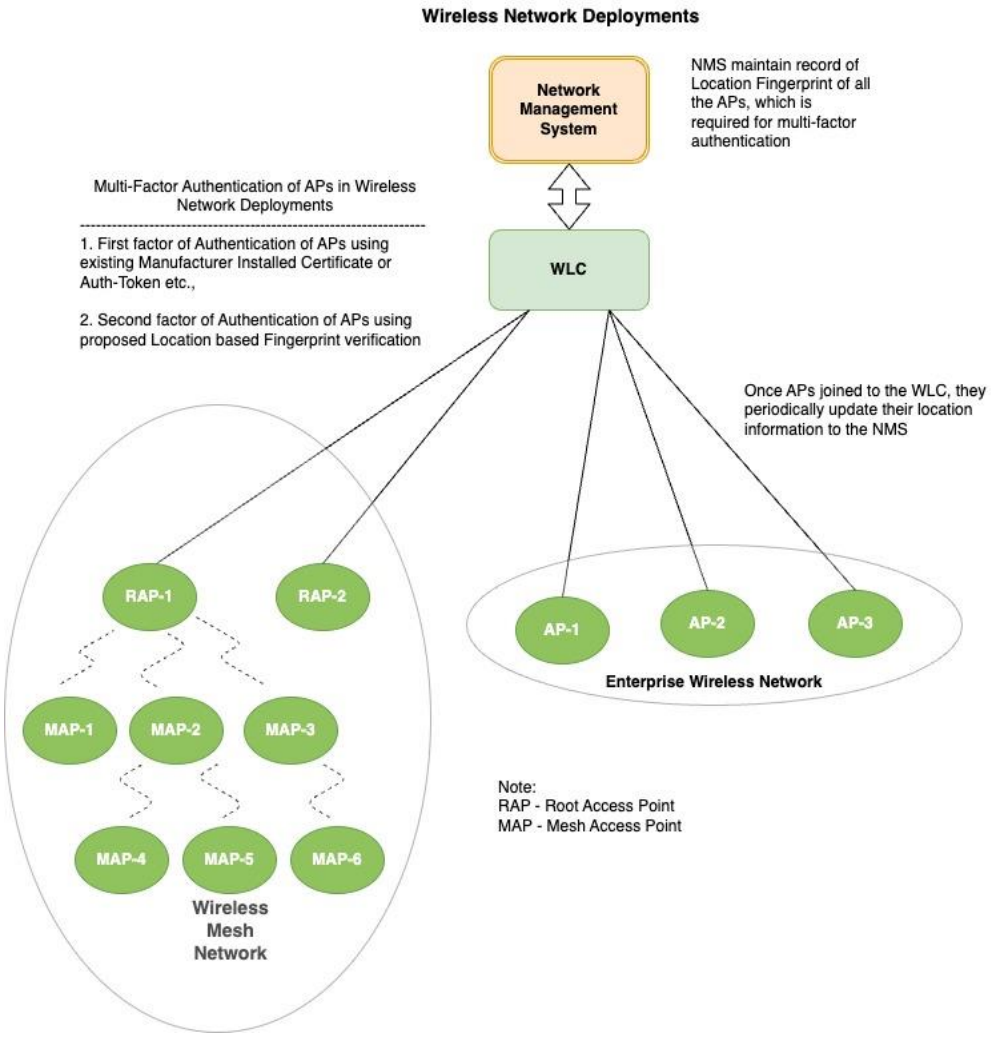

Figure-3

2. In Cluster Deployments:

The figure-4 depicts the proposed Multi-Factor Authentication in Wireless Network Cluster deployments (considering both Wireless Mesh Network and Enterprise Non-mesh Wireless Network). Here, WLCs form cluster where-in one of the WLC becomes Leader (Master) and all other WLCs becomes Workers (Members). Leader WLC control the whole cluster and in-turn it is managed by the Network Management System (NMS) , whereas Worker WLCs serve the APs and its clients connected to it. The above proposed method is applicable even for cluster deployment, where-in worked WLCs does initiate the second factor authentication with their APs.

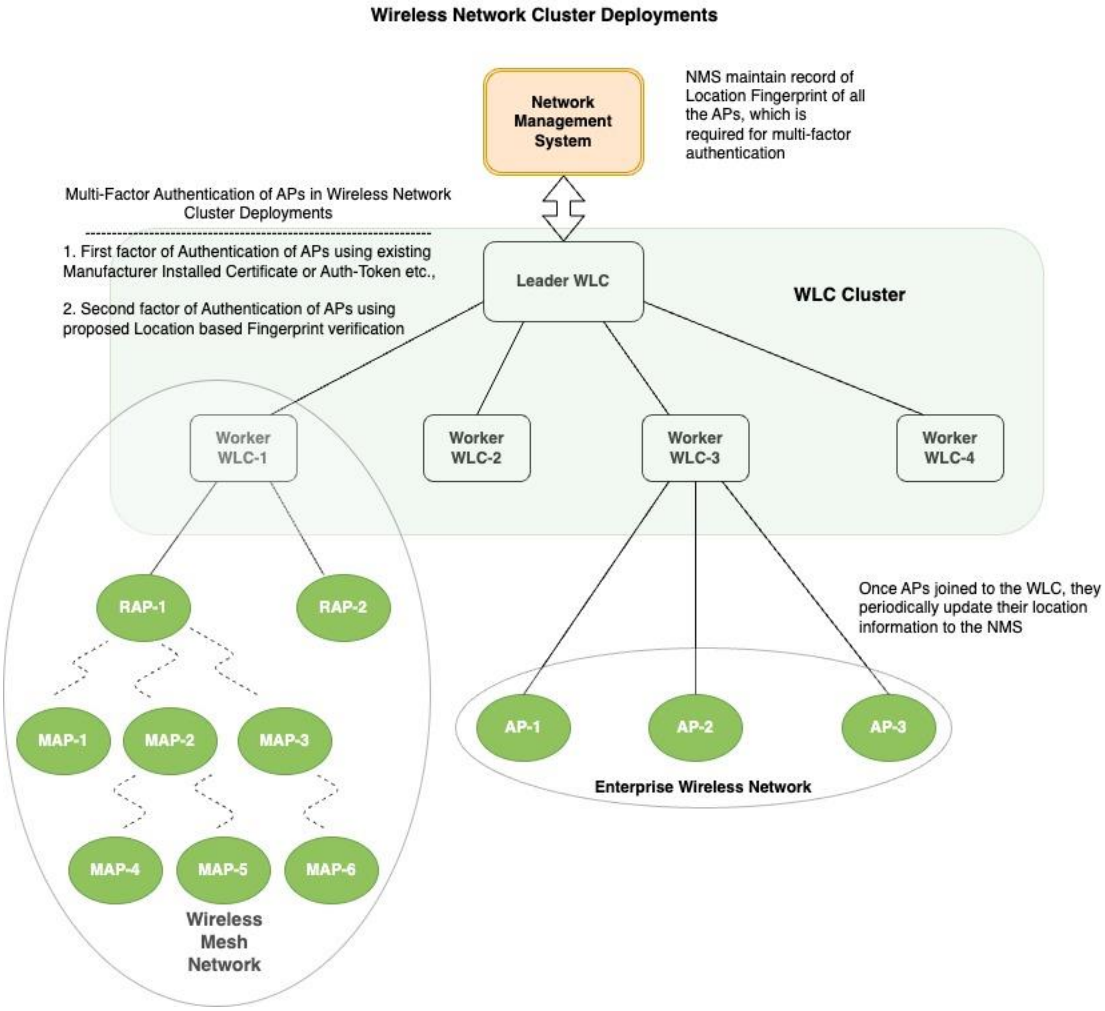

Figure-4

In summary, the techniques presented herein helps to improve AP authentication using MFA where-in Location Fingerprint is used as an identity. Additionally, this method helps to detect if any AP is stolen or misplaced. Moreover, this method very much required for the outdoor mesh deployments (i.e., APs are connected to Software Defined Wireless Mesh Controller), wherein providing physical security is utmost important.