Seamless Handover in Networks Based on IEEE 802.11 Standard

Ján Balažia*
Institute of Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 2, 842 16 Bratislava, Slovakia
jan.balazia@stuba.sk

Abstract

In recent years we have seen tremendous growth in the use of various multimedia services, either in terms of highres video, targeting realtime broadcasting or voice services that use IP protocol based networks. At the same time, small portable computers and tablets entered the market in big fashion and mobile phones became a fullyfledged replacement of computers on the road. With the rising number of mobile devices sold, the demand for these kind of services keeping the mobility of client grows enormously. This is the fundamental issue of IEEE 802.11 networks that are already part of every mobile device sold: the time needed to reassociate with access points is 50 milliseconds at best. Multimedia services using voice, however, for their smooth transmission have a maximum margin of tolerance at 40 to 50 milliseconds, which makes networks based on the IEEE 802.11 standard hardly usable.

The aim of this work was to propose an architecture and protocol support necessary to achieve the beforementioned transition in negligible time in order to eliminate problems connected to transmission of multimedia services and at the same time make it unnecessary in any way to interfere with the software and hardware of existing mobile stations. The proposal was verified on existing hardware in laboratory environment and test results confirmed the correctness of the architecture design proposal.

Categories and Subject Descriptors

C.2.1 [**Computer-communication networks**]: Network Architecture and Design; C.2.3 [**Computer-communication networks**]: Network Operations—*network management, network monitoring*

Keywords

802.11, seamless handover, handover latency, remote MAC separator, network architecture, network management

1. Introduction

This work was originally inspired by mobile 3GPP architecture, where mobile users has access to multimedia services even while being on the move[1]. However, mobile networks have great advantage in crompare with networks based on 802.11 standard. These networks are allowed to have more associations at a time. By this possibility the handover is quick enough, so the user us unable to experience unpleasant disruptions by watching live video call or having a VoIP session while traveling in a train or in a car. In compare, 802.11 standard strictly defines single association at a time [2]. As a result, the mobile station (MS) has to pass each time while reassociating via three phases defined by 802.11: Detection phase, Selection phase and Execution phase [3]. All these phases are connected with delays that end up in the best case scenarios with approximately 50ms interruption (while using 802.11r standard). According to authors [4],[5] the maximal tolerance for disruption of voice services is between 40 to 50 milliseconds, which is even for latest standards hardly reachable. To be able to explain problem in more detail we will define before-mentioned handover phases.

The detection phase starts in mobile station in given time intervals and uses several techniques to detect the link quality. Once etc. the the level of RSSI reaches level of -80 dBm the station should go to the next phase, which is selection Phase [6]. However, there are several problems connected with this decision. What if the increase of RSSI was caused accidentally by a signal mirroring or by a temporary obstacle. When is actually the right time to switch to the next phase? There might be several more factors that could tell that the connection is starting to be problematic. Etc. the rapid throughput decrees or signal to noise ration decrease. Existing solutions will be discussed later.

Once the station decides that there is a right time to move forward, the Selection phase takes place. This phase is used for scanning for new Access Points (AP). We can say, that this phase is also one of the most time and energy

*Recommended by thesis supervisor: Assoc. Prof. Ivan Kotuliak.
Defended at Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava on August 25, 2016.

Balažia, J. Seamless Handover in Networks Based on IEEE 802.11 Standard. Information Sciences and Technologies Bulletin of the ACM Slovakia, Vol. 8, No. 2 (2016) 37-44

consuming. When the station start to search for new APs, it is unable to transport data any more. Therefore the search has to fit between data transportation gaps, which is of course decreasing throughput at a time. After finishing the search, the station needs to select a best AP in range. Again, there might be several variables that the equation might include. The first one is the Service Set Identifier (SSID) which is crucial to stay in the same network. If there are more APs with different Base Service Set Identifier (BSSID), the station selects one with the best service delivery (etc. QoS support, security settings, ..)[7].

After selection of a new AP the phase of realisation is in charge. In general, mobile networks use 802.11 security (802.11i) and QoS (802.11e) amendments as that are causing big delays due to necessary message exchange[8]. These delays are now in status quo caused by latest standardised amendment 802.11r that defined procedures for proactive security information exchange (in order to save time), while not defining protocols to be used. Therefore, most vendors implemented their proprietary solutions, which are incompatible, and amendment was implemented only by a big companys in their proprietary solutions [9][10][11].

2. State of the Art

The main focus of our work is to bring a seamless handover to MSs while roaming the network (in infrastructure mode) within one Extended Service Set (ESS). This set covers Distributed System (DS) compound from more Basic Service Sets (BSS) which represents APs[12]. Within the communication with AP over 802.11, MS uses frames belonging to these three categories:

- Data frames - these frames are used for data communication on L2 and use LLC and SNAP headers to address frames.
- Control frames - frames used on medium to directs MSs to use medium only within the assigned time slot via CTS, RTS and ACK messages.
- Management frames - frames used for management functions as association, handover, disassociation, channel switching, QoS management and so on[13].

In the first step, before MS can start to communicate, a successful association with BSS has to occur. This association is based on Service Set Identifier (SSID) that belongs to whole ESS. To get this parameter MS might passively listen on the medium, or use active scanning to get the information sooner. In exchange of successful network probe the MS receives network information like authentication method and the next process may start. After authentication frame exchange AP and MS exchanges their capabilities and MS may start to communicate over the channel. Once the MS decides to leave the de-authentication management frame is sent and MS may leave the medium. This process is shown on Figure 1 [8].

One of the most crucial part in our work is MS mobility. In nowadays networks the handover management is located within MS. The whole decision process starts periodically in MS (etc. each 500ms) and measures current RSSI, throughput, packet loss and other connection parameters as well as the parameters of neighbouring APs

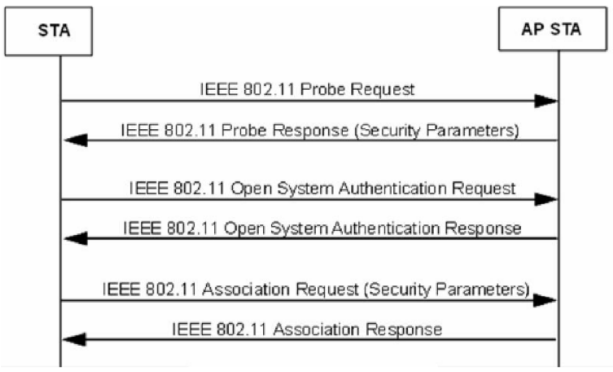

Figure 1: Authentication process.

(via active or passive scanning). Once the MS finds out that parameters of other AP are better, MS issues a handover process, starting with de-association from current AP and continuing with already explained association process (if there is not used 802.11r or 802.11i with key cashing explained later)[14].

To ensure better or quicker, handover several tweaks might be used within all handover phases described in following sections.

2.1 Discovery Phase

In the discovery phase preemptive search might be used instead of searching once MS decides that the current RSSI is not good enough[25]. This type of search might decrease a throughput by a little, because it is issued periodically, while still having connection with the present AP. Other drawback is that it is much more energy consuming to do scann proactively. Other approach is to not use active scanning, but passively listen on channels to save as much energy as possible [16]. On the other side the drawback is that the station might not receive all beacon messages from APs around in the time. The next method discussed is SyncScan [17], which is passive scanning method, trying to predict the time of beacon reception so the time waiting on each channel can be rapidly decreased. Other approach is to use 802.11k that advertises ordered list of alternative APs that the MS may use for future communication [18]. To avoid unnecessary handovers also some mathematical models are used as smoothening the RSSI data via Moving Average or Exponential Weighted Moving Average[16].

2.2 Selection Phase

The selection of appropriate AP selection mechanism is necessary. In general, there are solutions based on client, server or mixed solutions, all with the main aim to avoid something that is called ”jo-jo” effect. This effect is hoping between two or more neighbouring AP because ”better” connection parameters. As a result the communication is killed by non stop re-associations. For avoidance, several algorithms are used. The most basic algorithms issues the handover once the throughput is below the acceptance, so the chance to hop back is minimal. Extension to this algorithm is to use history, so if the throughput is decreasing in time the handover can be issued. Some algorithms also uses trends while observing other APs and making a correlation with current signal strength. The typical handover algorithms are based on signal strength and may use: best signal, thresholds, hysteresis or trends

and prediction; or by observing throughput and may use: load balancing, or 802.11k [16].

2.3 Realisation Phase

While speaking about handover, two types may occur: on second and third OSI layer. In our work we focus on the second layer and we are trying to solve following delays: radio signal changing, reauthentication, reassocation and QoS negotiation. This phase is one of the most important, because while the MS is in realisation phase the connection is lost. While being so important, most of the companies patented their solutions, or they are closed source and proprietary[9][10][11]. From those that are open we picked up 802.11f protocol that was used for communication between APs to proactively distribute MS security context, so the MS may spare some time with security negotiation. However, because authors did not define message exchange the implementation was vendor to vendor specific and the 802.11f amendment was later withdrawn[19]. The other solution in use is 802.11i with proactive key cashing. The advantage is that the AP stores already exchanged keys so once the MS visits the AP agin there is no need for extra negotiation[20]. The drawback is that the MS has to exchange the full 802.11i authentication while visiting new APs, which is actually the major case. Currently a best solution on the market is 802.11r that uses proactive key derives distributed to potential APs that MS may visit. As a result only 4 way handshake has to be performed between MS and AP. This process is aproximately 50ms long [21].

2.4 Experimental Solutions

This work was also inspired by three experimental works. The first one is Personal AP [22], which defines architecture of flying ghost APs following MS, so MS does not have to perform handover. This architecture is based on so called Split MAC separator approach. To explain it, IEEE defines three types of 802.11 networks:

- Local MAC separator based - the whole logic of an AP (radio, control and management) is located at Wireless Terminal Points (WTP). This is the most used approach in the 802.11 networks we know.
- Split MAC separator based - in this architecture the radio layer and the delay sensitive management and control functions are located at WTP (logical AP). The rest as QoS management, device configuration and load balancing are shifted to Access Controller (AC). As an example of integrator we may use Meru Networks Systems [10], or an experimental approach called Personal AP [22].
- Remote MAC separator based - solutions based on this architecture shift all the management and the control logic to the AC. WTP is used only as a radio controller and a bridge between wired and wireless medium. Our architecture proposal is based on this type of architecture as well as the proprietary solution of Aruba Networks Systems [9].

Second inspiring work is called D-Scan [23] and is focused on gathering data from AP dense area. Authors extracted useful data from 802.11 frames in the air to better observe current environment. The third and the last called Improving the latency of 802.11 hand-offs using neighbour

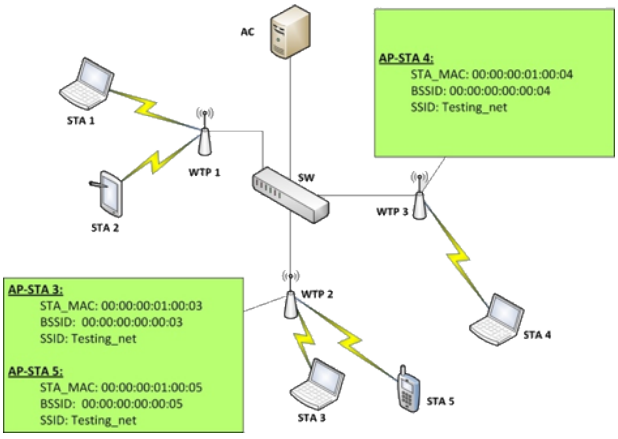

Figure 2: MS communicating via WTP2 before transition.

graphs [24] focused on graph creation, where edges represented useful paths between nodes that represented APs. This technique might be used for better predictions.

3. Open Problems

As a result of current environment overview we decided to look at the 802.11 network as a homogenous entity instead of looking on counterparts and solving their problems separately. Based on this we defined following open problems:

- New architecture proposal that allows MSs to perform seamless transition between different WTPs and that allows them to roam across the network without data loss that will affect multimedia services. The architecture is created with aim not to change any exiting client behaviour so current stations can seamlessly use services provided by this architecture.
- New protocol proposal that will support the network management and client handover.
- Algorithm that will support the client transition between different WTPs and that will allow them to roam seamlessly.

The proposed architecture will be verified on existing hardware and compared with generally used 802.11 solution.

4. Architecture Specification

According to open problems we defined entities that cooperates within our new architecture:

- Access Controller (AC): The distributed network core that coordinates vital functions of the whole network. By those functions we mean especially WTP coordination, user and service management and handover decision with the final execution.
- Access Point (AP): Each MS has dedicated AP created within AC. As the architecture is Remote MAC separator based the connection between AP and MS is mediated via WTP.

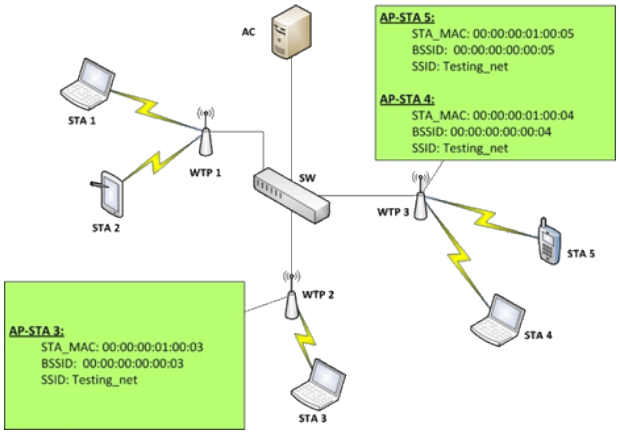

Figure 3: MS communicating via WTP3 after transition.

- Wireless Terminal Point (WTP): Physical device that spreads wireless signal and coordinates control messaging on a medium. All other 802.11 vital functions are shifted to the network core - AC.
- Mobile station (MS): User device that communicates towards its AP located in AC via WTP. This device is unaware of architecture type and is unable to see how the data are transferred towards its dedicated AP.

Figure 2 and Figure 3 shows, how is the communication established on L2 and how does the transition of MS between two WTPs looks like. The important thing is that whole AP related context is exactly same within whole ESS.

To be able to ensure this transition we have specified requirements for all network entities:

- AC - has to use communication protocol to talk to WTPs on the network, has to manage WTPs on the network, has to create logical APs and manage its context for all connected MSs on the network, has to analyse network and MS behaviour and based on gathered data make appropriate decisions, has to transport user data to the right destination.
- WTP - has to use communication protocol that talks to AC, has to bridge management and data frames between AC and MSs, has to implement control messaging for a wireless medium, has to implement the handover functionality, has to gather and send statistical information of connected client to the AC.

According to requirements we created proposal that covers required functionality. Each of following chapters deals with one exact part of the architecture proposal.

4.1 APMP Management Protocol

Access Point Management Protocol (APMP) is our proprietary solution that has one primary aim: to execute handover in minimal possible time. Therefore, none existing solution like CAPWAP[25] or OpenFlow[[13] is used. These will only extend the time that we need to shorten. Also, architecture use UDP to transport control messages

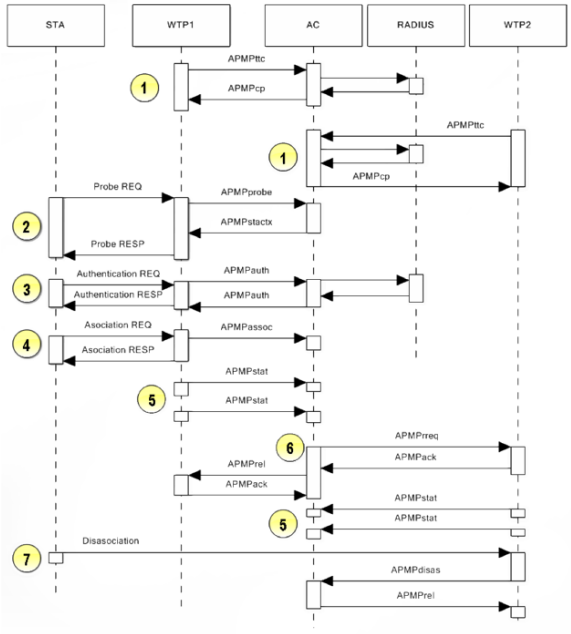

Figure 4: APMP state diagram.

and L2 extension is used to transport data frames (will be discussed in next chapter). APMP protocol consist from 1B long message ID followed by TLV fields: 1B used for type, 2B used for length and last value is long according to previous field.

This protocol defines seven basic processes that are vital for architecture functionality and are shown in Figure 4.

The description of processes is as follows:

1. Accepting new WTP: New WTP is accepted by AC after an exchange of APMPttc message (that might be verified with AAA server) and connected APMPcp reply message containing WTP parameters. Otherwise the communication is rejected by APMPrecreq and all the future messages are discarded until next successful authorisation. WTP has to send APMPkeepalive messages to hold active connection.
2. MS network discovery: The communication starts by forwarding MS Probe request forwards AC via APMPprobe message. In exchange, AC replies specific MS AP context via message APMPstactx. This context contains personalised BSSID, which will be used for future communication.
3. MS Authentication: Based on the context received, MS start authentication with AP via WTP. This WTP uses APMPauth message to forward the authentication frame to AC. The authentication might be validated via Radius server. Important is that the key derive used by MS for communication with AP is stored in the AC and is never propagated to WTP.
4. MS Association: After authentication MS exchanges association messages trough WTP and APMPassoc message. WTP immediately response so the MS may start to communicate.

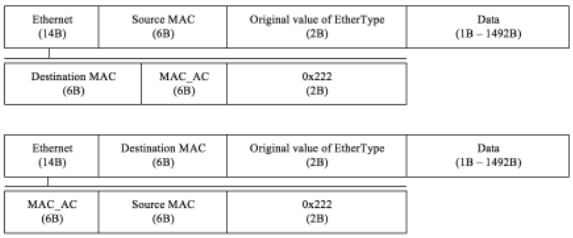

Figure 5: Data encapsulation frame from AC towards destination (top) and from source towards AC (bottom).

5. Statistics: Each WTP periodically collect and send MS statistics to AC via APMPstactx message. Aggregated information is parsed by AC and on its basis handover decision could be made.
6. Handover: Handover always originates in AC and is propagated via APMPrreq message. In the first step new WTP is informed. Once WTP decides to accept MS, it replies with APMPack message. Otherwise APMPrej message is sent. After successful reception by AC, old WTP is informed via APMPrel message to release the client. This message is agin confirmed by APMPack.
7. Disassociation: Once MS decides to leave the ESS a Disassociation frame is sent. This frame is forwarded to AC via APMPdisas message and AC replies with APMPrel.

4.2 APMP Management Protocol

The primary purpose for joining the wireless network is to send data towards destination. In compare with Local MAC separator based solution we have to make one more hop on L2 to be able to transport encrypted frame from MS to the logical AP located in AC. The frame has to be delivered to AC, because WTPs does not hold encryption keys so it is unable to understand data above L2 as same as no other device anywhere. According to 802.11 and 802.3 addressing schemes we had to encapsulate original destination address created by MS and replace it with the MAC address of AC so the frame can be processed decrypted and agin sent towards the proper destination. Again, if the destination is wireless client, AC has to encrypt the frame with the key of destination MS, replace the source address with the address of AC, encapsulate the original source and send it towards destination. For encapsulation we have created new ether type with value 0x2222 and the structure is shown in Figure 5.

As a side effect we had to lower the MTU from 1500 to 1942 which is having a small impact on data throughput evaluated in a Results chapter.

4.3 Access Controller

As we already defined management protocol and data communication, we can move on to describing processes within AC. The first and most important process is connected with MS behaviour starting with joining the network, moving across ESS and at the end leaving the network.

The lifecycle starts with a new MS starting with association process by Probe message or by resuming from sleep. Both options have to pass authentication and once it is finished MS may start to communicate.

Each station is afterwards observed by a statistics module. If this module tells that there is a better WTP, then AC amy start the handover process. The start is invoked by APMPrreq message sent towards new WTP. This step may finish in the successful handover (MS is accepted by WTP), or in case of failure AC will select next possible WTP to tray the handover again. After successful MS reception by WTP and AMPMack message, the old WTP is informed to flush the MS context and the circle may start again. If the AC do not get any statistical message with MS identifier for certain amount of time, MS context is automatically discarded and last known WTPs is informed to flush the MS context via APMPrel message.

The next important process is connected with gathering statistics used to decide wether to roam the MS or not. Each station is monitored right after successful association. After reception of a first APMPstat message MS is included calculations, otherwise the station is marked as expired and after certain amount of time is discarded. The same thing happens once the MS is not included in any statistic received from all connected WPTs. Once the AC finds out that the MS on current WTP is about to reach the RSSI threshold, the handover process is started and the station is market as in roaming progress until the successful roam or the failure. According to the result the list of potential WTPs per MS is recalculated.

4.4 Wireless Terminal Point

The role of WTP is to manage 802.11 physical layer and to bridge connection between MS and AC. The diagram of MS behaviour is easier in compare with AC and can be described as follows.

Association process of MS starts with sending Probe request (by MS) on the network with known ESSID. From now on, all WTPs that receives this message creates their own MS diagram. This Probe message is then redirected to AC via APMPprobe message and as a reply APMPstatctx is sent back to MS. This message contains MS context needed for creation of WTP interface that will be used for communication with the MS. After the reception the state is set to the active. Otherwise, APMPrej is sent to WTP (telling that MS is unable to join network) and status is set as rejected. The association is finished after exchanging APMPauth a APMPassoc messages and status is set to associated so the MS may start to transfer the data.

Next important scenario is the handover. As was mentioned before, the decision is made according to statistics exchanged via APMPstat messages. Once AC decides that it is a time to make handover APMPrreq message is sent towards a new WTP. If this WTP is capable to serve another client, associated state is set and APMPack message is sent back to AC. In exchange, previous WTP receives message APMPrel to releases the context of MS.

4.5 Results

Verification of proposed architecture was done in laboratory conditions on existing hardware using two Ubuntu based computers serving as WTP via our modified version of HostAPd[26]. As a hardware usb WiFi stick TP-Link TL-WN821N v3 with chip Atheros AR7010+AR9287

managed via nl80211 driver was used. AC was implement in C using native Linux network calls and lpthread library for threads management. As a MS Android, iOS, Windows XP and Windows 7, Mac and Linux based devices were used. The testing and evaluation software was IXIA IxChariot software with Wireshark and ping command. The topology is shown in Figure 8, where STA was roamed between two WTPs. On AC and on STA had IxChariot endpoints that were monitoring traffic passing via the test architecture.

The testing was executed on our remote MAC separator based architecture and on general local MAC provided by unmodified HostAPd in the same version. The test handover was issued manually by the AC at the specific time. Both WTPs had the same channel to produce some interference (in distance of several meters).

The testing scenarios were split in two cases: The first one was focused on ICMP response time and route while measuring which path was used to transport the ICMP packet from a source (MS) to a destination (AC). The second one was focused on a throughput, a data loss and a link reliability while transferring RTP stream from the MS to the AC while performing the handover.

The first test consisted from ICMP Echo message exchange between the MS and the AC and between the MS and both WTPs, while a packet filter was set to not forward ICMP between mediating WTPs. Results shown in Figure 6 tells that while using our proposed architecture the MS did not notice any outage. For comparison, while using local MAC separator based architecture a long gap in communication occurred, as is shown in Figure 7. In he graph a blue line represents the response from AC and a red and a green responses from the current WTP / APs. The X axis shows time and Y shows the number of packet transferred in the time interval.

In the graph showing our architecture the response time from WTP2 and AC decreased after handover, while the throughput raised. This effect was caused by shutting down a hardware interface on the WTP1 that was producing interference as both WTPs were communicationg on the same channel.

The second test measured an optimal throughput while using our proposed and the original architecture. We used IxChariot to generate TCP steam and results showed that our architecture had 2 Mbit/s slower throughput. This slowdown was caused by lowering the MTU needed by the extra header in data frames and by user space implementation of the data transport protocol.

Once we had optimal values of throughput for both architectures we generated RTP stream (via IxChariot) starting in MS and ending in AC. We measured delays and the data loss for both, while performing the handover. The handover was issued in the 15th second and we can clearly see the difference between our architecture in Figure 9 and original in Figure 10. Detailed statistics provided by the IxChariot shown that the gap in our architecture was 1,41ms long in comparison with 3,337s long cut in original local MAC separator based architecture.

Figure 6: ICMP message exchange in our proposed architecture.

Figure 7: ICMP message exchange in original architecture.

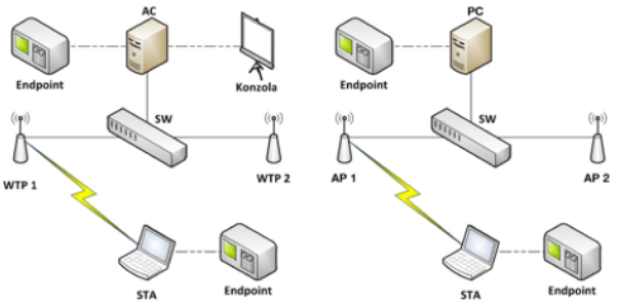

Figure 8: Testbed topology of our proposed architecture (left) and the original (right).

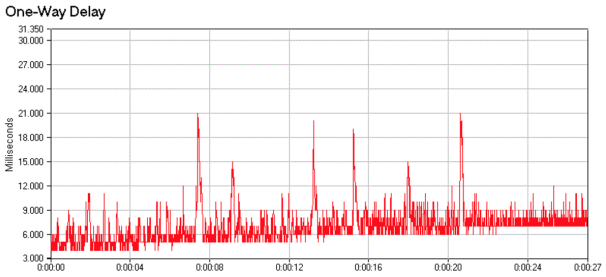

Figure 9: One-way delay test in our architecture.

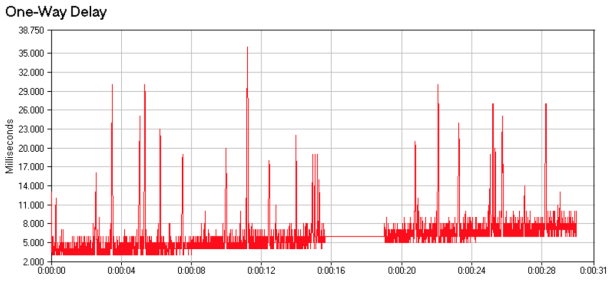

Figure 10: One-way delay test in original architecture.

5. Conclusions

We have proposed a centralised IEEE 802.11 architecture based on Remote MAC separator with the main goal to reduce all unnecessary delays associated to handover process. The reduction was done by shifting the handover logic away from mobile station and placing it the network core. Our tests confirmed that the architecture proposal was correct and that the existing 50ms handover status QOU can be easily lowered while not breaking any existing IEEE standards. The drawback of this proposal is the enlargement of Ethernet headers which may bring a little throughput slowdown that we measured as 2Mbit/s.

Acknowledgements. This work was partially supported by the Scientific Grant Agency of Slovak Republic, grant No. VEGA 1/0836/16.

References

[1] K. Ahmavaara, H. Haverinen, and R. Pichna. Interworking architecture between 3GPP and WLAN systems. IEEE Communications Magazine, Vol. 41, pages 74âĂŞ81, Nov. 2003.

[2] IEEE Standard for Information technology. art 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://standards.ieee.org/getieee802/download/802.11-2012.pdf, Marec 2012

[3] Kashif Nizam Khan, Jinat Rehana. Wireless Handoff Optimization: A Comparison of IEEE 802.11r and HOKEY. https://hal.inria.fr/hal-01056504/document, 2014

[4] I.F. Akyildiz, J. Xie, and S. Mohanty. A survey of mobility management in next-generation all-IP-based wireless systems. In Wireless Communications, IEEE (See also IEEE Personal Communications), pages 16-28, August 2004.

[5] Tim Szigeti, Christina Hattingh. Quality of Service Design Overview. Cisco Press, http://www.ciscopress.com/articles/article.asp?p=357102&rl=1, December 2004

[6] Ali Safa Sadiq, Kamalrulnizam Abu Bakar, Kayhan Zrar Ghafoor, and Alberto J. Gonzalez. Mobility and Signal Strength-Aware Handover Decision in Mobile IPv6 based Wireless LAN. http://www.iaeng.org/publication/IMECS2011/IMECS2011_pp664-669.pdf, 2011

[7] Microsoft. How 802.11 Wireless Works. http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx, March 2003

[8] Intel Corporation. Understanding IEEE* 802.11 Authentication and Association for Network and I O. http://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000006508.html

[9] Aruba Networks. http://www.arubanetworks.com/.

[10] Meru Networks. http://www.fortinet.com/meru/

[11] Cisco Systems. http://www.cisco.com/

[12] Cisco Systems Wireless LANs: Extending the Reach of a LAN. http://www.ciscopress.com/articles/article.asp?p=1156068&seq Num=4, 2008

[13] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J. OpenFlow: Enabling Innovation in Campus Networks. http://archive.openflow.org/documents/openflow-wp-latest.pdf, 2008.

[14] Anthony Noerpel and Yi-Bing Lin. Handover Management for a PCS NetworkâĂİ, IEEE personal communications. http://ieeexplore.ieee.org/iel4/98/13833/00637379.pdf?arnumber=637379, December 1997.

[15] Pejman Roshan and Jonathan Leary. 802.11 Wireless LAN Fundamentals. 1st Edition, http://docstore.mik.ua/cisco/pdf/other/Cisco%20Press,%20802.11%20Wireless%20Lan%20Fundamentals%20(2003)%20Kb.pdf, December 2003

[16] Vivek Mhatre and Konstantina Papagiannaki. Using Smart Triggers for Improved User Performance in 802.11 Wireless Networks. MobiSys'06, Uppsala, Sweden, http://portal.acm.org/citation.cfm?id=1134706&dl=ACM&coll=&CFID=15151515&CFTOKEN=6184618, June 2006

[17] Ishwar Ramani and Stefan Savage. SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. http://www.cs.ucsd.edu/ savage/papers/Infocom05.pdf, 2005.

[18] IEEE Standard for Information technology. 802.11k-2008 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4544755&filter=AND(p_Publication_Number:4544752), June 2008

[19] IEEE Computer Society. IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11TM Operation. http://standards.ieee.org/getieee802/download/802.11F-2003.pdf, 2003

[20] Benjamin Miller. Is it the network Solving VoIP Problems on a Wireless LAN. http://www.users.miamioh.edu/roseaw/cit286/WP_Miller_VoIP_LAN.pdf, 2007.

[21] KUANG-HUI CHI, CHIEN-CHAO TSENG AND YA-HSUAN TSAI. Fast Handoff among IEEE 802.11r Mobility Domains. http://www.iis.sinica.edu.tw/page/jise/2010/201007_12.pdf, 2010.

[22] Lei Zan, Jidong Wang and Lichun Bao. Personal AP Protocol for Mobility Management in IEEE 802.11 Systems. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1541021&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1541021, 2005.

[23] Jin Teng, Changqing Xu, Weijia Jia, Dong Xuan D-Scan: Enabling Fast and Smooth Handoffs in AP-dense 802.11 Wireless Networks. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5062198&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5061887%2F5061888%2F05062198.pdf%3Farnumber%3D5062198, 2009.

[24] Minho Shin, Arunesh Mishra, William A. Arbaugh. Improving the Latency of 802.11 Hand-offs using Neighbour Graphs. https://www.usenix.org/legacy/publications/library/proceedings/mobisys04/pdf/p70-shin.pdf, 2004.

[25] Internet Engineering Task Force. Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP). https://tools.ietf.org/html/rfc4118, July 2004.

[26] Hostapd and wpa_supplicant. https://w1.fi/

Selected Papers by the Author

J. Balažia, I. Kotuliak. Seamless handover in 802.11networks. In *Proc. of 2012 5th Joint IFIP Wireless and Mobile Networking Conf.*, Bratislava, Slovakia, September, 2012.

J. Balažia, R. Bencel, I. Kotuliak. Architecture proposal for seamless handover in 802.11 networks. In: *Proc. of 2016 9th Joint IFIP Wireless and Mobile Networking Conf.*, Colmar, France, July, 2016.