Mechanisms of reducing reauthetication delay on IEEE 802.11 WLANs

Juha Kaskenmki
Helsinki University of Technology
juha.kaskenmaki@tkk.fi

Abstract

In this paper, we present of mechanisms for reducing reauthentication delay in Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Networks (WLAN). We survey some common reauthentication methods e.g. 802.11r and ERP and we compare the methods' efficiency. The focus is in managed networks, where client authenticate by the default to a remote Authentication, Authorization, Accounting server (AAA-server).

In reauthentication the client and AAA-server change information and after that the AAA-server recognise the client and AP which it is in registered. After the registration the client's Internet Protocol (IP) address might be change and the users open sessions is closed and the sessions have to build up again. If we can change reauthentication such as we don't need to rebuild sessions, then we get efficiency WLAN.

KEYWORDS: WLAN, IEEE 802.11, Reauthetication, Authentication, Authorization, Accounting, Key-exchange.

1 Introduction

In some public buildings and area we have WLANs, which can be used by the customers. The WLAN may have been restricted that only customers can use it. The network consist of many APs that cover the whole area as shown in figure 1. When the client moves to one AP area to the other APs area a device have to do handover. In handover the device moved from current AP area to the other APs' area. In the handover the device and AAA-server exchange the messages that grant that the device is allow to use the network. The user can't use the network while the client and AAA-server exchange the status messages.

In the messages exchange both parties negotiate network parameters. After that the network regocnize the client which have moved under the other AP's area. After the regocnize the client can use the network. The handover porcedure should perform when the client's signal strength is too low. The signal strength affect the bandwidth, whith low signal strength you can get sufficiency network bandwhith. Users require bandwith for real time network applications e.g. Voice Over IP (VoIP).

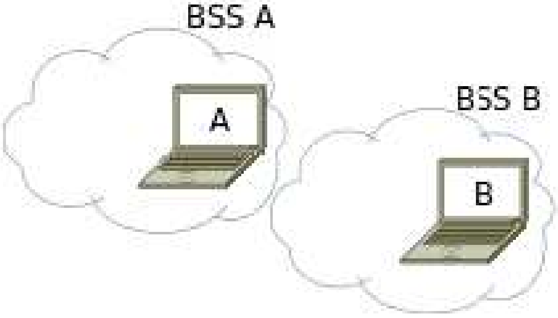

Figure 1: Handover

In real time applications user might notice when the handover procedure is performed. In voice or video services the user detects the packets loss when suddenly the voice or picture disappear for a little time. The packet loss might cause start of the handover procedure and reauthentication.The reauthentication procedure cause that the network session is closed and the session must be rebuild. The real time applications are sensitive to packet loss because it carry the time critical data. Human ear notice if the loss of voice data is more than 50ms and people don't accept these kind of interreupts in real time applications.

The packet loss is critical in the real time applications other network traffic isn't so ciritcal. Other network traffic e.g. web-traffic, users can't notice if the web page open in 50ms slower. Usually these time critical traffic is priorized so they get better quoality of service. In this paper we concentrate to survay the reauthentication procedure. We introduce the known standards and the solutions for reducing the reauthentication delay.

2 IEEE 802.11-2007

The IEEE 802.11-2007 standard family introduces the basic methods in wireless networks. The standard specify the mechenism for Medium Access Control (MAC) and Physical Layer (PHY) specification for IEEE 802.11 WLANs. This also specify the methdos for the moving station within wireless local area. The Preauthentication is developed to manage moving stations. This method is specify in IEEE 802.11-2007 standard family. In Preauthentication the device decide while it is assoisated in AP that what is the next AP to assosiate. In this method we get faster handovers in wireless network. The problem in preauthentication is that the station have to forecst the users movement and chose the best AP for the users new position.

In follow we introduce the basic handover procedure in

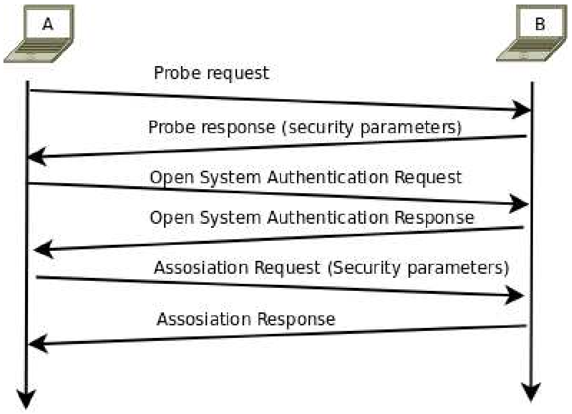
A
B
Probe request
Probe response (security parameters)
Open System Authentication Request
Open System Authentication Response
Assosiation Request (Security parameters)
Assosiation Response

Figure 2: Messages exchange in association

IEEE 802.11 WLAN. The handover scenario is introduce in figure 1 [1]. In handover the station change from the current Basic Service Set (BSS) to another BSS. In figure 1. station A have low singnal strength and have to do handover to the BSS B. First it have to scan all WLAN channels to find another AP which have better signal strength. In this example the AP to assosiate is BSS B's AP. In figure 2[7] is shows the message exchange in assosiation procedure. During these message exchange the station and AP establish the OSI (Open Systems Interconnection) layer 2 connectivity. After the assosiation the station and the AP is interconnected to the Distribution System (DS). The DS is the system where stations and APs are listed and we can perform the queue which AP is serving station A? The DS is basic network infrasturcture e.g. Local Area Network (LAN) or Wide Area Network (WAN).

After the association the station and AP have knowledge of others and now station have to authenticate whit the network authentication server. In authentication the station exchange the keys whit the authentication server. In the follow we introduce authentication mechanism the IEEE standard 802.1X, which is called Port-based network access controll.

3 IEEE 802.1X

This standart introduce mechanism to control the network access based on port. In wireless networks the authentication is based on locical port. The Port-based network access control performed methods to authenticate and authorized client to use the network. The client is authorized on authentication by the AAA-server e.g. Remote Authentication Dial In User Service (RADIUS) or other authentication server. The users database is located in AAA-server and the server authorized the user to use the network. In follow we introduce the Port-based authentication mechanism.

3.1 Port-based network access control

In port-based network access control the individual switch port or AP locical port can be authorized or unauthorized. This decision is made by authentication server and it is based on the users credentials e.g. username and password. The authentication server accept all users to use only 802.1x traffic before they have authenticate on the server. After the authentication the port is authorized state and the user is authorized to use network. The port is closed when the user send logoff message to authentication server to move the port to the unauthorized state.

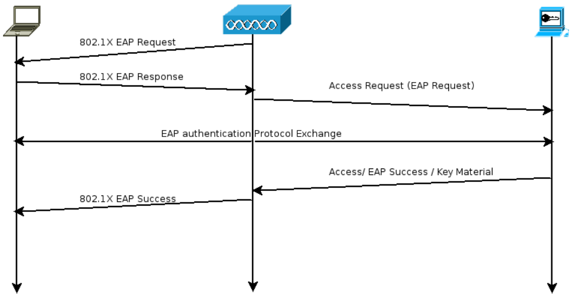
802.1X EAP Request
802.1X EAP Response
Access Request (EAP Request)
EAP authentication Protocol Exchange
Access/ EAP Success / Key Material
802.1X EAP Success

Figure 3: IEEE 802.1X authentication

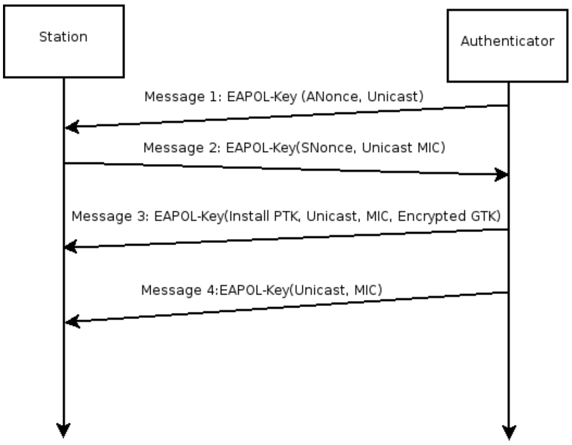
Station
Authenticator
Message 1: EAPOL-Key (ANonce, Unicast)
Message 2: EAPOL-Key(SNonce, Unicast MIC)
Message 3: EAPOL-Key(Install PTK, Unicast, MIC, Encrypted GTK)
Message 4:EAPOL-Key(Unicast, MIC)

Figure 4: 4-Way Handsahke

In figure 3. introduced the message exchange in 802.1X. In 802.1X the authentication starts when the authenticator send the 802.1X EAP Request. The 802.1X messages is delivered to the authentication server via AP's uncontrolled port. After the 4-way handshake the parties have authenticate each other and the port is in authorzed state. The 4-way handshake is introduced in figure 4. After the authentication the station is allowed to use the network via the authorized locical port. The authentication is made by the Extensible Authentication Protocol (EAP) and this standard provide the mechanism to deliver the EAP authentication messages. EAP authentication messages are delivered by the EAP Over LAN (EAPOL) protocol. This is the packeting technique which deliver the authentication and authorized keyes between station and authentication server.

The 802.1X standard provides port based connection in 802.11 WLAN. The port based connection is faster to rebuild after the handover. The session keys are nogotiate and the parties knows the locigal port to communicate. The authentication is done in AP on the border of the network. The authentication traffic is delivered from AP to the AAA-server, the station can't access to the network before the authentication is performed.

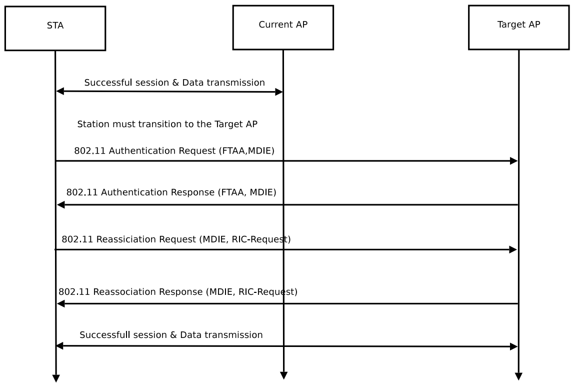
STA
Current AP
Target AP
Successful session & Data transmission
Station must transition to the Target AP
802.11 Authentication Request (FTAA,MDIE)
802.11 Authentication Response (FTAA, MDIE)
802.11 Reassiciation Request (MDIE, RIC-Request)
802.11 Reassociation Response (MDIE, RIC-Request)
Successfull session & Data transmission

Figure 5: FT handover procedure

The advantace based on hadover is that "Controlled Ports remain authorized during reauthentication and transition to the unauthorized state only if reauthentication fails" [2]. So we don't need to authenticate the port after the handover. This feature reduce the sended messages in session rebuild procedure. In key managemant the key expiration time can be fixed. After the time expired and the session expired the session have to rebuild. We can reducing the expired time so the need of the reauthentication procedure reduce. The draw back is the network security, becuse attacker can use the open sessions. The choice between network security and fast handover have to think carefully.

4 IEEE 802.11r

This standard introduce the mechanism to handle the handoffs in wireless networks. Standard IEEE 802.11r reduce the numbers of messages to send on the handoff procedure. IEEE 802.11r support secure key negotiation and continous connectivity to the network. The mechanism wich enable the fast handover is Fast Basic Service Set (BSS) Transition (FT). This method helps real time applications e.g. VoIP to quick handovers in wireless network. The real time applications network traffic can be consider to all the time critical network traffic. In quick handover the packet loss is smaller so the user might not noticed the network packet loss. In follow we introduce the Fast Basic Service Set Transition.

4.1 Fast Basic Service Set Transition

Fast Basic Service Set Transition is secure key negotiation protocol which allow continous network connectivity for the users. The device negotiate secret key with the authentication server. "The FT protocols are part of the reassociation service and only apply to STA transitions between APs within the same mobility domain within the same ESS.". [3] The mobility domain cover the APs which are connected on the same LAN switch. The reason for the fast handoffs is the way that FT cached the session keys in network. The session keys can be regenerate by the cached keys. The key negotiation is introduced in figure 5.

The key negotiation is similar to earlier introduced 802.11. In 802.1r there is two messages which enables the fast key generation in handover procedure. Whit these keys it can be regenerate the session keys. In 802.11r have two way to perform the handover. The handover can be make Over-The-Air or Over-The-DS. The difference in these two methods are the way the station communicate with the AP. In Over-The-Air the station communicate straight to the target AP and Over-The-DS the AP communicate whit target AP via current AP. The Over-The-DS LAN network is used to exchanging the keyes.

5 EAP

The EAP provides framework for user authentication. "EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP." [4]. In EAP framework it have some common key negotation mechanisms for the specific authentication methods to establish connection. In EAP the authentication is based on key negotations. The peer and authentication server exchange the Master Session Key (MSK) to establish secure chanell for the communication. The EAP provide the mechanism to deliver the MSK between the authenticator and peer. The number of the packets that have to send to establish the chanell for the communicatiosn is critical. In EAP handover the parties exchange the same numbers of packets to built up the communication channel. If in the re-authentication the partis send less packets, the handover time is smaler and the re-authentication is efficient. Here we can assume that the network is ideal and haven't packets loss. If the packet loss is high the messages exchange take more time to execute. To redeuce the sended packets in authentication there is inroduced the EAP extension called EAP Re-authentication Protocol (ERP).

EAP framework introduces the re-authentication protocol ERP, whitch try to reduce the number of sended packets in handover procedure that means reducing the handover time. It is certain if we can reduce the number of packetes that is needed to send to do the handover. In the same time we reduce the handover time so possible user don't notice the connection closed caused by the handover procedure. ERP uses the previously performed EAP authentication key material to do the fast reauthentication.

The reauthentication messages exchange start when the authenticator send the EAP-Initiate/Re-auth-Start message and start to wait the response. Now the peer can start the ERP exchange to send EAP-Initiate/Re-auth start message. After the authenticator get this message it start EAP authentication procedure. The authenticator send this message to the authentication server e.g. RADIUS (Remote Authentication Dial-In User Service). The RADIUS server is centralized user account database. The server verify the message and send reauthentication MSK (rMSK). The server rMSK add in to the EAP-Finish/Re-auth message and send it to the peer. The peer verify the message and after the verification it is ready to start authentication procedure.

6 Summary

The delay of reauthentication delay consist of packets which is send between peer, authenticator and authentication server. In non-theoratic networks there are packet loss and delays. These bring more delays on handover procedure. In reauthentication the network connection is closed and there is hurry to rebuilt it. The optimal reauthentication mechanism do the authentication in such way that user can't notice handover procedure. In handover procedure how the statoin choosing the next possible AP to assosiate whit is critical for the good handover procedure. Making the dicisions for next possible AP to assosiate with have to concern the station movements. In these mechanism we can't allways get the best possible AP to assosiate with because the staion can't predict where the user might to want to go. In predicting where the user want to go we need other solution.

The 802.1x gather the users sessions in one piece. This helps to rebuild the sessions after the handover procedure. This is the advantege of the IEEE 802.1x standard. The IEEE 802.1x help only to do user authentication whit the AAA-server. This is good protocol to control the access to network and it's good ground to build up the system which perform fast handovers. In fast handover network this standard cover only authentication and packet of sessions. The other service need to build up above this standard.

In the 802.11r finding the AP to assosiate with have two ways, over-the-air or over-the-ds. The method efficiency for the fast handover is based on the network infrastructure. It depends on the situation in network is it faster to communicate via DS or straght to the target AP. In Over-The-DS communications the delay can perform in concestion in LAN. The advantage of IEEE 802.11r is that it supports two mechanism to find the next AP to assosiate with. The media can be choose for the assosiation communications which is advantage if the other media have congestion so we can use the other media to assosiate. The session keys regeneration is the similar than other this kind of protocols e.g. EAP ERP. In next chapter we summarize the ERP benefits.

In the session key regeneration mechanism e.g. EAP ERP the session key is regenerated from the earlyer exchange keys. These keys are exchanged during the firs initial connection. The duration of the exchange of the few messages is not significant so the first initial negotiate doesn't get too long. The benefit of the these keys are significant because the station doesn't need to exchange the messages between the AAA-server only regenerate the session key and open the connection between the station and AP.

7 References

[1] IEEE 802.11-2007 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements. June 12 2007.

[2] IEEE 802.1X IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control. December 13 2004.

[3] 802.11r-2008 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 2: fast basic service set (bss). July 15 2008.

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz. "Extensible Authentication Protocol (EAP)". RFC 3748. June 2004.

[X] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz. "Extensible Authentication Protocol (EAP)". RFC 3748. June 2004.

[X] V. Narayanan and L. Dondeti. "EAP Extensions for EAP Re-authentication Protocol (ERP)". Qualcomm, Inc. RFC5296. August 2008.

[X] T. Clancy, M. Nakhjiri, V. Narayanan and L. Dondeti. "Handover Key Management and Re-Authentication Problem Statement". RFC 5169. March 2008.

[X] Uri Blumenthal, Milind M. Buddhikot, Juan A. Garay, Scott C. Miller, Sarvar Patel, Luca Salgarelli, and Dorothy Stanley. A "Scheme for Authentication and Dynamic Key Exchange in Wireless Networks". Wiley Periodicals, Inc. 2 Dec 2002.

[X] Roger M. Needham, Michael D. Schroeder. "Using Encryption for Authentication in Large Networks of Computers". May 1978.