JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Roaming and Its Optimization in WLAN's

[1]B Mohit Rao, [2]Deepika Dash
[1]Student, [2]Assisstant Professor
[1,2]Department of Computer Science and Engineering,
[1,2]RV College of Engineering, Bangalore, Karnataka

Abstract: -

In these modern times each and every organizations are adopting WLAN's to get internet connectivity throughout the workspace. Once a client enters a network it will do all the validations by providing the usernames and other authentications and will get connected to the network. Once any WLAN client device enters a particular area in this workplace and gets connected to any particular AP, the entire time even with its movement outside the AP's range. How is this possible? This is due to roaming in WLAN. This project aims to understand how does roaming happens in WLAN and how we can optimize roaming scenarios.

Index Terms: -

Access Point (AP), Wireless LAN(WLAN), beacons, probes, authentication.

I. Introduction: -

As discussed when a device enters the network and connects to a network, device starts moving into the network. What happens is the moment with positional movement one WLAN client goes to the threshold of the connected AP's range, instead of disconnecting altogether and reconnecting it gets connected to the same network but different AP. This is called as roaming.

Initial Connection Sequence: -

When a device enters into a network a scan is triggered to identify which all AP's are in vicinity of the device. This scan is of two types. Active and Passive Scans.

Active Scan – This is a process in which mobile/device will send a probe request specifying its requirements and broadcast it to the network. And the Aps that will acknowledge those requests will send their responses and further exchanges takes place to get connected to it.

Passive Scan – This is the process in which Aps will send some special frames called as beacon frames and device needs to continuously capture those frames to get connected to a particular AP. And after a particular AP's beacon is captured the whole process of initial connection establishment is similar to one what happens in Active Scan.

After the scanning is done and a particular AP is identified the device will send authentication frames, based on the Wi-Fi profiles. It can be either WPA, WPA2 or 802.1X. After the authentication is successful from both the sides, the device will send association frames specifying what all data rates it supports and request for the connection establishment with the AP. In response to that AP will send a association response and after this frame is received the device finally gets connected to the AP.

II. Current Technology: -

Now after the device is connected to a particular AP it starts to roam. The device observes that there is decrease in the signal strength as it moves farther from the AP and sees that there is another AP which has more signal strength as compared to the current AP. At this point rather then full disconnection and reconnection to the new AP the device directly switches and connected back the new AP after performing necessary packet exchanges.

Wireless client roaming optimizes this transition between the Aps in order to avoid disruptions and delays. This is accompanied by using fast roaming session caching which avoids some of the authentication steps. Some of the techniques which are used in such scenarios are PMKID Caching and OKC.

There are various 802.11 standard improvements over the years which enhances the speed of data transfers as well as the distance up to which a proper signal strength can be achieved. Some of them are 802.11 a/b/g/ac/ax. 802.11 ac and ax are based on the type of frequency band channel offered by them (i.e. 2.4 GHz and 5 GHz).

III. Shortcoming in Current Technology

To understand what are the limitations to the current model let's take some use cases which will help in understanding the problem better.

For roaming we have to do certain packet exchanges between the client and the AP (based on 802.11 protocols) also mentioned above. But imagine there are multiple APs in the vicinity and the entire exchange for deciding a particular AP as the right candidate the client has to repeat the steps for all the APs. Imagine the device decides a new AP as the right candidate for WLAN roaming and moves along. After a while after few more roaming it again comes to back to the same location where it previously did all the packet exchanges just to verify which is the right candidate. Then again it will spend some more time to re-do all the work previously it did, wasting power as well time to select the right candidate.

Consider another situation where in we have been connected to an AP after a longer process of scanning and exchanging the packets for connection setup. The device is connected to the AP but after connection it is observed that AP is not responding properly. For e.g., it has suddenly sent a DE- authentication or a disassociation frame i.e. it wants to disconnect from a particular device. OR there has been a delay in sending a data frame or no acknowledge from the AP side. First time the device is connected to this AP and then it would have suffered with above problems mentioned. But if the device roams and then if it come back to the same AP then will perform all steps again for reconnection then device will suffer again the same issues which it had seen before.

With above use cases we need to come up with some strategy which will be able to resolve such cases so that smooth roaming is possible.

IV. Proposed Solution: -

With the current technology we are deciding the best candidate AP for roam in based only on the current scenario. But now to improve and optimize the decision of selecting an AP for the next roam would be to consider previous history also for decision making. When the device roams for the first time we should store the sequence of APs which device has connected to during its initial roam. So, when it tries to roam in same scenario again we can go and search in the historic sequence and identify in that case which ap was selected by the device for connection. This will allow to filter our scan i.e. we would know from historic sequence which channel was selected and the scanning can be done only on that particular channel thus reducing the battery consumption, CPU overhead etc.

Along with storing sequence of AP of roam if we store the behavior of AP when it is connected to a device like for long packet exchange take place, if there is a sudden disconnection or not, AP is able to acknowledge the requests made by the device or not. If such information is stored then we can identify the rogue Aps and when such Aps comes in front of the device during scan the device can ignore those Aps because they would not give proper connectivity based on the previous history (such conclusion can be made).

In this way to some extent the scanning can be optimized and proper candidate AP for next roam can be selected.

V. Future Work: -

This is kind of system which is proposed in this project is yet to be implemented. As the idea is to store a sequence we need to have some storage that can be used and easily implemented so that the searching of a particular roam sequence would be easier and extraction of information is flexible considering both space and time complexity. The idea for further improvement would be to create a machine learning model which could be trained for such roaming scenarios so that the machine only could help in selecting the right candidate AP for the next connection.

References

[1] C. Yap, "Issues with real-time streaming applications roaming in QoS-based secure IEEE 802.11 WLANs," in Proceeding of the 2nd international conference on Mobile Technology, Applications and systems, 2005.

[2] R. Chakravorty, P. Vidales, K. Subramanian, I. Pratt, and J. Crowcroft, “Performance issues with vertical handovers—experiences from GPRS cellular and WLAN hot-spots integration,” in Proceedings of the 2nd IEEE International Conference on Pervasive Computing and Communications (PerCom '04), pp. 155–164, March 2004.

[3] J. S. Stach, E. K. Park and Z. Su, "An Enhanced Authentication Protocol for Personal Communication Systems", IEEE Wksp. App.-Specific Software Eng. Tech., pp. 128-132, 1999.

[4] C. S. Loredo and S. W. deGrimaldo, Wireless LANs: Global Trends in the Workplace and Public *Domain*, 2002.