

# Analytical Model of Connection Establishment Duration Calculation in Wireless Networks

Y. Chaiko

**Abstract**—It is important to provide possibility of so called “handover” for the mobile subscriber from GSM network to Wi-Fi network and back. To solve specified problem it is necessary to estimate connection time between base station and wireless access point. Difficulty to estimate this parameter is that it doesn’t described in specifications of the standard and, hence, no recommended value is given.

In this paper, the analytical model is presented that allows the estimating connection time between base station and IEEE 802.11 access point.

**Keywords**—Access point, connection procedure, Wi-Fi network.

## I. INTRODUCTION

At present moment Wi-Fi equipment based on IEEE 802.11 standard is widely used in various applications. If in the beginning of the development devices were used mainly for wireless local networks at offices and other premises, today it is possible to find other application using Wi-Fi. For example, attempts of GSM/GPRS networks convergence with Wi-Fi access zones are made. Thus it is important to provide possibility of so called “handover” for the mobile subscriber from GSM network to Wi-Fi network and back. To solve specified problem it is necessary to estimate connection time between base station and wireless access point. Difficulty to estimate this parameter is that it doesn’t described in specifications of the standard and, hence, no recommended value is given.

## II. CONNECTION PROCEDURE IN IEEE 802.11 WIRELESS NETWORK

The process of connection establishment between any nodes in Wi-Fi network is described in the specification of standard IEEE 802.11 [1]. That consists of three consecutive stages: scanning and synchronization, authentication, association.

At the first stage the node finds a radio channel, on which the access point is operating, defines configuration parameters and makes synchronization.

Scanning can be made in a passive or active mode. In the first case the node listens to each radio channel and waits for transmission of the beacon frame for to receive access point configuration parameters. With active scanning in each of radio channels, user node transmit inquiry frame “probe request” and expects to receive answer frame “probe response” in which configuration parameters also transmitted.

Using parameters received during scanning, user’s node

makes synchronization with an access point. During a synchronization process, the node sets values of timestamp and the BSSID identifier, received from access point in the previous frames [1].

Having ended scanning and synchronization, the node starts second stage of connection establishment: authentication. In specifications of IEEE 802.11 standard, two authentication types is described: open system and authentication by means of shared. One more authentication type is described in specification IEEE 802.11i [2], however it begins only after standard connection procedure between node and an access point is performed, therefore it is not considered in this paper.

The first authentication type is the most simple and allows nodes to receive the authentication status, if an access point also uses opened authentication. When using opened authentication between node and access point there is an exchange with two authentication frames. First is query, and the second - the answer on authentication query.

Authentication by means of shared keys assumes support by node and access point of WEP protocol. When using this authentication type node and access point Exchange four authentication frames.

At the final stage of connection establishment association is performed in which the association identifier (AID) is given to the node, and which is also used to keep connection in sleeping mode. During association node sends association query frame to access point, and access point transmit association query answer. As a result of this exchange process AID is given to the node and connection process is finished.

All frames which the node and access point exchange with are transferred using base access media mechanism, and transmission speed for these frames at physical level is 1 or 2 Mbit/s [1].

## III. MODEL OF CONNECTION ESTABLISHMENT DURATION CALCULATION

To estimate of general time of connection establishment we will take advantage of decomposition method of connection establishment process with the subsequent account of time which is required for each separate stage of considered process.

So, general time of connection establishment between node and access point  $t_{\text{total}}$  consists from duration of three described stages: scanning and synchronization, authentication and association (1).

$$t_{\text{total}} = t_{\text{scan}} + t_{\text{auth}} + t_{\text{assoc}} \quad (1)$$

The duration of the scanning stage  $t_{scan}$ , mainly depends on the chosen scanning mode: passive or active. The maximum duration of the passive scanning mode ( $t_{scan,pass}$ ) is a function of the Channel Time which limits time of listening of one channel.

The Channel Time is not defined in IEEE 802.11 specifications, therefore each manufacturer has the option to use any value. In practice this parameter defined as equal or higher than the period of beacon frames  $T_{beacon}$ . Duration of scanning in the active mode  $t_{scan,act}$  depends on quantity of channels in range  $N$ , time spent to access media using the base mechanism and on frame transmission  $T_{deliver}$ , and also parameters  $MinChannelTime$  and  $MaxChannelTime$ , limiting time of listening for one channel. In active scanning mode the user's node expects the answer on probe request for the time specified in  $MinChannelTime$ . And, if in time  $MinChannelTime$  the node receives at least one frame it continues to listen to the channel before the expiration of time specified in  $MaxChannelTime$ . Both specified parameters also not defined in standard specifications, and consequently each manufacturer of the Wi-Fi equipment can set them to any values on the discretion.

Neglecting transmit time of frame in media, duration of passive and active scanning modes is possible to calculate using formulas (2), (3).

$$t_{scan,pass} = N \cdot T_{beacon} \quad (2)$$

$$t_{scan,act} = N_{used} (T_{deliver} + MaxChannelTime) + N_{noused} (T_{deliver} + MinChannelTime) \quad (3)$$

Here  $N_{used}$  is a number of used channels in a range, i.e. channels, on which access points work;  $N_{noused}$  is a number of not used channels in range;  $N_{used} + N_{noused} = N$ .

Duration of authentication stage  $t_{auth}$  varies depending on the chosen authentication type - opened authentication  $t_{auth,opened}$ , or authentication with a shared key  $t_{auth,shared}$ . In both cases duration of the stage depends on time spent for media access using base mechanism and on frame transmit. With opened authentication between node and an access point there is an exchange of two frames, and with shared keys authentication - four frames. Therefore, neglecting frame transmit time in a radio channel, it is possible to write down:

$$t_{a,miss,opened} = 2 \cdot T_{deliver}, t_{a,miss,shared} = 4 \cdot T_{deliver} \quad (4)$$

The association stage has no any modes essentially changing its duration, therefore on its duration  $t_{assoc}$  influences only time spent for media access using DCF mechanism and on frame transmit. At association stage of node and access point two frames are exchanged, hence, it is possible to write down:

$$t_{assoc} = 2 \cdot T_{deliver} \quad (5)$$

Parameters  $MinChannelTime$  and  $MaxChannelTime$  in (3) can be estimated with the help of the technique offered in [3], however it is necessary to keep in mind, that manufacturer of the concrete device can establish his own values for the given

parameters. Therefore produce more accurate estimation of these parameters it is necessary to make experimental research, using the equipment.

Special place in the connection establishment procedure between nodes in wireless local network IEEE 802.11 occupies access to the common media. To get access to media the station randomly chooses value back off timer in limits from 0 to current value of contention window and begins countdown with the clock period equal to duration slot (slot time), which is defined in physical level specifications of IEEE 802.11 standard.

The specified random factor will give to node media access time and, hence, general connection time probability characteristics. To estimate these characteristics it is possible to take advantage of one of the developed analytical models [4], [5], [6] or results. In works [4], [5], [6] it is shown, that the received by means of analytical models results with high degree of accuracy coincide with imitation modeling results, therefore it is possible for researches to choose any of method.

Having substituted (2), (3), (4), (5) in the equation (1), it is possible to receive general time of connection establishment of node with Wi-Fi access point. An example of duration calculation of connection establishment process in IEEE 802.11 wireless network is shown in Fig. 1. For the graph opened authentication mechanism is chosen, since it is the most simple and fast. Values  $MinChannelTime$  and  $MaxChannelTime$  are taken from [3]. Beacon period is equal to 100 ms, since this value is used by default by most equipment manufacturers. Number of the used channels is equal to 3, since in 2,4 GHz range for 802.11 b and g physical levels in Europe it is defined three not crossed radio channels from 13 accessible.

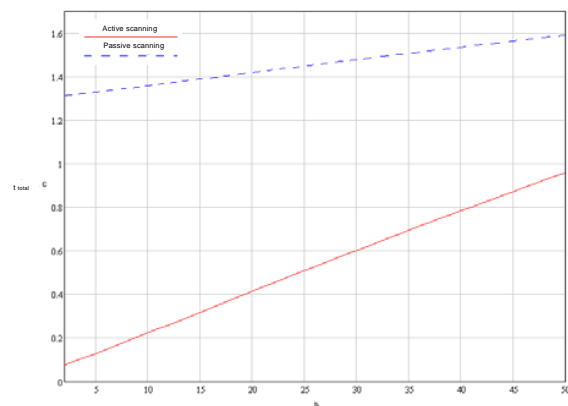


Fig. 1 Dependence of connection establishment time from quantity of stations in a service zone

Chart shows connection establishment time between access point and user's node in IEEE 802.11 wireless network depending on the number of the stations which are in a service zone. Calculation is made for a case, when at any station in a network at any moment there is packet intended for transmit, i.e. in the conditions of the big load in the network. The chart is shows two scanning modes: active and passive.

From chart dependences it is clearly visible, that big influence on total connection establishment time of user's

node and access point renders the chosen scanning mode. With passive scanning duration of connection establishment process exceeds 1 second for any quantity of nodes working in a service zone. However, when using active scanning this value is much lower. Therefore to reduce time of connection establishment of it is necessary to use active scanning mode and whenever possible reduce quantity of stations which are in a service zone.

#### IV. CHOICE OF THE RIGHT WiFi CHANNEL

With increasing density of WiFi networks, more and more WiFi networks popping up in the neighborhood, which may impact performance on the WiFi network, if frequencies interfere. Two WiFi networks operating on the same channel are forced to share bandwidth, as they can't "talk" simultaneously, which halves each network's bandwidth. In order to evade this effect, you need to change your access point's channel, but taking the adjacent one won't do it, as WiFi channels are arranged in an overlapping pattern, as shown on Fig. 2. Channel 1 overlaps channels 2 to 5, which therefore may not be used for a neighbouring WiFi network. If channel 1 is used, you should switch to channel  $\geq 6$ .

There must be a spacing of at least 5 channels (or more) between each WiFi network in order to avoid interferences. Further, if all your WiFi-devices support 802.11g (the 54 MBit/s WiFi-variant), you should set the router to 802.11g-only mode, as the 802.11b-compatibility impacts on bandwidth and range even among 802.11g-devices. Another possible cause of low performance may be proprietary WiFi acceleration modes like "SuperG", "MAXg", "125 High Speed Mode" or "Speed Booster", if not all devices in your network support the very same mode, why you should disable those. A lot of cordless phones in different countries operate at the 2.4 GHz band like Wifi and so most of them cause interferences WiFi, that can't be avoided by a channel change, since those phones use a very broad spectrum or perform permanent frequency hopping.

If you own a 2.4 GHz phone, try switching it off and removing the power supply of it's base station. In case your wireless signal improves, replace your cordless phone with a new one operating at 1.8 GHz or 5.8 GHz.

#### V. CONCLUSION

So, on the basis of the analysis of connection establishment process between user's node and access point in Wi-Fi wireless network, in this paper offered the model allowing analytically define duration of considered process. Key parameters influencing connection establishment time are defined, and also the recommendations to reduce them are given.

#### REFERENCES

- [1] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-1999, IEEE, New York, 1999.
- [2] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) Specifications. Amendment 6:Medium Access Control (MAC) Security Enhancements, IEEE Std. 802.11i-2004,IEEE, New York, 2004.
- [3] H. Velayos and G. Karlsson. "Techniques to reduce IEEE 802.11b MAC layer handover time", KunglTekniska Hogskolen, Stockholm, Sweden, Tech. Rep.TRITA-IMIT-LCN R 03:02, ISSN 1651-7717, ISRN KTH/IMIT/LCN/R-03/02SE, April 2003..
- [4] P. Chatzimisios, V. Vitsas, A. C. Boucouvalas. Throughput and delay analysis of IEEE 802.11 protocol. Proceedings of IEEE 5th International Workshop on Networked Appliances, October 2002.
- [5] I. N. Vukovic, N. Smavatkul. Delay analysis of different backoff algorithms in IEEE 802.11. IEEE VTC 2004.
- [6] C M. Ergen, P. Varaiya. Delay Analysis of Distributed Coordination Function in IEEE 802.11. IEEE GLOBECOM 2006.

**Yelena Chaiko** (M'07).Ph.D, in 2004 – Doctor of Science at Riga Technical University. From 2006.01.10., she is the head researcher, Institute of Industrial Electronics and Electrical Drives at Riga Technical University. Her research interests are Telecommunication systems, Electronics and Electric Drives (e-mail: jelena.caiko@rtu.lv).

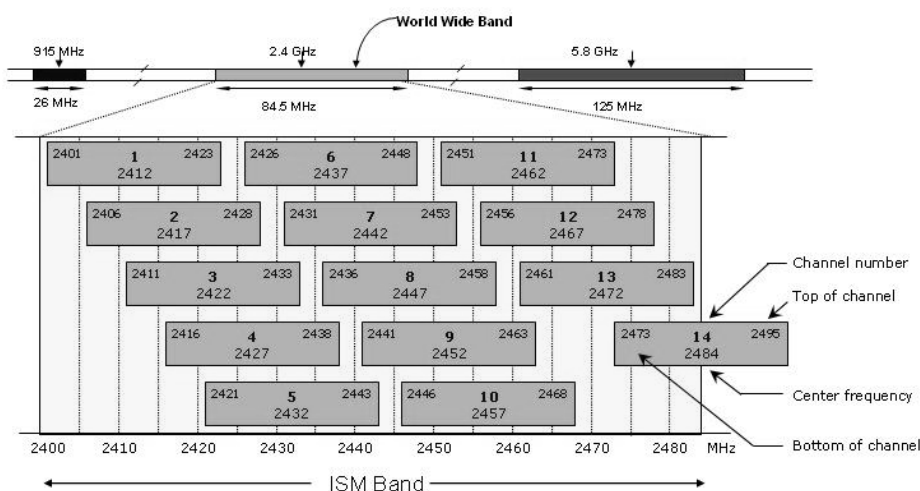


Fig. 2 WiFi channels are arranged in an overlapping pattern