Telecommun Syst (2013) 52:2713–2720
DOI 10.1007/s11235-011-9590-5

On the fast BSS transition algorithms in the IEEE 802.11r local area wireless networks

Przemysław Machań · Jozef Wozniak

Published online: 9 September 2011

Abstract Handover performance is critical to support multimedia services that are becoming increasingly available over the wireless devices. The high transition delay can be unaccepted for such services or can be a source of disruption on the session. On the other side, IEEE 802.11 standard is being extended with new functionalities. Security and QoS features, included in recent IEEE 802.11-2007 standard, add management frames that are exchanged during the transition process. In consequence the handover delay is increased. IEEE 802.11r-2008 amendment introduces Fast BSS Transition (FT) that simplifies the handover process. The authors propose the new handover algorithms based on FT protocol and compare them with existing solution. Additionally, simulation experiments are conducted to answer the question if multimedia services can be properly supported in IEEE 802.11r networks. The authors prove that handover delay can be reduced to 13 ms in the average case.

Keywords Wireless LANs · Handover algorithms · 802.11r · Simulation model · Performance

This work has been partially supported by the Polish Ministry of Science and Higher Education under the European Regional Development Fund, Grant No. POIG.01.01.02-00-045/09-00 Future Internet Engineering.

P. Machań · J. Wozniak (✉)
Faculty of Electronics, Telecommunication and Informatics, Gdańsk University of Technology, Narutowicza 11/12, Gdańsk, Poland
e-mail: jowoz@eti.pg.gda.pl

P. Machań
e-mail: przemac@o2.pl

1 Introduction

IEEE 802.11r-2008 [1] is an amendment to the IEEE 802.11-2007 standard [2] that introduces Fast Basic Service Set Transition. The handover has already been supported under the base 802.11-1999 standard; four messages were required to connect to the new AP in the typical case. However, with the new extensions of the standard, the number of management frames went up dramatically. The 802.11i-2004 introduced frame exchange for 802.1X authentication, while 802.11e-2005 introduced frame exchange for admission control request. IEEE 802.11r-2008 amendment proposes algorithms to bring the number of frames required for handover down to the level of 802.11-1999. This is expected to be achieved by limiting the number of frames for 802.1X authentication and 802.11e admission control.

2 Legacy handover

The typical handover scenario is presented in Fig. 1. The whole handover process is divided into phases. Each phase is defined as a separate procedure that introduces handover delay. The handover begins with the Detection Phase when a Mobile Station (MS) determines the requirement for the handover. Detection Phase is not covered by the IEEE 802.11 standard and strongly depends on proprietary handover detection algorithms. For example MS may wait for a few consecutive beacons to be lost or a number of failed retransmissions. The link layer may also receive an information from the physical layer that the Mobile Station lost or is about to lose radio connection with the current AP. During that phase some packets may already be lost.

The station begins the Search Phase i.e. it scans all physical channels by switching radio frequency for APs in vicinity. According to the IEEE 802.11-1999 standard the station

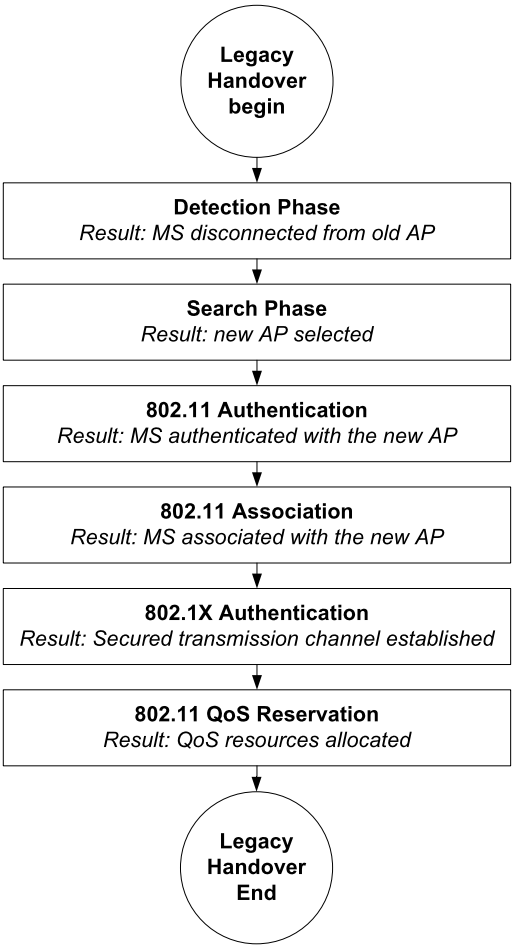


Fig. 1 IEEE 802.11-2007 handover

can perform either passive or active scanning. In the passive scanning the station waits for beacon frames on the channel for implementation-dependent time. The active scanning means that the station sends at least one Probe Request frame on each channel and receives zero or more Probe Responses from each AP operating on the selected channel. When the scanning procedure is completed the Mobile Station chooses the AP and begins authentication procedure. In the following consideration the active scanning algorithm is assumed. The AP selection algorithm can be extended with a resource query. The Mobile Station may select Access Point that can reserve sufficient resources for connection and will guarantee required QoS level.

However, the handover procedure in a real environment can be more complicated. As it has been presented in [12], the station is able to exchange data in the period of time during the Search Phase. The old Access Point (oAP) is not aware that station begins Scan Phase. Thus, the old AP retransmits data to the station which is not responding. Accidentally, the old AP is successful in sending data to the station during the Search Phase. This can happen when the station scans the channel the AP is working on. To avoid such problems the Mobile Station can inform the Access Point that it enters power save mode (by setting Power Management Bit to 1 in a data frame). The Access Point will buffer data directed to the station assuming that the station is sleeping.

The next phase is 802.11 Authentication. The IEEE 802.11-1999 standard defines two authentication methods: Open System and Shared Key. The first method consists of two-frame sequence and does not use any authentication algorithm. Shared Key is the four-frame sequence algorithm based on WEP. Because of known weaknesses of the WEP algorithm (initially described in [5]) it is not considered as a secure solution. To configure network for the highest security IEEE 802.11i extensions were introduced in the IEEE 802.11-2007 standard.

Before the station continues data transmission throughout the new Access Point it has to reassociate with the new AP. The procedure consists of two messages sequence, namely: Reassociation Request and Reassociation Response. The station is allowed to send data via the new AP when response with successful code is received.

The next phase is 802.1X Authentication, introduced in IEEE 802.11i amendment. During that phase EAP authentication is executed between Mobile Station and the AAA server, proxied by the AP. EAP supports a wide variety of authentication protocols which support a range of credential types raging from passwords to certificates. Upon successful authentication EAP protocol derives a Master Shared Key (MSK). In the last stage the Mobile Station executes QoS procedures as described in 802.11e-2005 amendment.

3 Fast BSS transition

Fast BSS Transition protocol allows Mobile Station to fully authenticate only with the first AP in the domain and use shorter association procedure with the next APs in the same domain. The amendment defines domain as the group of APs that support FT Protocol and are connected over Distribution System (DS). The MS session i.e. security and QoS information is cached in the network. When the station associates with the first AP in the domain it is now pre-authenticated with the other APs in the domain.

The first AP, the station authenticates to, will cache its PMK and use it to derive session keys for other APs. This AP is named R0 Key Holder (R0KH) as it holds level 0 PMK (PMK-R0). When MS reassociates with a new AP, R0KH generates PMK-R1 and forwards that to the new AP, which is called R1KH. The new AP interacts rather with the R0KH, than directly with AAA server.

The amendment defines two methods of FT: Over-the-air and Over-the-DS. In the first case MS communicates over a

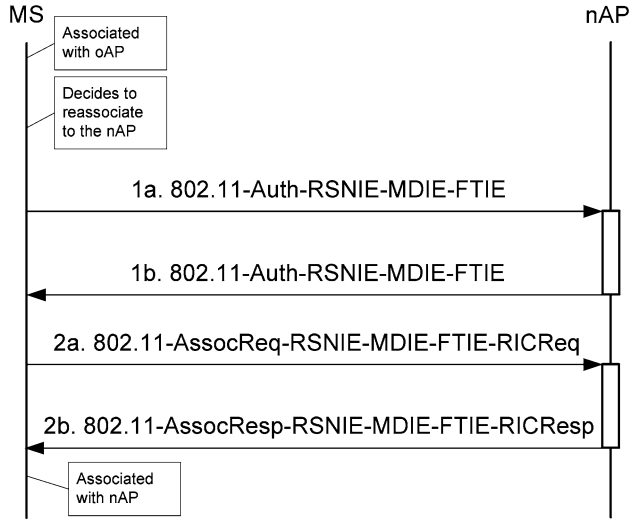


Fig. 2 Over-the-air FT protocol

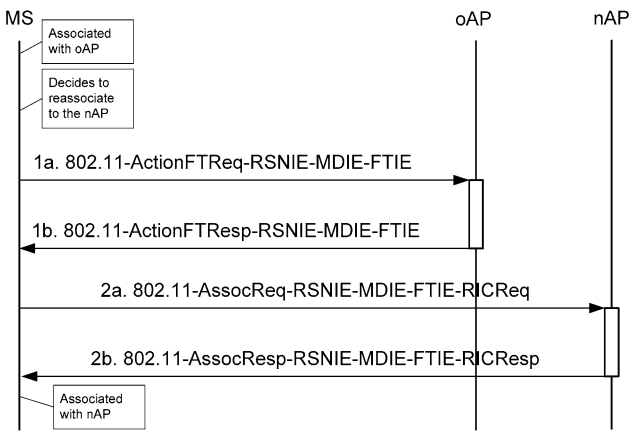


Fig. 3 Over-the-DS FT protocol

direct 802.11 link to the new AP. In the Over-the-DS method the MS communicates with the new AP via the old AP. Over-the-air FT protocol is presented in Fig. 2. Mobile Station is already associated with the old AP from the domain. At some point MS decides to reassociate with a new Access Point (nAP), sending 802.11 Authentication frame with Information Elements required by FT Protocol (message 1a in Fig. 2). Robust Security Network IE (RSNIE) contains PMK-R0 obtained from the first AP in the domain that MS associated with. Mobility Domain IE (MDIE) contains a domain identifier, capabilities and policies advertised by nAP in Beacon and Probe Response frames. Fast BSS Transition IE (FTIE) contains R0KH identifier that is obtained from the first AP in the domain and SNonce generated by MS. The new AP responds with 802.11 Authentication frame that contains the same types of Information Elements as the request (message 1b). RSNIE confirms the PMK-R0 identifier sent by the station. MDIE, in turn, contains information advertised by the nAP in Beacon and Probe Response frames. And finally FTIE contains R1KH identifier provided by nAP, ANonce generated by nAP and SNonce sent by MS.

In the next step MS sends 802.11 Association Request message (2a) with RSNIE, MDIE, FTIE and Resource Information Container Request (RIC-Request). RSNIE contains PMK-R1, MDIE contains the same information as Authentication message sent by MS. FTIE conveys ANonce, SNonce, R0KH identifier, R1KH identifier. FTIE data together with MS and AP MAC addresses is used to calculate MIC which is also included in FTIE. RIC-Request is the collection of Information Elements that contains TSPEC and TCLAS IEs if an 802.11e QoS model is used. Access Points responds with 802.11 Association Response message (2b) that conveys RSNIE, MDIE, FTIE and RIC-Response. RSNIE and MDIE contain similar information as in Association Request. FTIE contains ANonce, SNonce, R0KH identifier, R1KH identifier and MIC calculated on AP side. RIC-Response contains TSPEC and Schedule IEs.

Figure 3 illustrates Over-the-DS FT protocol version. The MS uses Action frame to communicate with the old AP, providing the address of the new AP. Old AP communicates over the DS with the new AP forwarding STA request. The new AP responds over DS and the oAP sends Action FT Response to MS. At this step MS is authenticated with nAP. Then, MS changes the channel and begins association procedure with nAP. The type and content of information elements is the same while using both methods: Over-the-air and Over-the-DS.

4 IEEE 802.11r analysis

The important problem that is not defined by the 802.11r-2008 amendment is station context distribution (e.g. security credentials, QoS settings). Fast BSS Transition protocol assumes that as the MS initially associates with the first AP the station context is available at the all APs in the domain. In the basic scenario the first AP the MS associates with will broadcast station context to the all APs in the domain. However, this solution may be considered a waste of RADIUS protocol resources and bandwidth [3]. The other scenario assumes that the list of APs inside the mobility domain changes as the Mobile Station moves between APs. The mobility domain is related to MS and composed from the neighbors of AP the Mobile Station is associated with at a particular time. The AP that is removed from the mobility domain deletes the context related to the MS. This algorithm is proposed in [6], however it requires MS to control the list of APs within the domain. Moreover, the Mobile Station needs to know the new AP that is outside the mobility domain to transfer context beforehand. This requires the "Link going down" trigger that is hard to implement in 802.11 networks.

The cache size for station context is also an important issue. The mobility domain may have a dedicated R0KH to limit the number of security associations between APs. Otherwise, if the first AP is the default R0KH, there will be a full mesh of security associations between all APs in the domain. This may require for each station $n(n-1)$ keys to be managed between n Access Points. With this assumption 802.11r-2008 may not scale to large networks [7].

The article [8] presents performance analysis of Over-the-DS 802.11r handover. From the paper it follows that the transition delay can be reduced by over 90% for VoIP traffic scenario. The experimental study of Over-the-air method is presented in [4]. The measured time consumed by authentication and association procedures is 42 ms. However, that value does not include delay introduced by other handover phases. In the following paper the authors compare both Over-the-DS and Over-the-air methods in the same scenario. Moreover, the handover procedure is divided into phases to fully understand the sources of delay. The handover model in the following article includes the detection phase which is typically skipped in the other articles.

5 Proposed algorithms

Three algorithms were proposed for the purpose of the analysis: Legacy, FT-air and FT-ds. In the Legacy scenario the handover algorithm described in IEEE 802.11-2007 standard is used. The next two algorithms are border cases that present the possible implementations of Fast Transition protocol. FT-air is the modifications of the Legacy algorithm that uses Over-the-Air Protocol to shorten the 802.1X authentication. FT-ds scenario is the new algorithm that is designed to minimize the handover latency. The Mobile Station proactively determines the new AP based on its position and uses Over-the-DS Protocol to execute the transition. The modelled positioning scheme introduces no delay to the handover algorithms as we'd like to validate the best possible case.

Both proposed algorithms are presented in Fig. 4. The frames exchanged during the 802.11r Authentication and Association procedures are extended with Information Elements specific to the Fast BSS Transition algorithm. For the FT-ds method the Mobile Station needs to decide when the transition procedure should be started. In our model MS is aware of its location and all Access Point locations in the domain. Based on that knowledge the Mobile Station can instantly transition to the nearest AP. This simple algorithm allows for stable and repeatable transition performance measurements. When MS detects the nearest AP it sends IEEE 802.11 Action FT Request frame to the old Access Point, the station is still associated with. Old Access Point transmits station context to nAP over the Ethernet network. In the next step Old AP responds with IEEE 802.11 Action FT Response frame. At that stage the Mobile Station changes the channel to the new AP's channel and executes IEEE 802.11 Association procedure.

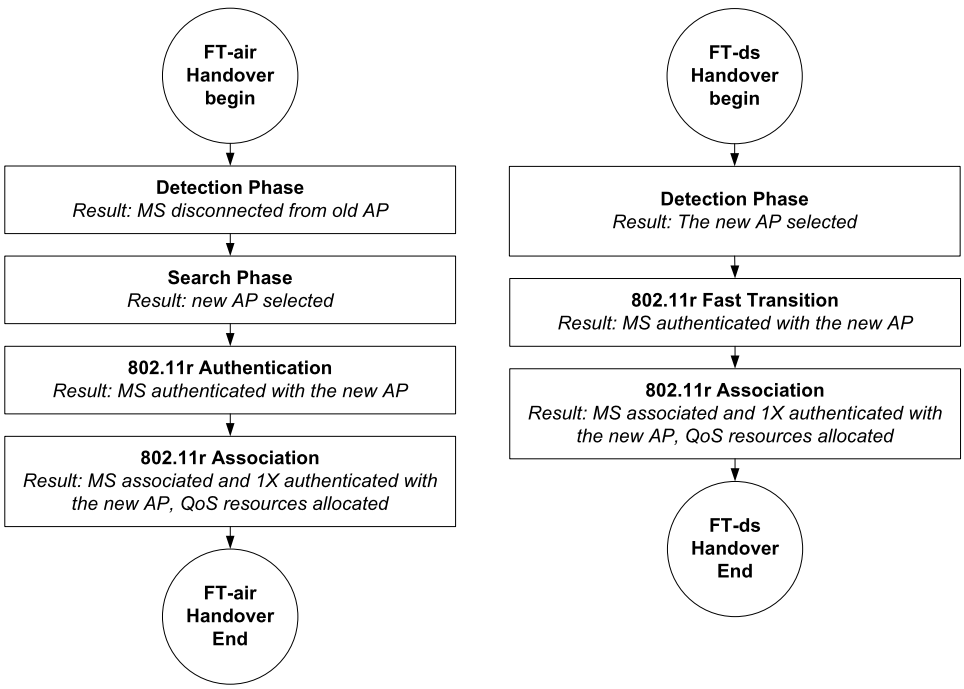
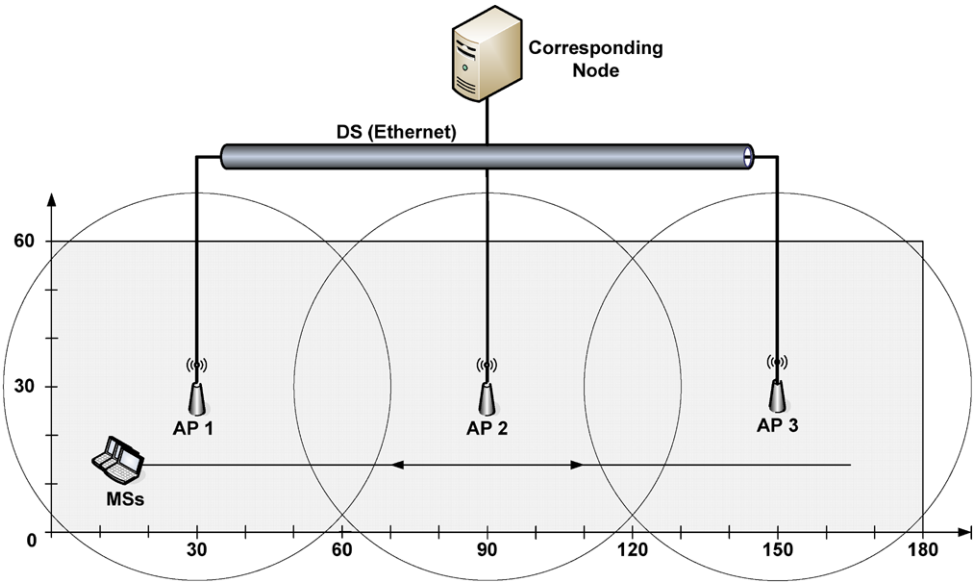


Fig. 4 FT-air and FT-ds algorithms

Fig. 5 Simulation scenario



6 Simulation Model

Fast BSS Transition protocol was implemented in ns2, a widely used network simulator. For the purpose of the simulation the model of a "city market" was created, as presented in Fig. 5. The three Access Points (AP) in the domain supports FT protocol and are connected over an Ethernet network. The wireless network operates in the 802.11g-only mode. The Mobile Station moves within an area of 180×60 meters with the velocity of 1 m/s. The measurements were conducted in the scenario with only one MS to avoid interferences due to traffic from the another sources. The MS sends VoIP traffic to the Corresponding Node. UDP protocol is used and packet payload is 64 kB. The Corresponding Node generates a similar traffic destined to MS.

The reason for using UDP, and not TCP, is that TCP infers congestion from packet loss and scales back its send window accordingly. The experiments aimed at how throughput, handover delay and packet loss are affected by handover algorithms, rather than due to protocol-induced throughput reductions. Although TCP is used for many network applications, the majority of real-time multimedia services are based on UDP.

Whenever 802.11r is used the Mobile Station is already preauthenticated with three Access Points in the domain. In the experiments the reassociation scenario is only considered and the initial authentication in the domain does not influence the handover delay. EAP-TLS is used as 802.1X authentication method. The RADIUS authentication procedure is simulated as a delay of 540 ms, based on measurements in [11]. The Mobile Station also creates a single TSPEC for the purpose of VoIP traffic.

The traffic in network was generated as CBR streams and modified by the inter-packet delays. The default network load is 1 Mbps with half of traffic sent from MS to Corresponding Node and the other half the opposite way. The load value changes but the load is always split in half between directions. The Mobile Stations move between Access Points with the assumption that at any time MSs are evenly distributed between APs.

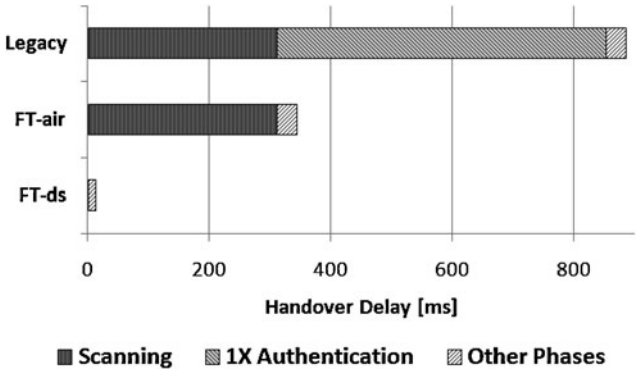


Fig. 6 Handover delay for different modes

7 Performance evaluation

The handover delay for different modes is presented in Fig. 6. The longest phases that contribute to the total delay are marked with bar patterns. Scanning is one of the longest phases because the station has to check each 802.11 g channel for available Access Points. 802.1X Authentication also introduces a substantial overhead because the station needs to authenticate with RADIUS server in the network. The measured values are consistent with results published in literature [4, 8, 10–12].

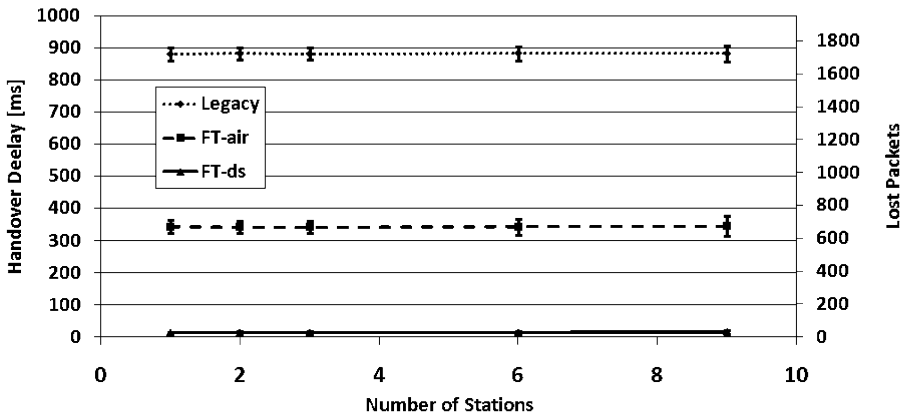


Fig. 7 The influence of number of stations on handover delay

Table 1 Delay intervals [ms] for handover phases and different handover algorithms

Phase/algorithm	Legacy	FT-air	FT-ds
Detection	20.371	21.549	0.689
Search	311.211	310.996	0.000
Authentication/FT	10.304	10.660	2.944
Association	0.576	0.837	12.970
1X authentication	541.468	0.000	0.000
4Way authentication	0.656	0.000	0.000
QoS	0.796	0.000	0.000
Total	885.381	344.042	12.970

The datailed values of handover intervals are presented in Table 1. The Detection Phase is a time interval from last packet sent via the old AP to the moment when Mobile Station begins the handover. The detection algorithm for Legacy and FT-air algorithms is based on beacon status and transmission quality. The station disassociates when beacons are lost or the number of failed retransmissions is high. The Detection Phase delay for FT-ds algorithm is shorter because the Mobile Station decides to reassociate at predefined location and does not need to use a time window to evaluate handover detection metrics.

The Scanning procedure covers active scanning of 11 channels. The algorithm defined in IEEE 802.11-1999 standard is used. The radio channel switchover time is set to 10 milliseconds, as defined in [9]. The authentication procedure for Legacy protocol is defined in IEEE 802.11-1999 standard. The authentication delay is introduced by Open System handshake between MS and AP. In the Legacy and FT-air methods the authentication time includes channel switching.

FT-air algorithm uses authentication scenario defined in IEEE 802.11r amendment. The Authentication frames contain new information elements: RSNIE, MDIE and FTIE. For this reason the Authentication Phase delay is slightly higher for FT-air vs. Legacy algorithm. When FT-ds algorithm is used Mobile Station sends Action frame to the old AP requesting Fast Transition to the new AP. It is important to note that the Mobile Station remains associated with an old AP. The association is broken when FT Response is received. In FT-ds method handover delay may include context transfer between old AP and the new AP which is not modelled. Depending on the context distribution algorithm the Fast Transition delay may vary. The association time includes channel switchover time.

The 802.1X authentication delay includes a full authentication between Mobile Station and RADIUS server. For Legacy algorithm the Mobile Station communicates with Authentication server each time MS reassociate with the new AP. When 802.11r algorithm is used the station is preauthenticated in the domain, so there is no delay at that phase. The 4Way Authentication delay includes message sequence to establish PTK and is applied only in Legacy algorithm. Finally QoS configuration is issued with Add TSPEC messages. In the 802.11r amendment QoS procedure is concurrent with reassociation protocol.

The influence of the number of stations and network load is presented in the Figs. 7 and 8 respectively. The handover delay is stable whenever the network parameters changes. In the Fig. 7 the right axis presents the number of 64-byte-long packets lost during a single handover.

For multimedia services it is important to keep the standard deviation of handover delay is low as possible. Cumulative Distribution Functions (CDFs) for examined scenarios are presented in Fig. 9. The average handover delays in Legacy as well as FT-air algorithms are too high to fulfill requirements of multimedia services. If FT-ds is used the handover delay varies between 10 and 29 milliseconds which is acceptable for both voice and video services nowadays.

The noise level in the wireless channel increases with the transmission distance, so the Signal-to-Noise Ratio (SNR) drops down dramatically. In 802.11 protocol the transmission rate is reduced as the Mobile Station's distance from the current Access Point increases. The transmission rates for send and receive directions are reduced to assure that

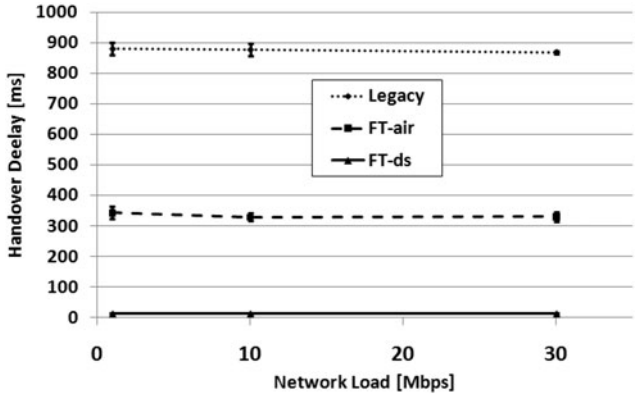


Fig. 8 The influence of network load on handover delay

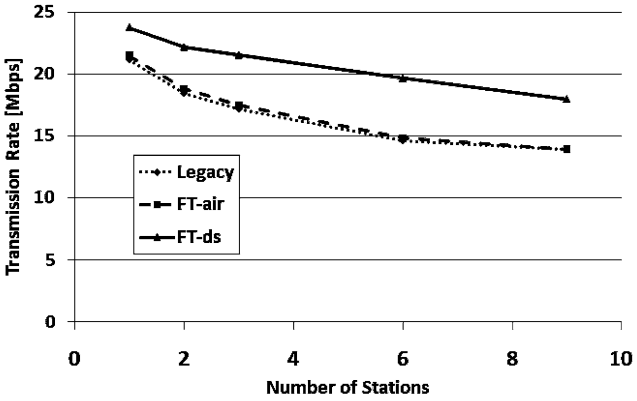


Fig. 10 Average Transmission rate versus number of stations

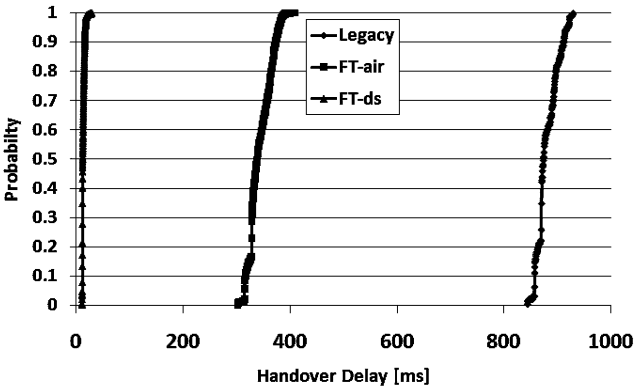


Fig. 9 CDFs of handover delay for different methods

maximum error level, that can be accepted for successful transmission, is not exceeded. In consequence the station may not use the wireless channel effectively when located away from an Access Point.

Event though the maximum transmission rate is 54 Mbps in the Legacy and FT-air algorithms both uplink and downlink rates drop frequently to 6 Mbps. It typically happens just before the station switches to the new AP. Figure 10 illustrates average transmission rates for different number of stations. When FT-ds algorithm is used the Mobile Station executes handover sooner as in other algorithms and the transmission rate is not reduced frequently. In consequence the packets are sent with higher average rate and the wireless resources are used more efficiently. The average transmission rate decreases with the number of stations because of sharing wireless channel.

8 Conclusions

The handover delay is smaller for both FT-air and FT-ds scenarios comparing to the Legacy algorithm, as defined in IEEE 802.11-2007. FT-air algorithm reduces handover delay by over 60% mainly because the station is already pre-authenticated in the domain. Communication with an Authentication server stands for the substantial delay in the legacy handover, as defined in IEEE 802.11-2007 standard. However, the average handover delay of 344 ms is still too high for current multimedia services. FT-ds algorithm reduces handover delay to 13 ms and offers higher packet transmission rates. The whole algorithm executes longer but the association is broken only during the association procedure and channel switchover that is becoming the primary performance bottleneck. However, the FT-ds algorithm is considered the most optimistic case in which MS is not required to perform AP detection.

The next step is to design the handover detection algorithm for FT-ds scenario. For most appliances it is not accepted to perform handover based on current MS location and fixed AP position preconfigured at MS. The authors used location-based handover detection algorithm just to evaluate the potential performance improvements that can be achieved with FT-ds protocol. Handover detection algorithm can use physical and mac statistics or 802.11k measurements to determine the new Access Point and the moment of handover.

References

1. IEEE 802.11: Amendment 2: Fast Basic Service Set (BSS) Transition, IEEE Std 802.11r-2008, July 2008.
2. IEEE 802.11-2007: Part11: Wireless LAN Medium Access Control and Physical Layer Specifications, June 2007.
3. Aboudagga, N., & Quisquater, J. J. (2004). Wireless Security and Roaming Overview. DIMACS workshop: mobile and wireless security, November 2004.
4. Bangolae, S., Bell, C., & Qi, E. (2006). Performance study of fast BSS transition using IEEE 802.11r. IWCMC'06, July 2006.

5. Borisov, N., Goldberg, I., & Wagner, D. (2001). Intercepting mobile communications: the insecurity of 802.11. In *7th annual international conference on mobile computing and networking*, Rome, July 2001.
6. Chung-Ming, H., & Jian-Wei, L. (2008). A context transfer mechanism for IEEE 802.11r in the centralized wireless LAN architecture. In *IEEE 22nd international conference on advanced information networking and applications*, March 2008.
7. Clancy, T. (2008). Secure handover in enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11r. *IEEE Wireless Communications Magazine*, October 2008.
8. Hassan, A., & Hassanein, H. (2008). A performance study of roaming in wireless local area networks based on IEEE 802.11r. In *24th biennial symposium on communications*, June 2008.
9. Pal, S., Kundu, S., Basu, K., & Das, S. K. (2006). *Emancipating the IEEE 802.11 network from handoff delay*. Crewman Lab, June 2006.
10. Ruckforth, T. (2004). *AAA context transfer for fast authenticated inter-domain handover*, Swisscom SA, Innovations Broadband Network, Bern, September 2004.
11. Tsao, S. L., & Hsiang, Lo P. (2007). DualMAC: a soft handoff mechanism for real-time communications in secured WLANs. *Computer Communications*, Vol. 30, June 2007.
12. Vatn, J. O. (2003). *An experimental study of IEEE 802.11b handover performance and its effect on voice traffic*. Royal Institute of Technology, Stockholm, Sweden, July 2003.

Przemysław Machań was born on 2nd July 1977 in Gdańsk, Poland. He received his M.Sc. in Computer Science (2001) and M.Sc. in Information Management (2003) from Gdańsk University of Technology (GUT).
Since March 2002, he has been working as Software Engineer for Intel Corporation at R&D site located in Gdańsk. Currently, he completes his Ph.D. in Computer Science at GUT. His research interests include IP and WLAN mobility and WLAN architectures. He is married and has two children.

Jozef Wozniak is a Full Professor in the Faculty of Electronics, Telecommunications and Computer Science at Gdańsk University of Technology. He received his Ph.D. and D.Sc. degrees in Telecommunications from Gdańsk University of Technology in 1976 and 1991, respectively. He is author or coauthor of more than 250 journal and conference papers. He has also coauthored 4 books on data communications, computer networks and communication protocols.
In the past he participated in research and teaching activities at Politecnico di Milano, Vrije Universiteit Brussel and Aalborg University, Denmark. In 2006 he was Visiting Erskine Fellow at the Canterbury University in Christchurch, New Zealand.
He has served in technical committees of numerous national and international conferences, chairing or co-chairing several of them. He is a member of IEEE and IFIP, being the vice chair of the WG 6.8 (Wireless Communications Group) IFIP TC6 and. For many years he chaired the IEEE Computer Society Chapter at Gdańsk University of Technology. His current research interests include modeling and performance evaluation of communication systems with the special interest in wireless and mobile networks.