Technical Disclosure Commons

Defensive Publications Series

November 08, 2018

Establishing a trusted federation of wireless access points

Jiwoong Lee

Jérôme Poichet

Establishing a trusted federation of wireless access points

ABSTRACT

A federation of wireless access points (APs) enables superior network connectivity when compared to a single wireless AP. This disclosure describes secure formation of an AP federation. An AP discovers the presence of a neighboring AP by detection of beacons and probe responses transmitted by the neighboring AP or by explicit transmission of a probe request. A known credential is presented by the AP to the neighboring AP to establish a connection and obtain an IP address. A federation service discovery message is transmitted specifying a port number and the IP address associated with the neighboring AP. A response message is transmitted by the neighboring AP that includes a base MAC address associated with the neighboring AP, a federation service IP address associated with the base MAC address, and the port number. Federation service discovery messages are exchanged between the APs that denote the access points as trusted members of the federation.

KEYWORDS

- Access point
- AP federation
- Wi-Fi
- 802.11
- Router
- Service discovery
- Probe response
- Beacon

BACKGROUND

Wireless access points (APs) are utilized to provide network coverage service to proximate user devices. In some scenarios, a group of cooperating APs, referred to as an AP federation, can provide superior network connectivity to user devices and can be utilized for multi-path routing, radio resource management, fast roaming with session caching, triangulation, providing location services, etc. A secure process for forming a federation of APs can enable secure transmission of sensitive data between the APs.

DESCRIPTION

This disclosure describes secure formation of access point (AP) federations. AP federations are groups of two or more APs that are physically proximate and configured as a single autonomous system to interoperably provide network access to user devices in their proximity.

Fig. 1 illustrates an example AP federation that includes access points, AP(X) (120) and AP(Y) (130). In a typical scenario, the access points belong to a local area network (LAN) under control of the same owner, and share a switch router (110) with the same network prefix. A common set of firewall rules govern the APs. An AP configured as member of a federation is reachable by at least one other member of the federation at a low physical layer (PHY) rate. The low PHY rate ensures an AP federation coverage area adequate to discover eligible APs while mitigating the risk of an attack originating from an AP that joins the federation from outside a specified area.

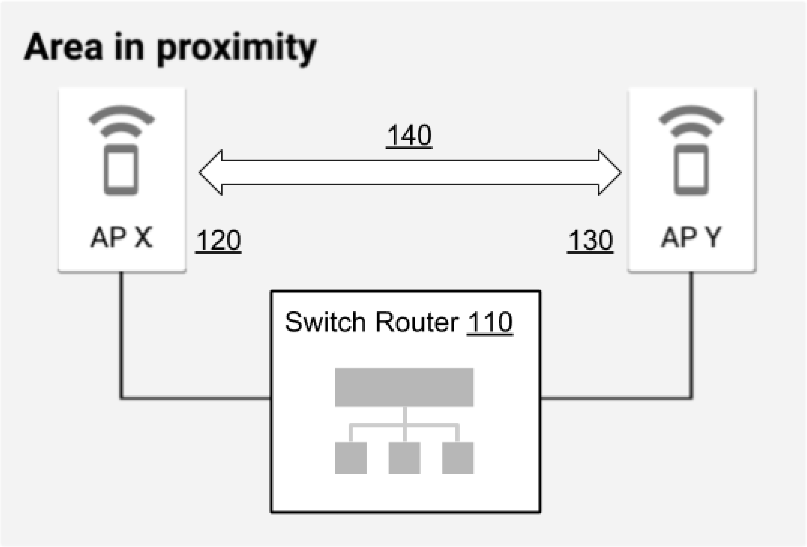

Fig. 1: Proximate APs are configured to form AP federation

APs that constitute the AP federation are provided with an identical extended basic service set identifier (ESSID). The common ESSID of the APs signals intention of the network operator to use the APs for shared and/or common use.

Fig. 2 illustrates an example mechanism by which a trusted federation of APs is formed. The federation formation process is an infrequently performed action, with relatively low impact on the networking service provided to the AP clients.

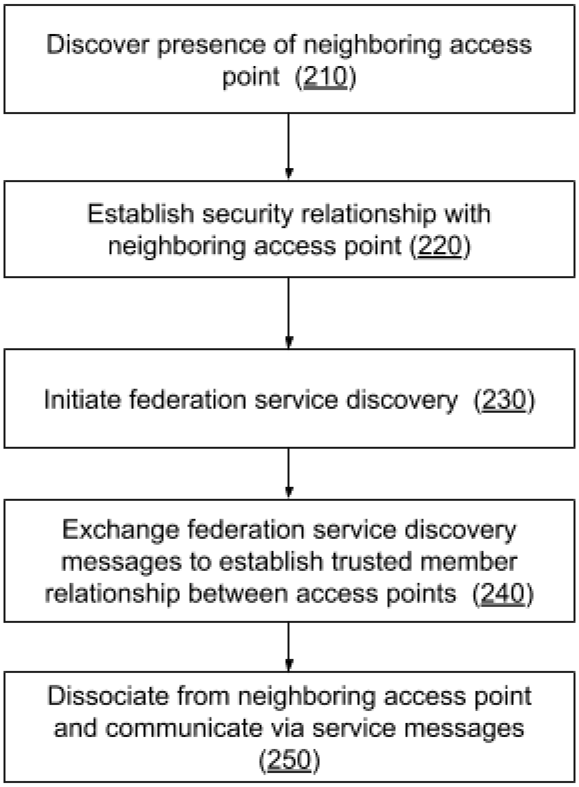
Discover presence of neighboring access point (210)
Establish security relationship with neighboring access point (220)
Initiate federation service discovery (230)
Exchange federation service discovery messages to establish trusted member relationship between access points (240)
Dissociate from neighboring access point and communicate via service messages (250)

Fig. 2: Process of AP federation formation

An access point, for example, AP (X), discovers (210) the presence of a neighboring AP, e.g., AP (Y), with a common ESSID either by monitoring on-channel or off-channel beacons and probe responses that are transmitted from the neighboring AP. The discovery of a neighboring AP can also occur via an explicit transmission of a probe request to the ESSID across sweepable channels. The timing, frequency, trigger events, etc. are configurable and extensible. The data frames associated with the beacons, probe responses, probe requests, etc., are generally transmitted at a lowest possible basic PHY rate, designed to reliably traverse a wide area, and are easily detectable in typical layouts of offices and houses. A detection range of 50m can be attained based on a maximum transmit power of a typical AP.

AP (X) then attempts to connect (220) as a client to neighbor AP(Y). A known credential, e.g., for example, a WPA2-PSK passphrase, four-way handshaking, etc., is presented by AP(s) to AP(Y) to verify if a secure over-the-air relationship can be established. Successful verification leads to AP(X) being connected to and obtaining an IP address from AP(Y).

A flexible timing option is provided for an AP to connect to a neighboring AP. The connection attempt to a neighboring AP is made preferably at times when there is no client device associated with the AP, when the AP is in power-saving mode, or when the AP has a relatively low traffic demand, etc.

Next, AP(X) initiates (230) a federation service discovery message specifying a port number, e.g., a remote procedure call port at AP(Y), and an IP address associated with AP(Y) as a destination IP address. If AP(Y) is configured such that it can participate in a federation, a response message is generated by AP(Y). The response message includes a base MAC address associated with the AP(Y) and hosted in the LAN, a federation service IP address associated with the base MAC address, and the port number. For example, the federation service IP address can be a unicast address, an IPv6 link local address, etc.

AP(X) and AP(Y) successfully exchange (240) federation service discovery messages that denote the access points as trusted members of the federation. The exchange of messages and the formation of the AP federation is completed by the APs (250). The access points disassociate, and return to their respective modes of functioning. An IP connection is established between AP(X) and AP(Y), and requests, response, notifications of service messages are transmitted and received by the APs via remote procedure calls.

In some implementations, an AP federation can be formed wherein a persistent IP connection or IP connectivity over a LAN connection is not maintained between the access points. In this scenario, subsequent to the formation of the AP federation, member APs periodically exchange information by synchronizing their respective operating frequencies and utilize Layer 2 or Layer 3 connectivity established between the APs. A configuration state of other APs in the federation is set analogous to that of power save clients, and an association between the APs is maintained. The APs that form the federation serve as access point to their respective clients, and in general, at different frequencies, but periodically revert to a common operational frequency in order to exchange information. A lowest possible modulation and coding scheme is utilized by the APs.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

A federation of wireless access points (AP) enables superior network connectivity to user devices when compared to a single wireless AP. This disclosure describes the secure formation of an AP federation. An AP discovers the presence of a neighboring AP by detection of beacons and probe responses transmitted by the neighboring AP or by explicit transmission of a probe request. A known credential is presented by the AP to the neighboring AP to establish a connection and obtain an IP address. A federation service discovery message is transmitted specifying a port number and the IP address associated with the neighboring AP. A response message is transmitted by the neighboring AP that includes a base MAC address associated with the neighboring AP, a federation service IP address associated with the base MAC address, and the port number. Federation service discovery messages are exchanged between the APs that denote the access points as trusted members of the federation.