2-2020

Channel Scanning and Access Point Selection Mechanisms for 802.11 Handoff: A Survey

Dhananjay Singh

Santa Clara University

Department of Computer Engineering

Date: February 26, 2020

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Dhananjay Singh

ENTITLED

Channel Scanning and Access Point Selection Mechanisms for 802.11 Handoff: A Survey

BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN COMPUTER SCIENCE AND ENGINEERING

B. Dezfouli

Thesis Advisor
Dr. Behnam Dezfouli

Thesis Reader
Dr. Silvia Figueira

for Nam Ling

Chairman of Department
Dr. Nam Ling

Channel Scanning and Access Point Selection Mechanisms for 802.11 Handoff: A Survey

By

Dhananjay Singh

Dissertation

Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Computer Engineering
in the School of Engineering at
Santa Clara University, 2020

Santa Clara, California

Acknowledgments

I would like to thank my advisor Dr. Behnam Dezfouli for all his help and support over the last 3 years. Your heartfelt guidance and invaluable advice have greatly helped during my career at Santa Clara University. Your beliefs have inspired me to think uniquely on both personal and professional levels. Without your support, this thesis would not have been possible and I shall eternally be grateful to you for the assistance. The hands-on experiences gained on IoT devices have greatly helped me enhance my system and networking skills and this will be a huge turning point for the rest of my career.

I have great pleasure in acknowledging my gratitude for my fellow Ph.D. researchers, Jay Sheth and Puneet Kumar, for providing valuable advice and assisting me with technical issues in the lab. I enjoyed the guidance and brainstorming sessions with both of you and greatly appreciate for being there at all times when I required motivation and propelling me during the thesis work.

My acknowledgment would be incomplete without thanking my biggest strength: my family. The blessings of my parents Mr. S. P. Singh & Late Mrs. Shanti Devi and all the love and care of my brother, Mrityunjay, has been my greatest strength during difficult times. Unfortunately, I lost my mother last year but her positive thinking and insatiable desire to achieve big has always inspired me. Had it not been her unflinching insistence and support, my dreams of excelling in higher education would have remained mere dreams.

Finally, I would like to thank all my SCU friends and professors for always making sure that good times keep flowing. I would like to express my special gratitude to Professor Farokh Eskafi and Dr. Keyvan Moataghed, for being extremely supportive and helpful, and making me become a better learner.

Channel Scanning and Access Point Selection Mechanisms for 802.11 Handoff: A Survey

Dhananjay Singh

Department of Computer Engineering
Santa Clara University
Santa Clara, California
2020

ABSTRACT

While the cellular technology has been evolving continuously in recent years and client handoffs remain unnoticed, the 802.11 networks still impose an enormous latency issue once the client device decides to roam between the Access Point (AP). This latency is caused by many factors reckoning on scanning the channels and searching for APs with better signal strength. Once data from all the nearby APs has been collected, the client picks the most suitable AP and tries to connect with it. The AP verifies if it has enough capability to serve the client. It also ensures that the client has the required parameters and supported rates to match with the AP. The AP then processes this request, generates a new Association ID and sends it back to the client, thereby granting access to connect. Throughout this re-association process, the client fails to receive or send any data frames and experiences a lag between leaving the old and associating with a new AP. Originally, 802.11 authentication frames were designed for Wired Equivalent Privacy protocol, but later it was found to be insecure and thus got depreciated. Keeping these security aspects concerning shared key authentication in mind, few additional drafts were introduced by IEEE that concerned many key exchanges between the devices.

IEEE 802.11r was introduced in 2008 that permits wireless clients to perform faster handoff along with additional data security standards. The key exchange method was redefined and also the new security negotiation protocol started serving wireless devices with a better approach. This enables a client to set up the Quality of Service state and security on an alternative AP before making a transition which ends up in minimal connectivity losses. Although this was an excellent step towards minimizing the service disruption and channel scanning, failure to remain connected with consecutive suitable APs within the minimum time continued to be a challenge. Different manufacturers use their custom-built methodology of handling a client handoff and hence the latency costs differ based on the type of handoff scheme deployed on the device.

This thesis focuses on the foremost economical researches throughout recent years which targets minimizing the delays involved with channel scanning and AP selection. A wide sort of enhancements, whether it is on a client device or the AP, has been discussed and compared. Some modifications are associated with enhancing channel scan period or using beacons, and probe requests/responses in an efficient manner. Others concentrate on modifying the device hardware configuration and switching between Network Interfaces. Central controllers are a solution to handoff delays that may track the status of each device within the network and guide them to provide the appropriate Quality of Service to the end-users.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
EAP	Extensible Authentication Protocol
WEP	Wired Equivalent Privacy
SDN	Software-Defined Networking
FT	Fast BSS Transition
MAC	Media Access Control
BSS	Basic Service Set
QoS	Quality of Service
AC	Access Controller
WTP	Wireless Termination Point
PMK	Pairwise Master Key
DS	Distribution System
AP	Access Point
ESS	Enhanced Service Set
RSSI	Received Signal Strength Indicator
PTK	Pairwise Transient Key
MDIE	Mobility Domain Information Element
FTIE	Fast BSS Transistion Information Element
RSN	Robust Secure Network

NS3	Network Simulation 3
WNIC	Wireless Network Interface Card
ARP	Address Resolution Protocol
PM	Power Management
RTS	Request to Send
CTS	Clear to Send
TKIP	Temporal Key Integrity Protocol
RC4	Rivest Cipher 4
AID	Association ID
CRC	Cyclic Redundancy Check
MIC	Message Integrity Code
CCA	Clear Channel Assessment

Chapter 1

Introduction

The communications industry has changed significantly in the past few decades. The way people communicate every day has changed and so is their lifestyle. Nowadays, people rely more on seamless network connectivity and a higher Quality of Service (QoS) is expected from Voice over Internet Protocol (VoIP) services and video streaming. Since the emergence of 802.11 networks, we have been able to utilize them for almost every need when it comes to personal or business applications. The demands from the user's point of view are rising at a fast pace and existing technologies are starting to lag in terms of latency when compared to the services provided by cellular networks. Real-time applications now need seamless network connectivity to provide non-disruptive experiences to users.

Wireless Local Area Network (WLAN) provides support to a variety of users depending on their hardware configuration and data transfer capabilities. The popularity of WLAN is predominantly because of its convenience to use. It allows easy access to network users within their local environment whether at office or home. Nowadays, users are also able to access these networks at popular public spots like coffee shops, banks, and airports. This allows users to be more productive irrespective of the location and they can conveniently move from place to place.

A wireless network connection primarily consists of two components: an AP and stations. The location of an AP is fixed, whereas a client has the flexibility to change its position. For a client to successfully connect to an AP, a series of steps must be completed. These include channel scanning and AP discovery, authentication and association processes.

The channel scanning and discovery phase is the process of selecting an AP which can provide a reliable connection. This is performed either using beacons or probe requests and responses. During the authentication process, the client sends out an authentication frame to the AP and tries to establish its identity with the AP. This frame is acknowledged and responded with another frame which signifies either success or failure. Due to the broadcast nature of WLAN connections and the lack of physical links, the vulnerability issues have been an important topic since the emergence of WLAN. As a result, authentication algorithms utilized during the authentication phase has changed over the years.

The earliest version of the authentication algorithm used in WLAN is called Wired Equivalent Privacy (WEP). The primary objective was to provide at least the same security level as in wired networks, hence the name justifies. As time passed, more attackers were able to crack the encryption level on the data being transmitted. This forced cryptographers to discover the weaknesses of this algorithm and come up with a more secure one. As a result, IEEE introduced a newer version of the security infrastructure. This is described as an extension of the 802.11 standards and is called 802.11i. However, the switch from the WEP protocol to the 802.11i standard is not an easy task, as the complete hardware has to be changed. 802.11i has been very successful by not only providing a more secure communication but also supporting backward compatibility for the WEP based hardware which are used to date in many systems. The WEP-supported version is called Wi-Fi Protected Access (WPA) whereas the newer protocol defined in 802.11i is called Wi-Fi Protected Access 2 (WPA2).

For centralized networks or networks configured with 802.1X standard, WPA2 uses Extensible Authentication Protocol (EAP) frames to provide uniform access control throughout the network. 802.1X standard was designed to strengthen the security of WLANs which follows 802.11 standards. EAP is an extension of the data security feature of Point-to-Point Protocol and offers public key encryption authentication, one-time passwords and tokens to securely exchange data between the client and the authenticator using a 4-way handshake. This handshake requires multiple key exchanges every time a client attempts to roam but at the same time, it delays the process of reassociation for the clients.

Once the client has completed the authentication phase, it proceeds with sending association request frames to the AP. The request is either granted or denied based on the client's capabilities and other parameters that were sent within the association frame. The AP also checks if it has enough capacity to serve the client depending on the number of already connected clients. When the request has been granted, an Association ID (AID) is sent back to the client along with the association response.

The problem of unnecessary active scanning heavily impacts network performance. It can be analyzed from different perspectives. On the client-side, it induces latency while searching for an AP using probe requests and probe responses. On the other hand, this probe traffic causes more packet collisions and results in degraded network performance. The traffic consumes airtime and affects even those clients within the network which are not involved in active scanning. Another major challenge is the limited power source on the client devices. When a client is roaming frequently between the APs, the energy consumption during the scanning phase and next AP selection is more than what is being used to exchange the actual data packets. Furthermore, networks configured with 802.1X require additional key exchanges during the 4-way handshake, which adds to the overall roaming latency.

To overcome these challenges, the existing solutions can be divided into three major categories: client modification, network planning, and AP configuration. Client modification involves adding a control interface that can sense the environment parallelly during data exchange. Network planning includes modifying the channel scanning timers which have the flexibility to be configured to skip the unnecessary waiting period after the AP discovery on the channel. It also incorporates periodic scheduling of beacons and probe responses that enables a client to actively perform additional tasks in addition to exchanging data with the current AP. To minimize the computation done by the client while scanning, the APs can actively gather localization information of the client and determine the next best AP. This functionality can be utilized by configuring the APs in the network. The localization mechanism can also store the information of active channels on every AP which helps in resolving whether the closest AP has enough capacity to serve an additional client. For networks with centralized authentication servers, a cache of EAP exchange keys can be stored on the devices. The mobility domain defined in 802.11r immensely helps in resource reservation for a client in advance and reduces latencies during client roaming. It can also be formulated that the Distribution System (DS) can monitor channel load on the APs which can be utilized to maneuver the clients with delay-sensitive applications to lightly-loaded APs within the same mobility domain.

In this thesis, we have discussed how different mechanisms can be utilized to minimize channel scanning time, which contributes up to 90% of the total handoff latency. Some of these mechanisms focus on dedicating the scanning job to additional network interfaces and set to operate on an exclusively reserved channel. A few others introduce algorithms that can shortlist the best APs in the vicinity and skip the scanning process on all channels. It can be observed that the time spent on each channel can be significantly reduced by configuring the MinChannelTime and MaxChannelTime. Results show that these mechanisms can help to reduce the overall latency from 400ms to 70ms. Few caching algorithms further bring down this value under 10ms. These values vary depending on the number of channels, the band used, and the device manufacturer. We have also presented the operation of 802.11r or Fast BSS Transition (FT) and how context transfers can further improve client handoffs across multiple mobility domains within a centralized WLAN architecture.

The rest of this thesis is organized as follows: Chapter 2 presents the discovery phase and channel scanning in detail. Association steps and frame details have been summarized. Followed by this, the operation of WEP, design flaws and authentication algorithms involved have been discussed. The advantages of 802.11i, which can be viewed as the superseder of WEP, have been delineated in this chapter. It also explains the cryptographic keys derived in 802.11i and EAP 4-way handshake.

Chapter 3 discusses various mechanisms that tend to minimize the overall channel scanning time while a client is searching for a new AP. These include adding an extra wireless interface on the client or AP that can proactively search for nearby APs in advance, making a priority channel list and figuring out the active channels on APs in its proximity. The moving information of the client combined with a set of closest APs helps in sending selective probe requests instead of broadcasting it to all the APs, which has been discussed in this chapter in detail.

Chapter 4 focusses on APs and central controllers which assist the clients in making handoffs whenever necessary. Several neighbor caching algorithms have also been reviewed that generate a neighborhood report and perform client authentication beforehand based on prediction. Localization veracity plays an imperative role in making these decisions. It consolidates the existing 802.11r mechanisms with centralized Software-Defined Networking (SDN) architecture. Roaming across multiple mobility domains and cluster transitions for a client moving out of range have also been discussed.

Chapter 2

802.11 Operational State Machine

With the increasing number of mobile clients, 802.11 wireless networks have now become one of the most popular access networks. These networks provide portability to moving clients and allows them to easily roam between the APs. A client device follows a series of steps to get (re)associated with an AP, which are termed as state machines. These steps are followed either when the client is joining a network for the first time, or when it is trying to roam to another AP with better signal strength in the neighborhood.

2.1 Discovery and Channel Scanning

The discovery process is initiated either by implementing a passive or active scan. During the passive scanning mode, the client listens for beacon frames from the AP. This frame incorporates the Basic Service Set (BSS) ID which is the Media Access Control (MAC) address of the radio interface present on the AP. These beacons are transmitted periodically by the AP and sent every 100ms by default.

An active scan is initiated by a client requesting to join a wireless network. The client visits each of the channels in turn and sends out a probe request frame on the broadcast address. The IEEE 802.11 standard defines two timers, namely MinChannelTime and MaxChannelTime, which describe the duration for which a client needs to wait on a particular channel. The MinChannelTime defines the maximum duration a client waits for the first probe response after sending out a probe request. If no responses are received during this period, the client assumes that this channel is empty and moves onto the next channel. When it has received any response, it waits till the expiry of MaxChannelTime for any additional responses from other APs. Once MaxChannelTime is over, all the collected responses are analyzed and the client decides which AP to associate with, based on Received Signal Strength Indicator (RSSI) values.

2.2 Authentication Protocols

For a secure data transfer between an AP and client, and to verify the authenticity of either of them, authentication provides several security protocols. WEP was the first standard implemented by 802.11 wireless networks. However, several design flaws and associated vulnerability risks resulted in the development of a new standard, which is 802.11i.

2.2.1 Operation of WEP and its Design Flaws

There are two basic security issues in WLANs. First, the transmissions can be easily eavesdropped due to the wireless mode of communication. Second, any device can illegitimately try to gain access to the network because there are no direct physical links to the AP. WEP solves these problems by using cryptographic algorithms to encrypt messages and mandating the authentication for mobile clients before allowing them access to the network.

The authentication of a client is based on a challenge-based protocol, involving four messages. The client first sends a request to the AP to authenticate itself. In return, the AP generates a random challenge text and sends it back to the client. Followed by this, the client encrypts this text using a secret key which is known only to the client and the AP. This encrypted message is again sent to the AP. Upon receiving this message, the AP decrypts it using the same secret key and compares it with the original challenge text. If it matches, it is concluded that the response was generated by the client only (since no other device has the same key) and hence, the client is authenticated. Otherwise, the authentication step fails. The authentication result is then sent back to the client.

Once the client has been authenticated, it starts communicating with the AP using the same secret key which was used during the authentication process. The encryption algorithm utilized in the operation of WEP is the Rivest Cipher 4 (RC4) stream cipher. Stream ciphers generate a pseudo-random byte sequence using a secret seed. This random sequence is XORed to the original clear message byte-by-byte and forms the encrypted message. The sender (AP or client) uses the same process in the WEP operation. The original text (M) is XORed with a random sequence (S) to form the encrypted text ($M \wedge S$). On the receiver end, this message is again XORed with the same random sequence (S) to extract the original text, $(M \wedge S) \wedge S = M$. In fact, these XOR operations are so simple that it allows attackers to eavesdrop on an ongoing communication without much difficulty. By XORing two different encrypted messages together, the attacker gets the combined form of both the clear texts ($(M1 \wedge S) \wedge (M2 \wedge S) = M1 \wedge M2$). To overcome this problem, WEP appends an initialization vector parameter to the secret key. This parameter changes for every message and it ensures that a different pseudo-random sequence is being generated by the RC4 algorithm for every message.

Figure 2.1 shows that prior to encrypting the clear text, the sender attaches an Integrity Check Value to the cleartext. The primary purpose of introducing this value is to provide a mechanism for the receiver to verify the authenticity of the message and to detect any modifications by the attacker. In the case of WEP standard, this Integrity

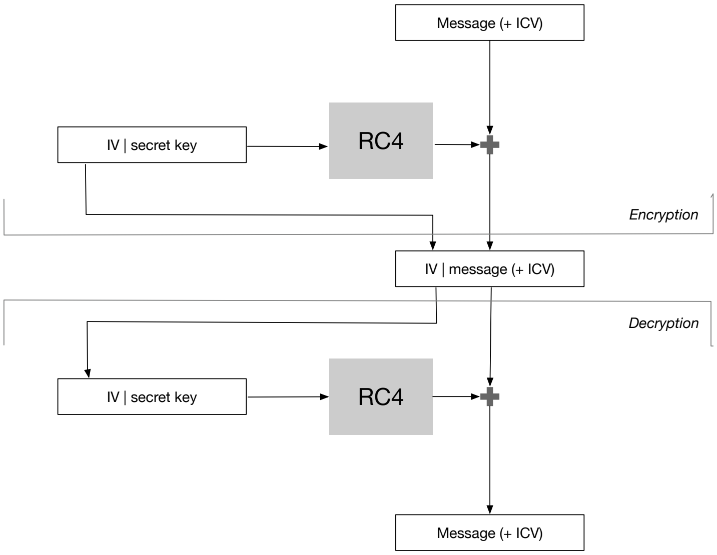

Figure 2.1: Encryption and decryption in WEP [1]

Check Value is the Cyclic Redundancy Check (CRC) value calculated for the cleartext. This CRC value is also encrypted along with clear text since the attacker can modify the clear text and append the new CRC value if sent without encryption. Now, to decrypt the CRC value, the attacker just needs to know the secret key. This solution can secure the network from outside attackers, but it is still prone to internal attacks since the default key implemented in WEP is common to every client and AP in the network.

The design of WEP was proved to have several security flaws. First, the same secret is used for both authentication and encryption mechanisms. This gives the attacker a chance to exploit the weaknesses of authentication and encryption to obtain the secret key. Second, the authentication process is not mutual. This means that the AP never used to authenticate itself to the client. The third problem is that the client is only authenticated once when it is trying to gain access to the network. Since the sessions are not managed by the AP, the encrypted messages recorded earlier from another client can be used by the attacker to fabricate the messages in the name of the current client. This is also known as a replay attack. The fourth problem is the use of a weak key in the encryption algorithm. The output after using such keys does not look random at all and can be easily inferred from the few initial bits. Also, the secret key can be easily cracked by eavesdropping a few million messages [9].

2.2.2 802.11i Architecture

To overcome the security flaws associated with WEP, the 802.11i specification introduced a new concept called Robust Secure Network (RSN). It was designed with better security features and newer methods for authentication and access control, which is based on 802.1X standards. The cipher used by RSN is Advanced Encryption Standard which provides better integrity protection than RC4.

However, the shift from WEP to RSN required much more than a firmware upgrade for the existing devices. It also requires hardware modification for the deployment of RSN. The developers of the 802.11i protocol were quite aware of these issues and hence introduced Temporal Key Integrity Protocol (TKIP) which still uses RC4, but fixes WEP security flaws. This allowed manufacturers to adopt TKIP without changing the hardware, and this specification is termed as WPA. WPA can be described as a subset of RSN which can be run on old devices that support only the RC4 cipher. The Advanced Encryption Standard supported devices implemented RSN and this specification is termed as WPA2.

Authentication and Access Control

The authorization in 802.11i is an enhanced version of 802.1X standards which was originally designed for wired networks. The 802.1X model has three major components required for carrying out the authentication process: supplicant, authenticator, and authentication server. The supplicant requests to join the network whereas the authenticator provides access to the network. The data traffic is disabled by default and hence initially the port is in a closed state. The supplicant sends authentication requests to the authentication server, and upon successful authentication, the server directs the authenticator to open the port. This results in granting network access to the supplicant.

In the case of centralized authentication servers, 802.11i utilizes EAP to carry messages which need to be transferred between the client and the authentication server. EAP consists of four types of messages: request, response, success, and failure. The EAP request and response messages facilitate the transfer of authentication data. The AP (authenticator) acts as a handoff agent for transferring the messages through it without any interpretation and understands either success or failure.

Since wireless networks do not have actual physical ports, they are vulnerable to spoofing attacks. An ongoing session can be easily taken over by other devices by spoofing the MAC address of the original supplicant. For this reason, 802.11i extends the properties of 802.1X by setting up a session key between the client and the AP. The same session key can be used for any further communications between this AP-client pair.

Key Generation and Management

One of the primary reasons for adopting EAP methods is the establishment of a session between the client and the AP. This is carried out by utilizing a key known as Pairwise Master Key (PMK). The key is termed pairwise since this key is unique to any client-AP pair. PMK being a master key, is not used directly for encryption or decryption of messages. Instead, it helps the client and AP to derive four other keys out of it. These are data-encryption key, data-integrity key, the key-encryption key, and key-integrity key. Together these four are known as Pairwise Transient Key (PTK). In addition to

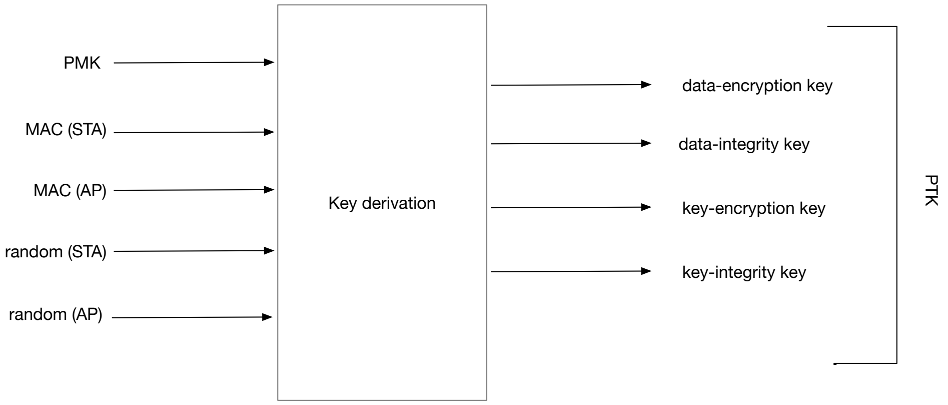

Figure 2.2: Derivation of the PTK [2]

PMK, the derivation of PTK also requires the MAC addresses of both the devices (client and AP) and two random numbers spawned by the devices, as shown in Figure 2.2.

The random numbers involved during the PTK generation are exchanged between the client and AP using the EAP 4-way handshake protocol. It ensures that both the devices possess the PMK. The operation is carried out in the following steps:

1. First the AP sends its random number to the client. After receiving this number, the client has all the necessary information to generate the PTK. Hence, the PTK is computed on the client device.

2. The client computes the Message Integrity Code (MIC) using the key-integrity key derived from PMK and forwards it to the AP along with its own randomly generated number. Now the AP derives PTK on its end and verifies the received MIC using the key-integrity key. When the verification is successful, it is believed that the client possesses the PMK.

3. The AP calculates the MIC value of the PTK generated and sends it to the client along with an initial sequence number. If the MIC is verified successfully by the client, it is believed that the AP also has the PMK. The sequence number is used to mark further packet transfers and detect any replay packets. From the received

message, the client is also informed that the keys have been installed on the AP and it is ready for encrypting packets for further communication.

4. Finally, the client sends an acknowledgment of the previous message to the AP, in addition to indicating that it is now ready to encrypt any following data packets.

After the derivation of PTK, the keys are installed on both devices. Thereon, data encryption and integrity keys facilitate the transfer of data packets securely between the client and AP. However, the same keys are not sufficient enough when the packets are broadcasted from an AP. To protect such packets, the AP generates an additional key which is termed as Group Transient Key. Group Transient Key comprises a group encryption key and group integrity key. These keys are known to every client in the network and sent to all of them separately along with the key-encryption key of the corresponding client device.

2.3 Association Process

Once the authentication process is complete, the client can associate with the AP to gain full access to the network. This process allows the AP to record each client so that the corresponding frames can be properly delivered to the respective recipient. One limitation of the association process in wireless networks is that a given client can only associate with one AP at a time.

In order to provide access to the client, the AP allocates a unique AID and responds to the client along with a status code of 0, which means that the association process was successful. This AID is utilized to deliver the packets (or any buffered frames) to the correct owner. If the association request fails, the AP responds with only a status code. This marks the end of the association process.

2.4 Summary

In this chapter, we analyzed the discovery and channel scanning process on 802.11 devices. This procedure has been broadly treated in the literature when a client needs to switch from one AP to another. We also conferred the operation of WEP and discussed its shortcomings. The authentication and key management mechanisms of 802.11i were presented. The necessity of compatibility with old WEP devices was a serious design constraint and TKIP has been successful in eliminating the weaknesses of the RC4 encryption algorithm. We also presented how different keys during the EAP handshake is generated and finally, the association steps between AP and clients.

Chapter 3

Channel Scanning on Client Devices

The 802.11 discovery process concerns the optimization of the Layer 2 handoff when a client roams between APs. The number of channels, link quality, and packet collision delays the scanning process during roaming. The unnecessary timers on each channel sometimes also add to this latency. This chapter discusses various strategies that focus on effective communication between the client and the AP by utilizing the information provided by beacons and probe responses, thereby eliminating delays and resulting in a faster roaming process.

3.1 Channel Assessment and Unicast-based Scanning

When an AP is listening and replying to the probe requests from a client, it misses the reception of packets from other clients. There is a high chance that packets from multiple clients are transmitting at the same time, which may lead to loss of data packets [10]. To avoid such collision, clients use Request to Send (RTS) and Clear to Send (CTS) mechanism to determine if the medium is busy. They send out control frames and the Network Allocation Vector timer lets the client know how long it has to wait for sending RTS frames to the AP. If the AP replies to an RTS frame with a CTS frame, it means that the AP is ready to receive data. If the AP fails to send any data frame, the client has to wait until the MaxChannelTime is expired. MaxChannelTime is the longest time

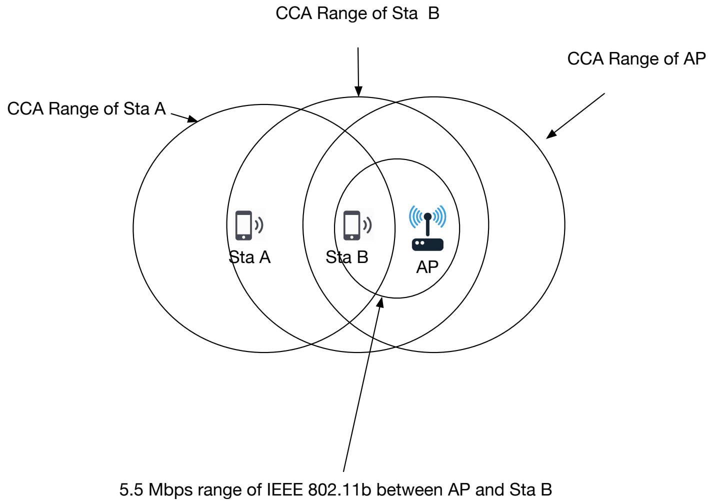

Figure 3.1: Undesirable behavior example caused by MaxChannelTime [3]

interval a client can wait on a particular channel before moving on to the next channel. Similarly, MinChannelTime is the minimum duration for which a client needs to wait after sending out the RTS frame.

In some scenarios, the AP sends back a CTS frame but fails to send any data. This means that the AP has been found but it is not suitable for serving the clients because of resource constraints. Figure 3.1 depicts a scenario where client A is searching for an AP. It is present inside the Clear Channel Assessment (CCA) range of the AP and sends out a probe request. However, another client B is much closer to the AP than client A and is performing data exchange at a higher transmission rate. Since the AP is occupied with sending packets at a fast rate to client B, it fails to respond to client A with a data frame. As a result, client A has to wait for an inessential period which equals MaxChannelTime.

To address these problems, Sunggeun et al. [3] introduce two new concepts: channel assessment and AP search algorithm. During the channel assessment, the client utilizes RTS/CTS frames to identify suitable channels by accessing all the channels in a virtual AP environment. A virtual AP can be described as the capability of a Wireless

Network Interface Card (WNIC) to support multiple MAC addresses on the same physical interface card. It shares the specifically reserved MAC address between all APs and clients and this is used only for RTS/CTS exchange purposes. For the rest of the operations, it uses its unique MAC address.

During the AP search process, the client performs a unicast-based scanning on a selected channel to search for a suitable AP. The two algorithms that have been introduced are: first-fit and best-fit. The first-fit algorithm starts analyzing probe responses and as soon as any entry matches the requirements, it stops the assessment and tries connecting with the AP. In the near best algorithm, the values received on each channel are compared against the highest data rate found so far while the remaining entries are discarded. If more than one candidate has been shortlisted, the one with the higher value is picked.

One possible limitation of using the first-fit algorithm is that it may not always provide the best optimal AP. The hit ratios for these algorithms also vary depending on supported bandwidth and coverage since a successful RTS/CTS frame exchange directly depends on the coverage area.

3.2 Synchronized Passive Scanning

When a client device moves outside the range of one AP, it must temporarily leave the current AP and start looking for alternatives. The duration between leaving the current AP and joining a new AP could be even up to one second [11], which is a huge gap for applications sensitive to a network outage. The scanning process majorly contributes to this delay and can be calculated using the formula (3.1). For example, in a 2.4 GHz band with 10 channels (excluding itself) and a beacon interval of 100ms, the scanning

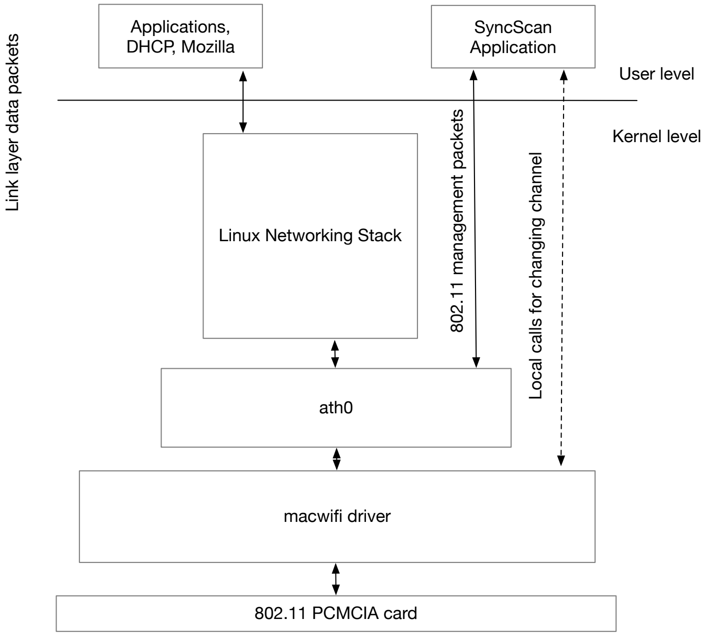

Figure 3.2: Architecture of a prototype SyncScan implementation in Linux [4]

and channel switching delay combined is well over a second.

$$ScanDelay = NumChannels * MaxBeaconInterval \tag{3.1}$$

Ramani et al. [4] replace this huge overhead of searching nearby APs by running a continuous process that audits other channels for detecting APs. In this approach, the periodic transmissions from each AP are synchronized with short listening periods on the client device. The APs are typically set to send beacons at 100ms interval and can be easily configured. The flexibility of modifying the beacon reception time on each channel can be beneficial when the clients are scanning passively and switch the channel to the original when the beacons are expected to arrive. The client device uses this property to discover every other AP in its surrounding area. By shifting to every channel in a timely fashion, a complete dataset of neighboring APs is gathered. Whenever a handoff is tried in this manner, the delay factor decreases for authentication and reassociation. The setup for this approach doesn't require any changes within the existing protocols, instead of some minor modifications as shown in Figure 3.2. The driver interacts directly with the SyncScan daemon and gets instructions when to switch channels and collect beacon frames. Since the beacon announcements do not impact any of the existing 802.11 standards, this method is also backward compatible for clients when they can't be synchronized with SyncScan infrastructure.

Velayos et al. [12] provide a mechanism and proof ensuring that a minimum of three dropped packets is enough to notify and trigger the search for an alternative AP. They conclude that the delays associated with an active scan can have multiple factors. MinChannelTime is one of the factors that can be customized depending on the need. This is the first parameter that decides whether or not the channel is empty and several researchers have recommended different values for MinChannelTime, ranging from 1 millisecond to 7 milliseconds. On the other hand, MaxChannelTime value is to be configured by the number of overlapping APs and also while reckoning the load on the channel. The MaxChannelTime is generally taken as 11ms. The paper concludes that the delays associated with search can be reduced by using active scanning if the timers are properly set, and the searching phase can even be performed parallelly with ongoing data transmission.

Bahl et al. [13] propose that a continuous scanning implementation will discover the presence of access points before the Signal-to-noise ratio value from the access points has fallen below its threshold. It additionally offers a chance for continuous location trailing of the mobile device. This is in contrast to traditional methods where a full scan was needed and as a result, this used to prevent any ongoing communication.

Although, running a search process alongside data communication does benefit during handoffs, but it also adds new complexities. SyncScan targets passive scanning which doesn't look like an attractive choice in today's WLAN devices. If multiple APs are operating on the same channel, it introduces interference among beacon frames.

Also, while a client is listening on other channels, it fails to collect data from its AP. An aggressive bound on MinChannelTime and MaxChannelTime [12] are too difficult to determine, especially when channel conditions, number of clients in the vicinity and network topologies vary. It also introduces a fair percentage of call drops during handoffs. Consequently, the maintenance and continuous search add a large amount of management overhead for large scale networks.

3.3 Concurrent Data Transmission and Scanning

At present, 802.11 networks use a break-before-make approach whereas cellular networks use a make-before-break mechanism. Make-before-break results in comparatively lesser handoff latency in cellular networks. If the scanning process can be isolated from an ongoing data transmission on an 802.11 client, it would drastically improve the latency involved with handoff for the clients. This isolation can be achieved by equipping either the client or AP with additional interfaces.

3.3.1 Multiple Interfaces on Access Point

Choi et al. [5] propose a mechanism to equip the APs with multiple WNIC keeping the client with a single WNIC. One of the AP's WNIC is assigned the task of providing scanning information on a reserved channel and every AP in the network uses the same BSSID. This considerably reduces the scanning time as the client only has to scan the reserved channel rather than all of them. This approach also eliminates the use of network graphs which stores the information of APs with their respective available channels.

They have also introduced a Power Save Mode to keep track of every packet des-

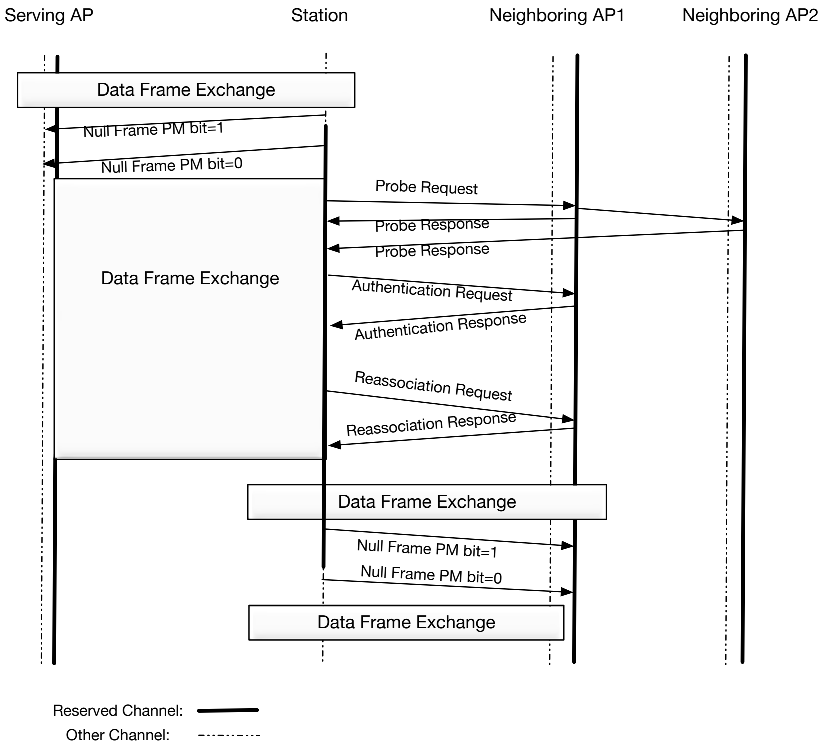

Figure 3.3: Handoff procedure using reserved channel [5]

tined for the client. A Power Save mode can be defined as a state in which when a client enters, notifies the AP to start buffering all the frames destined for that client. The client sends out a null frame with the Power Management (PM) bit set to 1 to inform the AP that it has entered the power-saving mode. While the AP is buffering all the frames, the client switches from the operating channel to the reserved channel for scanning APs. The client sends a probe request on the reserved channel and waits for a response, as shown in Figure 3.3. A probe response has the competence to carry channel load information of the AP [14]. Since the AP has a separate WNIC for sending back a probe response, it saves the task of responding on every channel. If no AP is found on the reserved channel, the client concludes that no AP is present in its proximity. As the probe response includes load information of all the channels, it helps the client to select the best channel to associate. When a satisfactory AP response has been received, the client proceeds authentication with this new AP. Once both authentication and reassociation procedures are complete, the client sends a null frame with PM bit set to 1 on the reserved channel and PM bit set to 0 on the regular channel. After switching the channel, the client resumes data transmission and receives all buffered frames via the new AP.

Luis et al. [15] suggest adding a Light Virtual Access Point on the AP. A Light Virtual Access Point shares the same MAC address of the AP. This is used for communicating with each client in such a way that the clients can only see a single AP. As a result, the client doesn't even need to switch between the MAC addresses during reassociation. They use a central controller device that adds subscriptions for change in threshold events on a client. When the client starts moving out of range of current AP and the RSSI value drops below the threshold, the AP publishes a message to the controller. The controller issues a scan request on all nearby APs and the APs switch to alternate interface to start listening for packets from the client. Upon receiving a positive search response, the controller directs the best suitable AP to send multiple Channel Switch Announcement packets to the client. This is followed by a successful connection between the new AP and the client.

Jeong et al. [16] also propose to add a wireless interface to the AP. However, their approach is very different from the ones discussed above. Instead of the client doing all the scanning, they suggest using the extra interface on the AP to assist during the scanning process. As a result, the clients stay on their channel and do not perform any kind of search. The AP, on the other hand, uses the additional interface to switch between channels and broadcast beacon frames. This facilitates the client devices to remain up-to-date about the neighboring AP's information. This approach eliminates the channel scanning process on client devices and avoids service disruptions.

3.3.2 Additional Interface on Client

A single radio interface on the client frequently gathers information from the network to optimize Layer 2 handoff while being associated with the current AP. However, a process switch from transmitting the data to scanning the neighborhood, and vice versa, add latency to real-time applications. This switching can be replaced by making use of an additional interface on a client.

Ramachandran et al. [6] propose to dedicate the task of transmitting data and scanning to data and control interfaces respectively. Whenever the data interface detects a weaker signal from the current AP, it notifies the control interface to search for the next candidate APs and perform the authentication and reassociation processes accordingly. Since the client has been connected to the new AP before breaking the connection with the old AP, it ensures the elimination of Layer 2 handoff. This approach can be further categorized into two divisions:

(1). Two dedicated interfaces (static approach): One interface is dedicated to exchange the data while the other interface is used for control. The data interface remains connected with the current AP and is constrained to handle data frames. On the other hand, the control interface actively keeps searching for nearby APs and is responsible only for management frames. The data collected from the control interface is consulted whenever the client goes out of coverage and this helps in determining the appropriate AP for the client. It then proceeds association with the selected AP and finally switching the channels. Since the scanning process is skipped in this manner, it helps to improvise the probe delays.

(2). Two interchangeable interfaces (dynamic approach): The two interfaces are used rotationally and they switch their functionalities accordingly. Once the client decides to associate with the new AP, the control interface connects with the new AP

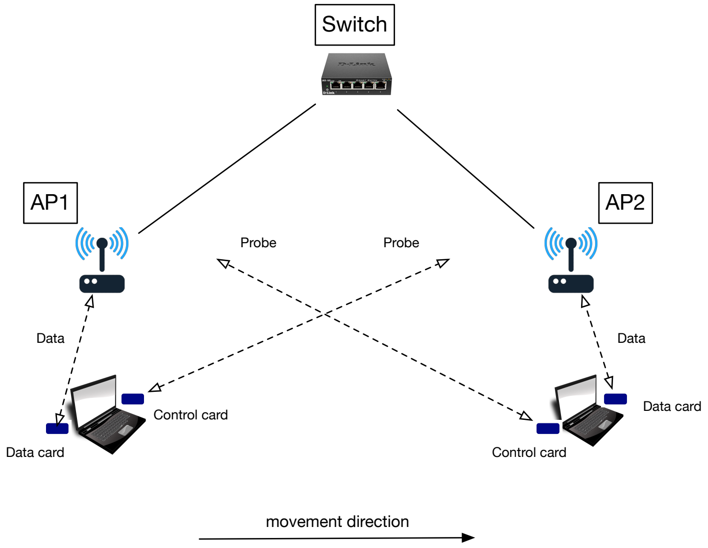

Figure 3.4: Two interface dynamic algorithm [6]

and itself becomes the data interface. Similarly, the data interface takes over the job of the control interface and starts performing management functions, as shown in Figure 3.4. The delays involved with this approach are associated with modifying routing tables on the client, connecting the AP with the control interface and submission of Address Resolution Protocol (ARP) requests.

Adya et al. [17] explore the effects of multiple network interfaces on hardware and software designs, along with algorithmic complications and use the interfaces for operating on different channels to create a path with multiple hops. They conclude that when both these interfaces are used simultaneously, it gives poor re-ordering results. The primary reason for this effect is because of the unequal load on the two wireless links and cross-interference between the radios.

Bianchi et al. [18] follow a similar approach and propose to use the secondary interface to figure out the list of nearby APs using management frames and then the client tries to connect with the new AP using the primary interface. The scanning process can be eliminated in this manner and the delay involved with switching the channels could be as low as 20ms which is quite remarkable [18]. This handoff is a precisely safe operation as nothing has been modified on the infrastructure except that the client seems to be skipping the scanning stage. The primary objective of this approach is to provide less latency with minimal modifications on the existing network devices. Both the interfaces are assigned the same MAC and IP addresses, which makes it appear as the same device has now been connected to a new AP without any latency. Once the handoff of the client is complete, an ARP is sent across the network by the AP advertising a new association for other devices to update their cached ARP entries.

In most of the cases, the addition of WNICs resolves the issues concerned with scanning delay. However, they have several shortcomings as well. The virtual AP approach [15] suffer from throughput degradation and signaling overhead with an increase in the number of clients. The additional interface on clients, as presented in [6], proves to be infeasible for small client devices due to limited power source. The approach proposed by [5] helps to reduce the scanning delay and benefits clients to skip searching on every single channel. However, there is still an inexorable delay associated when the client switches to the reserved channel and scans for APs. Similarly, there could be a loss of packets when the secondary interface has connected to a new AP whereas the packets in the buffer are destined for the primary interface are discarded by the AP [18].

3.4 Link Disparity and Proactive Scanning

Current 802.11 devices are assumed to be within identical transmission range and environmental conditions. However, there could be a scenario when device A is within the transmission range of device B, but the reverse is not true. This is termed as link asymmetry and could be because of multiple reasons. The client and the AP can have varying transmission and reception capabilities. Moreover, the hardware and software implementations could be entirely different.

Waharte et al. [7] suggest to calculate and compare Frame Loss Ratio to better understand link disparity. Frame Loss Ratio can be defined as the potential loss of Layer-2 frames in a wireless medium and this could be either in uplink or downlink directions. This incidence of link disparity can affect 802.11 handoffs. Most implementations are concerned with employing a trigger that measures the standards in one transmission direction and ignores the opposite one. It may result in inefficiency to discover poor performance in the opposite direction. Followed by this, if a client performs an inactive scan, it will solely have downlink link quality for making a handoff. Sometimes the beacon of an AP is detected by the client. The transmission packets of the client, however, is not acknowledged by the AP. In these cases, a handoff call may result in additional delays and may even result in a timeout.

They have performed active checks which can confirm reduced scanning time on every channel and identical uplink and downlink qualities with the AP. Adaptational algorithms can also be employed to alter the scanning interval and channel search sequence and store the updated information for carrying out a handoff. Additionally, it makes use of a handoff trigger that scans uplink and downlink quality and is split into two steps: one for triggering the scanning process and the other for client handoff. It ensures the correct balance between channel scanning overhead and handoff intervals. As a result, the service disruption interval for VoIP applications can be minimized.

The authors of [7] also propose to limit the number of channels to be scanned to reduce the overall scanning delay. This is achieved with the help of relay sensors that gathers nearby information and updates a distributed database. The mobile client broadcasts an AP List request to the sensors and provides a criterion to shortlist the APs, as shown in Figure 3.5. The sensors respond with the list of APs, which is then processed by the client and the scanning process is initiated based on the AP list entries.

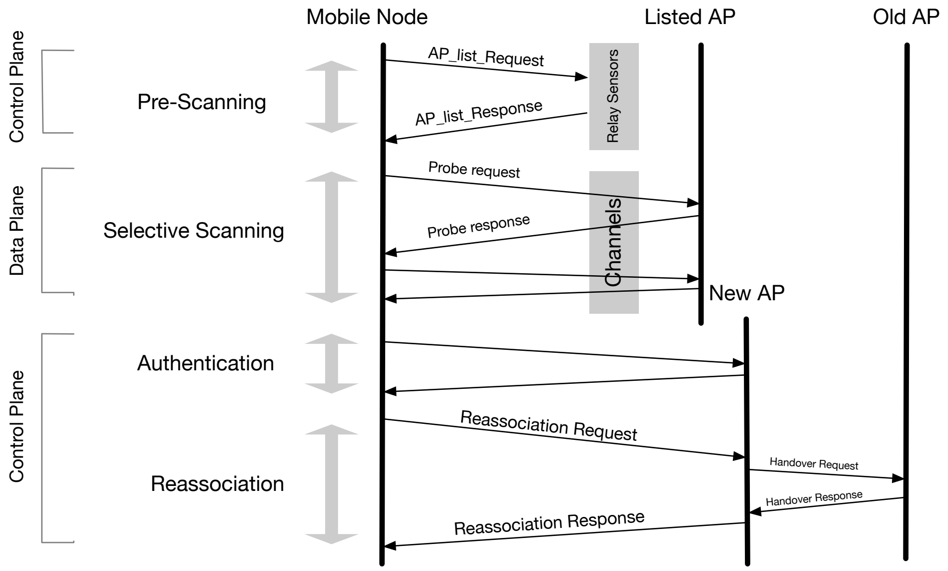

Figure 3.5: Selective-Scanning handoff process [7]

The rest of the handoff process remains the same, except that the pre-scanning and reassociation steps are carried out in the control plane. One major disadvantage with this approach is that the ongoing applications may notice additional delays because the scanning process is in progress on the remaining channels.

3.5 Non-Interfering Channels

Rodrigues et al. [19] introduce Network Simulation 3 (NS3) that comprises nodes where the named wireless devices perform on different channels and they can prevail altogether on different devices. Since cross channel coupling is not supported on the NS3 model, the simulation is not useful for every multi-channel scenario. For this reason, only non-overlapping channels can be used to assist Wi-Fi roaming in a networking topology. The network model according to NS3 confirms that the best AP is not selected by the best RSSI values obtained. Rather, the first satisfactory value is picked instead of waiting for a timeout. The only situation when it looks at responses received on other channels is when the association request fails. Other parameters also need to be taken into account other than RSSI.

They have implemented two methods for selecting an AP. In the first method, it collects the information of all the channels serving clients. In the second, it figures out all the other metrics which are necessary for a client to get associated with the AP. These metrics could be anything ranging from supported rates to the least latency offered during handoff. The final AP among all the candidates is chosen based on the combined results of the metrics mentioned above. The possibility of Wi-Fi devices to work on the same frequencies is still in development phases and could be a big boost for next-generation networks.

Bangolae et al. [20] conclude that beacons play a vital role during a passive search with the downside of consuming a lot of time. Since this is not the best way to search for neighboring APs, few topology alterations offer very effective solutions on top of passive scanning mechanisms. The 802.11 devices have multiple channels and this varies depending on the location. For example, devices in the United States are equipped with 11 channels while most of the European countries have 13 channels and this number can be even bigger depending on requirements. The most common channels used are 1, 6 and 11 to avoid any overlap or interference between each other.

Castignani et el. [21] conduct a study that shows that roughly 61.1% of the access points operate on channels 1, 6 and 11 only. They also suggest that for getting a latency within 50 milliseconds range, these channels should be the first ones to be scanned in the case of VoIP applications. However, for other applications, the delay could be longer and the range of channels needs to be increased.

3.6 Self Optimizing Parameters and Prediction-based Scanning

Hao et al. [22] suggest that to find the best suitable AP for a client, the scanning process covers every single channel which is sometimes not necessary. Instead, any AP matching the minimum requirements should be fine and it would minimize the overall delay. They have introduced a novel approach called Genetic Algorithm. Before a search process is initiated by the client, this algorithm is used to refine the scanning parameters and configure them for each client. Once an optimal value is found, the tables inside the AP Controller is populated with these values. The parameters are refreshed only when the clients have found a new AP or the APs go out of range. The primary purpose of the Genetic Algorithm is to avoid scanning all the channels and preserve the list with optimized timers. These entries also can be updated using adaptive timers.

A prediction based channel scanning could be a selective scanning with synchronic information transmission. The selective approach makes it attainable to focus solely on presently active channels, rather than synchronous data transmission. Scanning reduces the service dissolution of broadcasting in clients. This additionally defines a time-limited scanning with prediction technique, that helps to scan additional channels among a sensible scanning interval, and reduces total channel scanning time. In smart scanning, it is believed that clients will get the information of all neighboring BSS. The data includes the active channel range, the number of clients connected, and traffic information on every AP. The live channel range is employed to scan selected channels and traffic alerts, whereas the quantity of clients in every AP is employed to estimate the need for sensible scanning. This info will be obtained utilizing completely different approaches, like feedback exchange with MIHGetInformation Request or Media Independent Information Server [23], from the serving AP in IEEE 802.11k [24] or from any other external server.

Kim et al. [25] propose an algorithmic program that describes the operation of sensible scanning. When scanning through the channel range, the clients store the list of candidate channels. Before switching to any channel from the current one, the client sets PM bits to 1 within the outgoing message to AP, as suggested in [25]. It permits the serving AP to buffer the packet destined for scanning clients and eliminate packet loss. The average packet arrival rate considers uplink and downlink quality for each transmission packet. The prediction channel scanning time is combined with accumulated scan interval. If this value exceeds the maximum acceptable interruption duration, the usual data transmission is performed. Otherwise, the candidate channel is scanned.

3.7 Utilizing Spatiotemporal Information

Mishra et al. [26] introduce network graph concepts to reduce reassociation delays. This graph stores the moving information and current location of the client for short intervals until updated. The cache data of the network graph signifies possible APs for handoffs. A cache hit occurs when the client searches for a particular AP in the list and finds it. On the other hand, a cache miss occurs when the AP is not on the provided list. This approach works fine with a limited number of APs in the proximity, and the overhead increases with a rise in number.

Chen et al. [27] introduce a novel concept called spatiotemporal scheme which makes a list of APs that can be further used by the client. When a client enters a new mobility domain, the complete scanning procedure is re-initiated. The spatiotemporal graph consists of multiple triangles, where a triangle comprises of clients and APs. A triangle has been described as a group of three APs and one client, formed at one particular timestamp and location. If the triangle doesn't appear in the spatiotemporal graph, it signifies that the client has entered the region for the first time. This triggers another full scan on the network and a new triangle is added to the graph. Time synchronization is also needed for allowing the client to maintain the order of APs found during scanning. The scanning process ensures to handle the handoff operations comprehensively using graphs. During the handoff process, the client confirms whether the new target AP has enough resources to serve the client, and the AP is selected from the spatiotemporal triangle. This is more likely applicable to vehicular radios as they need dynamic information in every finite interval of time. The combination of motionless and progressive client scenarios analyses factors responsible for making wrong decisions and an effective method makes correct decisions providing accurate results.

Jihwang et al. [28] present a variety of challenges faced in wireless medium and end-to-end delays between a client and an AP. The concept of sniffing over a finite area can be a viable option to search the best neighboring AP. The pre-scan scheme discussed in [6] performs latency calculation and analyzes system models for delay-sensitive applications. The measurement of RSSI is not included in the handoff latency because it initiates along with the start of handoff operation and the cost is enfolded with the time spent during the pre-scanning process.

Almulla et al. [29] propose to blacklist those APs who have not been able to serve clients recently. In vehicular networks, it is important to figure out the exact position of the vehicle. To achieve this accuracy, the movement direction of the vehicle and surrounding APs is very crucial. Another need is to let these moving clients complete future associations with APs and to be given more priority over other clients. When a connection request has failed for a particular pair of clients and AP, connection requests with similar pairs should be avoided to save latency during the failure situation. This has been termed as blacklisting. The acceptable reason for connection request failures could be either no response or unavailability of network resources.

The blacklist scheme establishes a demand to exclude those APs, which might be incorrectly selected during high priority search. The database maintains an entry for each of this blacklisted APs. It is important to note that each entry has a timestamp and they are removed from the list after the fixed timer expires. This is to make sure that no AP has been blacklisted forever as network conditions may change with time. The APs in the list follow the least recently used approach where recently inserted blacklisted AP is removed at the end. It checks whether the MAC address of the AP matched with any of the database entries. For a successful hit, the timer remains the same and for an unsuccessful one, it starts decrementing by one. Once the timer count reaches 0, it is an indication of the removal of AP from the blacklisted list.

The paper suggest utilizing the Global Positioning System to find the exact location of vehicles and stores the location of APs in a local database. The scanning process is as follows: The client changes its regular communication channel to a constant channel for APs at a lower priority value. This is followed by searching for alternate APs having higher priority values. Instead of broadcasting the probe request, the client sends it to the specific MAC address of the AP which is extracted from the database.

The location-based techniques help reduce the overall scanning time by searching for selected APs. However, they add several overheads as well. Context caching [26] provides poor performance when the APs are densely deployed over several channels. In DeuceScan [27], the handoff time increases with an increase in the number of clients and payload size. This occurs as a result of competition between transmitted frames by the clients during scanning, It also requires a full scan every time the client enters a new region and it does not have the neighboring APs information in the cache. Similarly, the approach proposed by [30] needs the client to perform scanning multiple times to discover APs in a densely covered area.

3.8 Comparison of Discussed Channel Scanning Schemes

Table 3.1 compares the most common scanning schemes concerning the number of interfaces used, layer and modification in existing topologies defined by IEEE standards. The interfaces can be added either on the client or the AP. The location trailing feature adopted by some of these techniques follows backward compatibility, which means that it will switch to the typical client-AP architecture if the introduced algorithms are not supported.

Reference	Wireless Interfaces	Access Category	MAC/Link Layer	Access Method	Infrastructure Modification
[5]	2	Contention	MAC	Distributed	yes
[6]	2	Hybrid	MAC	Distributed	yes
[14]	1	Hybrid	MAC	Distributed	no
[31]	1	Hybrid	MAC	Distributed	no
[3]	1	Contention	MAC	Distributed	no
[21]	1	Contention	-	Distributed	no
[7]	1	Contention	MAC	Centralized	no
[32]	1	Hybrid	Link	Distributed	yes
[33]	1	Hybrid	Link	Distributed	no
[15]	1	Contention	Link	Distributed	no
[15]	2	Hybrid	MAC	Centralized	no
[18]	1	Contention	MAC	Centralized	no
[22]	1	Hybrid	MAC	Distributed	no
[34]	2	Hybrid	-	Distributed	yes
[17]	2	Hybrid	MAC	Distributed	no
[35]	1	Contention	Link	Distributed	no
[36]	1	Hybrid	MAC	Centralized	no

Table 3.1: Comparison between channel scanning schemes

3.9 Summary

As we saw in the previous sections, most of the schemes have been focussed on adding multiple interfaces or collection of data using clients and APs. These interfaces gather information on nearby devices and assist clients during roaming once it experiences a certain number of dropped packets. The interference between data packets is a major concern when the number of clients is large in a defined network. For devices with VoIP applications, it is crucial to provide consistent network connectivity. However, a continuous scanning process isn't always the best approach to deal with this problem. While the location of an AP is mostly fixed, tracking the position of moving clients is an efficient way to trigger the initialization of the scanning procedure.

Chapter 4

Fast Roaming in Centralized Networks

The generic process of 802.1X/EAP standard helps mitigate the security issues of legacy 802.11 networks. It introduces the generation and sharing of session keys which makes it difficult for attackers to gain access to the network. Further, Pre-Authentication facilitates the process of authentication of a client to other APs while it is already connected to its current AP in a centralized architecture. The Pre-Authentication support is publicized using the RSN information component within beacon frames. A significant downside with the Pre-Authentication method is scaling, as all the clients have to be authenticated with every AP within the network in advance. This produces an unnecessary load on the authentication servers. To overcome this issue, a new task group was formed and referred to as 802.11r. This group introduced a protocol known as FT that was suitable to offer resource reservations to only selected APs in the network.

4.1 Roaming Process in 802.11r FT

FT can be described as a mechanism by which clients can reestablish existing QoS parameters and security before its reassociation with a new AP. They are referred to as fast due to the significantly lesser time difference when a client moves from one AP to another. The process is carried out in three major steps: combining the 4-way handshaking with 802.11 authentications and association exchange, pre-allocation of resources and competent key exchanges. It introduces new information fields like Mobility Domain Information Element (MDIE) and Fast BSS Transistion Information Element (FTIE). MDIE consists of a domain identifier, capabilities and policy values of the AP [37]. On the other hand, FTIE includes key identifiers obtained from the primary AP and the client device, and key holders.

The Handshake is carried out by adding the EAP key messages over the existing 802.11 authentication, association request and association response frames. MDIE and FTIE are included within beacons, probe response, association request, and response. The remaining procedures for PTK derivation are completed throughout the authentication and reassociation steps. One fascinating feature of 802.11r is pre-reservation which implies a client that needs to connect with a target AP, will first complete the QoS admission process before authentication and reassociation.

Over-the-Air

Over-the-Air is performed directly between the client and the new AP using legacy 802.11 authentications along with the FT authentication algorithm, as shown in Figure 4.1.

Steps:

1. Client is currently associated with AP1, requests to roam to AP2
2. Client transmits an Authentication Request to AP2, receives an Authentication Response from AP2 in return
3. Client transmits a Reassociation Request to AP2, receives a Reassociation Response from AP2
4. Client completes roaming from AP1 to AP2

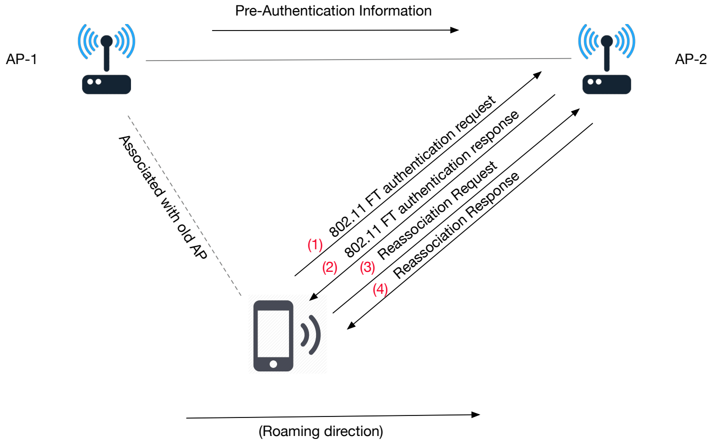
Pre-Authentication Information
AP-1
AP-2
Associated with old AP
(1) 802.11 FT authentication request
(2) 802.11 FT authentication response
(3) Reassociation Request
(4) Reassociation Response
(Roaming direction)

Figure 4.1: FT Over-the-Air [8]

Over-the-DS

Over-the-DS is applied using the DS or direct 802.11 links connecting the APs. The client communicates with the new AP via its current AP, as shown in Figure 4.2. Since the pre-reservation completed in advance will typically lead to unused resources, a novel mechanism referred to as QoS provisioning is additionally a part of 802.11r that makes sure the pre-reservation request is delayed until the particular association request and response.

Steps:

1. Client is associated with AP1 and requests to roam to AP2
2. Client sends an Authentication Request to AP1, receives an Authentication Response from AP1
3. The Pre-Authentication information is shared between the APs via the controller
4. Client sends a Reassociation Request to AP2 and receives a Reassociation Response from AP2
5. Client completes roaming from AP1 to AP2

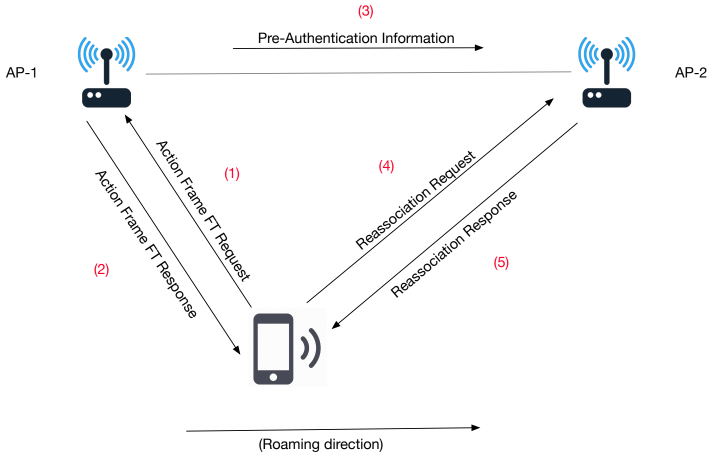

Figure 4.2: FT Over-the-DS [8]

4.2 Handoff Among Multiple Mobility Domains

IEEE 802.11r FT standards do not offer support for the roaming of devices beyond its mobility domain. This is a complicated scenario for those clients which are located at the boundary of two mobility domains. Chi et al. [38] introduce a unique approach to deal with these challenges. The mechanism presented is to Pre-Authenticate the clients with 802.11i security mechanisms. It keeps Pre-Authenticated security keys for promptly matching with some of the potential APs that are supposed to be present in the path of the client's movement. These keys are then employed for protecting the data after the handshake has been completed. To find out the next potential APs, the location servers serve as the controller and retain the information of all the devices in the network. After analyzing the moving tendency of the client, the location server figures out which APs the client may reassociate next. This helps the client in sending out connection requests to less number of candidate APs rather than to every AP in its proximity.

The neighbor graph being regulated by the location server provides viable options in determining the appropriate APs. It also stores the information regarding successful connections in the defined locality and past connections of the clients. If the client is simply moving back and forth among a bunch of APs, this will be easily detected by the location server from historical data. During the cases when PTK security association does not exist on the target AP, two possible solutions have been proposed. Firstly, if the AP still has the PMK, it will still accept the reassociation request and grant a response. Since the connection request has been granted but PMK is missing, it generates a status code for the client to complete the next steps. In this case, the client needs to complete the handshake procedure again. In cases when the AP is not holding the PMK, a response is issued for the client mentioning authentication failure as the status code. In such scenarios, the client needs to complete both, the 4-way handshake and the 802.1X authentication.

The location server serves as the network controller and it has prior knowledge of every mobility domain over the area being managed. This information can be collected even without knowing the entire topology and making use of client tracking along with registration with regional Authentication Servers. However, in a densely deployed region, the APs might suffer from memory limitations while storing too many security keys. Similarly, it would result in additional overheads for the location server to keep track of every device in the network.

4.3 BSS Transition on WLAN with SDN-based Distribution System

Enhanced Service Set (ESS) FT on Enterprise WLAN with SDN-based DS [39] uses cognitive management that permits checking for resource availability before choosing a target AP. It conjointly provides QoS handoff with resource requests over DS and proactive forwarding table updates of SDN-based DS. Within the current handoff processes, most of the clients try to associate with the closest AP with the strongest beacon signal strength without considering the traffic load and congestion status of the AP [40]. Hence, the BSS agent collects per-client traffic for every AP using sensible scanning and forwards it to centralized ESS Control and Management. ESS control and management then check the provision of requested network resources at the neighbor APs within the received list, selects some clients within its range and directs them to maneuver to less engaged neighbor APs.

The 802.11r FT procedure does not support any kind of notification from the client regarding delay-sensitive applications and corresponding resource requirements. As a result, the association requests may get denied due to limited resources on the AP. This results in a failure situation and the client again needs to look out for a different AP, which adds up to the overall latency. The forwarding table features are also missing in the FT standards. The chances of packet loss can be greatly minimized with the utilization of forwarding tables. The paper [39] propose a QoS-aware FT mechanism which guarantees better roaming support and load balancing for devices with delay-sensitive applications. The mechanism ensures checking the availability of resources on the AP before making a reassociation request. The roaming request is sent over the DS. It also provides forwarding table updates through the SDN controller. The average testbed results guarantee a disruption interval of less than 20ms with minimal packet losses.

4.4 Context Transfer in Centralized WLAN Architecture

Proactive Neighbor Caching is a method proposed by [41] to support context transfers during authentication and reassociation. A context comprises of the client's session details, QoS, and security state information. To facilitate FT, this context is transferred to a few potential Wireless Termination Point (WTP) [42] as per the information collected by network graph topology. The benefit of using context transfers is to skip doing the complete authentication/reassociation process again. Selective Neighbor Caching further minimizes the number of WTPs to specific ones having a higher probability for handoffs.

Huang et al. [43] utilize CAPWAP [42] to extend the context transfer mechanism to centralized WLAN architectures. It propose to divide a WLAN architecture into two segments: WTP and Access Controller (AC) [44]. An AC can be described as a centralized controller that manages, controls and configures WTPs. The paper presents a Cluster-Chain-based Context mechanism that helps with the monitoring and control of a large number of APs and administering a uniform configuration throughout all the APs with the assumption that every WTP belongs to the same mobility domain.

The operations involved with context transfer [45] can be classified into three major categories: Initial association, Reassociation with context miss and cluster transition. During the initial association, the client completes security key exchanges with WTP. Once successfully granted access, the controller is notified to find the mobility domain or cluster of APs. The list is then forwarded to the client along with other context transfers. In the reassociation process, the clients start moving and lose the connection with the original WTP. It then tries to re-connect with the WTP but fails. A cluster transition occurs when the nearby AP is not on the list of APs provided to the client.

The client requests access to this new AP by notifying the controller. Accordingly, the controller forms a new cluster APs and sends the list to the client. This is followed by context transfer between the controller and AP, and then reassociation with the new WTP.

In this case, the handoffs shift all the management and control logic to the AC. WTP is employed as a radio controller and a bridge between wireless and wired medium. This approach makes use of the idle time which remains unutilized by data packets throughout a handoff. Each client is discovered by its WTP and therefore the results are sent to the AC for creating the choice whether or not the client ought to roam to a different WTP. If the new WTP is capable of serving another client, the AC directs the current WTP to transfer the client's context. There are few drawbacks to this approach. WTP cannot perceive information higher than L2 and thus cannot hold encoding keys. Thus all the packets are processed, decrypted and once more sent towards the AC. It also ends up in the enlargement of Ethernet headers which increases the overall delay.

4.5 Summary

In this chapter, we discussed the different types of client roaming in a centralized architecture. Utilizing 802.11r for transferring session information is a great approach to skip most of the reassociation delays. Since the range of a mobility domain is limited, the clients at the boundaries of two different mobility domains might suffer from latencies while trying to exchange and store different security keys. A location server tracking the historical data of clients in a bigger network is a solution to this problem. Proactive caching and QoS-aware approach provides better context transfer mechanisms for devices with delay-sensitive sensitive applications.

Chapter 5

Conclusion and Future Work

The process of client roaming introduces latency factors which is a significant component in WLAN, especially for delay-sensitive applications like VoIP. The majority of this latency is caused by scanning all the WLAN channels while trying to search for an alternate AP. Several techniques have been discussed. The addition of wireless interfaces eliminates most of the unnecessary scanning latency. However, it is not a feasible solution for clients due to power constraints. It also results in interference between beacons, probe request/response packets during ongoing data transmission. Selective scanning and first-fit/best-fit algorithms provide the best results without having the client to compromise with packet collisions in densely deployed networks.

The introduction of 802.11r based techniques greatly helps in resource reservation of clients before losing connection with the current AP. It facilitates the transfer of security keys and other session information between the APs which reduces authentication and reassociation delays. Location data of a moving client provides an advantage by determining the next best APs. It helps the client to send (re)association requests to selected APs only based on its current location and resource availability of nearby APs. A blend of IEEE 802.11r with other standards, for example, IEEE 802.11k for radio resource measurement and IEEE 802.11e standard for QoS support proves to be a decent improvement for dealing with roaming capabilities in centralized WLANs.

In future work, investigating different ways to trigger the AP discovery process might prove important. For bigger networks with too many devices, it is necessary to emphasize on avoiding packet collisions and continuously switching channels to track nearby APs. A Metric Programming Interface component tracking the historical data of active channels, training the data and making decisions in real-time based on patterns can help in deciding when to start the AP discovery. This information can be combined with location data of client devices tracked by the AP, which can further help in deciding the right time to maneuver the clients to selected nearby APs.

Bibliography

[1] I. Mavridis, A.-I. Androulakis, A. Halkias, and P. Mylonas, “Real-life paradigms of wireless network security attacks,” pp. 112 – 116, 11 2011. ix, 9

[2] L. Dóra, “Wifi security – wep and 802.11i,” ix, 12

[3] S. Jin, M. Choi, L. Wang, and S. Choi, “Fast scanning schemes for ieee 802.11 wlans in virtual ap environments,” *Computer Networks*, vol. 55, pp. 2520–2533, 07 2011. ix, 16, 33

[4] I. Ramani and S. Savage, “Syncscan: practical fast handoff for 802.11 infrastructure networks,” in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 1, pp. 675–684 vol. 1, March 2005. ix, 18

[5] S. Jin, M. Choi, and S. Choi, “Multiple wnic-based handoff in ieee 802.11 wlans,” *IEEE Communications Letters*, vol. 13, pp. 752–754, October 2009. ix, 20, 21, 25, 33

[6] K. Ramachandran, S. Rangarajan, and J. C. Lin, “Make-before-break mac layer handoff in 802.11 wireless networks,” in *IEEE International Conference on Communications*, vol. 10, pp. 4818–4823, June 2006. ix, 23, 24, 25, 31, 33

[7] S. Waharte, K. Ritzenthaler, and R. Boutaba, “Selective active scanning for fast handoff in wlan using sensor networks,” in *Mobile and Wireless Communication Networks* (E. M. Belding-Royer, K. Al Agha, and G. Pujolle, eds.), pp. 59–70, 2005. ix, 26, 27, 33

[8] A. Srivastav, "https://amiyasrivastava.weebly.com/wireless/fast-transition-in-a-nutshell." ix, 37, 38

[9] "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements," *IEEE Std 802.11i-2004*, pp. 1–190, July. 10

[10] Seongkwan Kim, Sunghyun Choi, Se-kyu Park, Jaehwan Lee, and Sungmann Kim, "An empirical measurements-based analysis of public wlan handoff operations," in *1st International Conference on Communication Systems Software Middleware*, pp. 1–6, Jan 2006. 15

[11] F. Albinali, P. Boddupalli, and N. Davies, "An inter-access point handoff mechanism for wireless network management: The sabino system," in *International Conference on Wireless Networks*, 2003. 17

[12] H. Velayos, G. Karlsson, T. imit-lcn R, H. Velayos, and G. Karlsson, "Techniques to reduce ieee 802.11b mac layer handover time," tech. rep., ISSN 1651-7717, 2003. 19, 20

[13] P. Bahl and V. N. Padmanabhan, "Radar: an in-building rf-based user location and tracking system," in *Proceedings IEEE INFOCOM*, vol. 2, pp. 775–784 vol.2, March 2000. 19

[14] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2007*, pp. 1–1076, June. 21, 33

[15] L. Sequeira, J. L. de la Cruz, J. Ruiz-Mas, J. Saldana, J. Fernandez-Navajas, and J. Almodovar, "Building an sdn enterprise wlan based on virtual aps," *IEEE Communications Letters*, vol. 21, pp. 374–377, Feb 2017. 22, 25, 33

[16] J.-P. Jeong, Y. D. Park, and Y.-J. Suh, "An efficient channel scanning scheme with dual-interfaces for seamless handoff in ieee 802.11 wlans," *IEEE Communications Letters*, vol. 22, pp. 169–172, 2018. 22

[17] P. Bahl, A. Adya, J. Padhye, and A. Wolman, "Reconsidering wireless systems with multiple radios," *SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 39–46, Oct. 2004. 24, 33

[18] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 535–547, March 2000. 24, 25, 33

[19] J. B. Ernst, S. C. Kremer, and J. J. P. C. Rodrigues, "A wi-fi simulation model which supports channel scanning across multiple non-overlapping channels in ns3," in *IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 268–275, May 2014. 27

[20] S. Bangolae, C. Bell, and E. Qi, "Performance study of fast bss transition using ieee 802.11r," in *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, IWCMC '06, pp. 737–742, ACM. 28

[21] G. Castignani, A. Blanc, A. Lampropulos, and N. Montavont, "Urban 802.11 community networks for mobile users: Current deployments and prospectives," *Mobile Networks and Applications*, vol. 17, 12 2012. 28, 33

[22] L. Hao, B. Ng, and Y. Qu, "Self-optimizing scanning parameters for seamless handover in ieee 802.11 wlan," pp. 335–342, 10 2018. 29, 33

[23] "IEEE Standard for Local and metropolitan area networks–Part 21: Media Independent Services Framework," *IEEE Std 802.21-2017*, pp. 1–314, April 2017. 29

[24] "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band," *IEEE Std 802.11b-1999*, pp. 1–96, Jan 2000. 29

[25] I. Kim and Y. Kim, "Prediction-based smart channel scanning with minimized service disruption for ieee 802.11e wlan," *IEEE Transactions on Consumer Electronics*, vol. 57, pp. 386–394, May 2011. 30

[26] A. Mishra, M. Shin, and W. A. Arbaush, "Context caching using neighbor graphs for fast handoffs in a wireless network," in *IEEE INFOCOM*, vol. 1, p. 361, March 2004. 30, 32

[27] Y. Chen, M. Chuang, and C. Chen, "Deucescan: Deuce-based fast handoff scheme in ieee 802.11 wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 1126–1141, March 2008. 30, 32

[28] J. Yeo, S. Banerjee, and A. Agrawala, "Measuring traffic on the wireless medium: Experience and pitfalls," tech. rep., 2002. 31

[29] M. Almulla, Y. Wang, A. Boukerche, and Z. Zhang, "Design of a fast location-based handoff scheme for ieee 802.11 vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 3853–3866, Oct 2014. 31

[30] A. Arcia-Moret, L. Molina, N. Montavont, G. Castignani, and A. Blanc, "Access point discovery in 802.11 networks," in *IFIP Wireless Days (WD)*, pp. 1–6, Nov 2014. 32

[31] S. Yoon, S. Hong, J. Song, S. S. Lee, and S. Kim, “Seamless and secure service framework using multiple network interface terminal,” in *IEEE International Conference on Consumer Electronics (ICCE)*, pp. 261–262, Jan 2011. 33

[32] C. Yu, M. Pan, and S. Wang, “Adaptive neighbor caching for fast bss transition using ieee 802.11k neighbor report,” in *IEEE International Symposium on Parallel and Distributed Processing with Applications*, pp. 353–360, Dec 2008. 33

[33] Hyun Chul Lee, Kyung Tae Kim, Hee Yong Youn, and Ohyoung Song, “An efficient ap channel scanning scheme for real-time streaming over wlan,” in *8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 558–563, March 2010. 33

[34] J. Jeong, Y. D. Park, and Y. Suh, “An efficient channel scanning scheme with dual-interfaces for seamless handoff in ieee 802.11 wlans,” *IEEE Communications Letters*, vol. 22, pp. 169–172, Jan 2018. 33

[35] H. Wu, K. Tan, Y. Zhang, and Q. Zhang, “Proactive scan: Fast handoff with smart triggers for 802.11 wireless lan,” in *IEEE INFOCOM - 26th IEEE International Conference on Computer Communications*, pp. 749–757, 2007. 33

[36] D. H. Kim, Y. Kim, D. Estrin, and M. B. Srivastava, “Sensloc: Sensing everyday places and paths using less energy,” in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pp. 43–56, ACM, 2010. 33

[37] K. Khan and J. Rehana, “Wireless handoff optimization: A comparison of ieee 802.11r and hokey,” vol. 6164, pp. 118–131, 06 2010. 36

[38] K.-H. Chi, C.-C. Tseng, and Y.-H. Tsai, “Fast handoff among ieee 802.11r mobility domains,” *J. Inf. Sci. Eng.*, vol. 26, pp. 1345–1362, 07 2010. 38

[39] H. Hwang and Y. Kim, “Enhanced fast bss transition on enterprise wlan with sdn-based distribution system,” in *13th International Conference on Network and Service Management (CNSM)*, pp. 1–5, Nov 2017. 39, 40

[40] A. R. Rebai, M. F. Rebai, H. M. Alnuweiri, and S. Hanafi, “An enhanced heuristic technique for ap selection in 802.11 handoff procedure,” in *17th International Conference on Telecommunications*, pp. 576–580, April 2010. 40

[41] Sangheon Pack, Hakyung Jung, Taekyoung Kwon, and Yanghee Choi, “A selective neighbor caching scheme for fast handoff in ieee 802.11 wireless networks,” in *IEEE International Conference on Communications. ICC*, vol. 5, pp. 3599–3603 Vol. 5, May 2005. 41

[42] L. Yang, P. Zerfos, and E. Sadot, “Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP).” RFC 4118, June 2005. 41

[43] C. Huang and J. Li, “A context transfer mechanism for ieee 802.11r in the centralized wireless lan architecture,” in *22nd International Conference on Advanced Information Networking and Applications*, pp. 257–263, March 2008. 41

[44] “Control and provisioning of wireless access points (capwap) protocol specification.” 41

[45] Chun-Ting Chou and K. G. Shin, “An enhanced inter-access point protocol for uniform intra and intersubnet handoffs,” *IEEE Transactions on Mobile Computing*, vol. 4, pp. 321–334, July 2005. 41