Evaluation of IPv6 Services in Mobile WiFi Environment

ZOLTÁN GÁL, ANDREA KARSAI, PÉTER OROSZ

University of Debrecen, Service Center of Informatics
zgal@cis.unideb.hu, kandrea@fox.unideb.hu, oroszp@delfin.unideb.hu

Keywords: Internet2, IPv6, WiFi, L2 and L3 roaming, TCP Slow Start algorithm, TCP Windowing algorithm

IPv6 may play an important role in the introduction of mobile services in next generation networks. One of the key questions in this context is the impact of mobility on the TCPv6 and UDPv6 services. In this work, comparative measurements have been carried out in an outdoor WiFi test system, containing IEEE 802.11b access points and mobile clients, to understand the effects of the processes occurred during the roaming phase of the WiFi system on the IPv4 and IPv6 connections. One of the conclusions is that the TCP connections are significantly affected by the interaction between the relative speed of mobile clients to the APs and the execution of roaming, whilst it has minor effect to the UDP transfer. Furthermore, we demonstrated that the IPv6 protocol provides a higher quality in a mobile environment than its predecessor, the IPv4.

1. Introduction

The appearance and spreading of the sophisticated mobile services over IPv6 is the most significant advantage of the Internet2. The effect of mobility on the TCPv6 and UDPv6 protocols reveals an exciting user and professional issue. In order to picture the qualitative answer with quantitative attributes, comparative measurements are needed.

The operability, availability of services during the physical movement of the node is a requirement that appears as one of the important demands from an advanced network with good reason. The development of wireless IP telephony, wireless laptops and PDAs show the way to this direction. The mobility feature of wireless LANs drives to a new result:

– *Innovative application development:*
  alarm and message sending. Appearance of the constantly online workflow systems.
– *Increase of efficiency and productivity:*
  the permanent network connectivity makes it possible to perform tasks from any place without delay.
– *Increase the authenticity of data:*
  data is available any time, any place.
– *Availability:*
  user can be virtually online at his home, on the street and in the workplace as well.

In this paper we intend to show a quantitative comparison of different applications of the IP terminals communicating over a mobile WiFi network. Furthermore we provide the explanation of the experienced phenomenon, and draw the conclusions about the expected directives of developments.

2. Mobile data transmission

As we already know, the IP versions 4 and 6 are able to provide mobile functions beyond the conventional fixed, wired network communication. The wireless data-link layer connections can be also capable of forwarding frames for the network layer. Thus for transport layer protocols the behavior of the lower layers will be considered more or less depending on the IP version.

The mobile function of IP means that the terminal moves physically from his place during the communica-

Table 1.

Distinctive features	Mobile IPv4	Mobile IPv6
Special routing function (foreign agent)	Yes	No
Route optimization ability	Part of the protocol	Extension
Symmetrical connection between the MT and the router in the current location	No	Yes
Routing overhead bandwidth requirement	High	Low
Ability to disconnect from Layer 2	No	Yes
"Tunnel soft" state handling required	Yes	No
"Dynamic home agent" address discovery	No	Yes

Table 2.

Network	Protocol	
	IPv4 / IPv6	Mobile IPv4 / Mobile IPv6
Wired	√	√
Wireless	√	√

tion, therefore his network layer environment changes. At the new location an IP router with foreign agent function keeps the connection henceforward with the original home agent router by means of an IP tunnel [1]. Thus the IP terminal is able to communicate at the new place. The speed of interaction between the agent processes and the additional network load are important issues. The IP version 4 and 6 show different behaviors from this aspect as well. These features are listed in *Table 1*.

In the case of wireless data links there is a possibility for the mobile terminal to remain in the same broadcast domain, therefore the route of the forwarded frames changes, but the IP address of the terminal doesn't. This is the typical event of L2 roaming, when the terminal switches to another access point and only the data-link layer devices changes theirs CAM tables. This paper studies the effect of roaming occurred during cell changes generated by a terminal placed in a moving vehicle in a real outdoor WiFi environment for IP v4 and v6 connections *(Table 2)*.

3. Roaming mechanisms

In wireless LANs, nodes are able to virtually connect to the corporate network. The cell change (roaming) is a time consuming process during that the terminal re-associates with a new AP from the current AP. We are talking about data-link (L2) roaming when this process occurs between APs belonging to the same subnet *(Figure 1)*.

If the terminal connects to an AP in a different subnet, then network (L3) roaming will happen. Network roaming can occur only after a successful L2 roaming [2].

Changing the cell is based on the decision of the client whose task is to discover the possible APs, to evaluate their parameters, then to choose between the selected APs. The data-link cell change involves the followings:

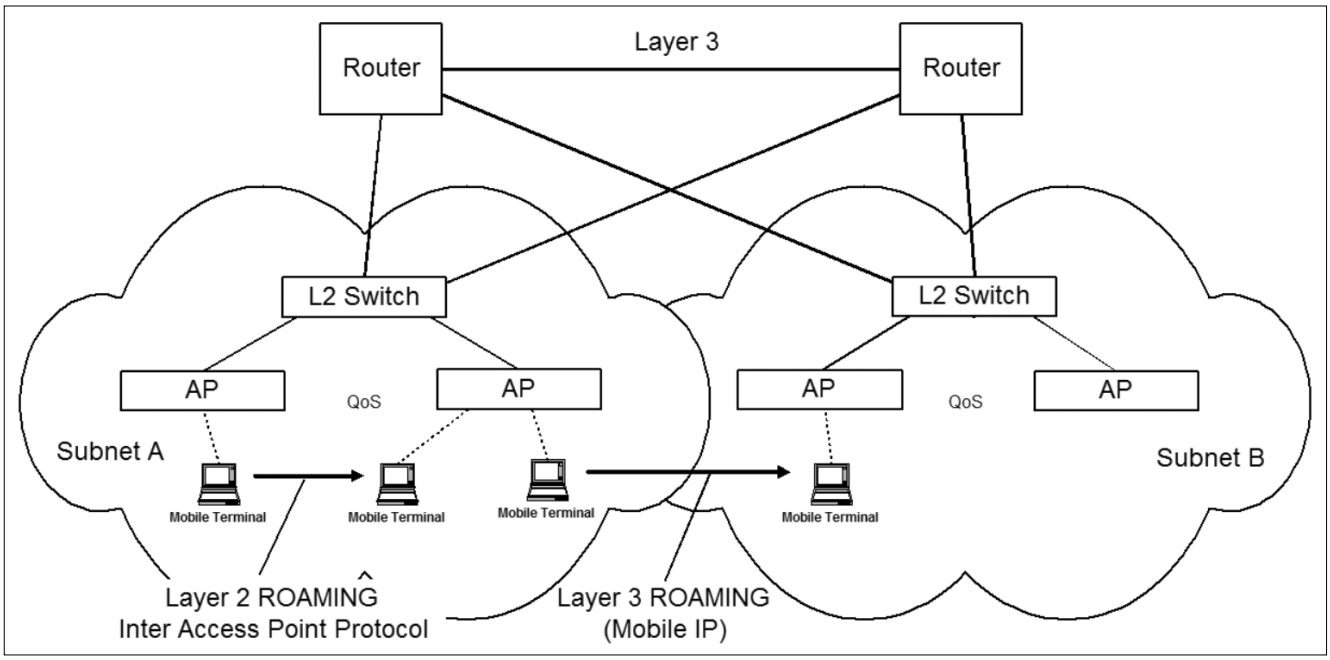
1) The terminal moves from cell "A" to cell "B". The access points belong to the same subnet, so it's an L2 roaming. As soon as the client gets out of cell "A", one of the parameters of the connection with AP_A reaches the given threshold and generates the roaming process.

2) The client scans all of the IEEE 802.11 radio channels, and looks for an available AP. After finding the AP_B, authentication and association phases occur on the physical radio channel.

3) The AP_B sends a zero content multicast message with a source MAC address identical to the address of the mobile terminal. Switches in the wired LAN update their CAM tables on the basis of this message. Therefore Ethernet frames addressed to the terminal reach AP_B instead of AP_A.

4) AP_B sends a multicast message with its own MAC address notifying all APs on the subnet that the terminal with the given physical address is associated to it. As the AP_A gets this message, deletes the MAC address of the mobile terminal from its association table.

Figure 1. The L2 and L3 roaming



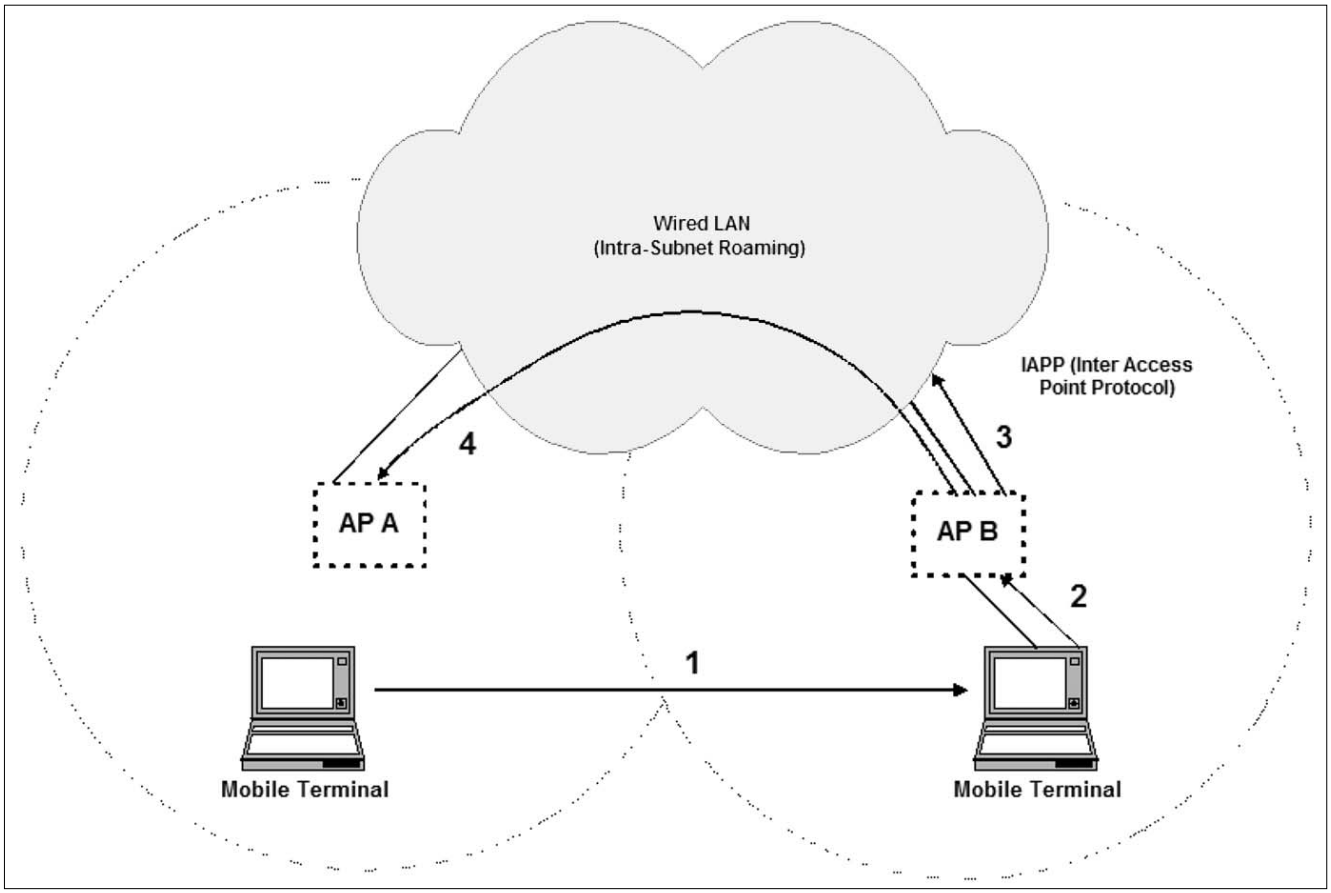


Figure 2. Steps of the L2 roaming

The roaming process is always initiated by the client, but no IEEE standard exists currently about this process [7]. Generally the roaming is triggered by the following events:

a) *Exceeding the Maximum Data Retry Count threshold:* when the client is uable to transmit the data after its preconfigured retry count, the station initiates a roaming process. This counter is set to 16 by default and is configured in the wireless adapter management software (e.g. Aironet Client Utility).

b) *Missing too many beacons:* all clients associated to an AP receive beacons periodically. APs send a beacon every 100 ms by default according to the beacon period configuration setting. A client learns about the AP's beacon interval from a beacon component. If the station doesn't receive eight consecutive beacons, the roaming event occurs and the roaming process is initiated. Even an idle client is able to detect the loss of radio link quality by monitoring the incoming beacons.

c) *Change of data rate:* Under normal conditions packets are transmitted at the AP's default rate. This rate is the highest that can be set as "enable" or "required" parameter on the AP. Every time a packet has to be retransmitted at a lower rate, the retransmit counter is increased by three. For packets transmitted successfully at the default rate, the retransmit counter is decreased by one, until it reaches zero. When this counter reaches 12, one of the following scenarios occurs: 1. If the client has not attempted roaming in the last 30 seconds then the roaming process occurs. 2. If the client has already attempted to roam in the last 30 seconds, the data rate for that client is set to the next lower rate. A client transmitting at a lower rate than the default one will increase the date rate to the next higher rate after a short time interval if transmissions are successful.

d) *Periodic Client Interval:* For Cisco Aironet v6.1, the rate and the signal intensity for the mobile terminal's search for a base station with better reception can be configured. With these settings, the client will look for a better base station when both of the following conditions have been met:

– The client has been associated to its current access point for at least 20 seconds. This restriction is needed to prevent a client switching between access points too rapidly. Valid values are from 5 to 255 seconds.
– The signal intensity is less than 50%. Valid values range from 0 to 75%. The periodic scan is a roaming event that causes the occurrence of the roam process.

e) *Initial Client Start-up:* When a client starts up it goes through the roaming process, to scan for and associate with the most appropriate access point.

Searching for a new AP is needed for the roaming process [3]. When a roaming event occurs the client station scans each 802.11 channel in order to determine the list of available APs and to select the best

one. On each channel the client station sends a probe, and waits for probe responses or beacons from access points on that channel. The probe responses and beacons received from access points are discarded unless they have matching Service Set Identifier (SSID) and encryption settings.

When the scan process is completed and the mobile client has a list of responding access points, it selects the access point to compare with the others. If the terminal is in its initial start up phase, then the new AP will be the first element of the list, when the terminal is in roaming phase then the new AP will remain the same if it answered to the test probe frames, in case of no answer the first element of the list will be the new AP.

The current access point is compared to each of the access points in the list. In order to be considered as a new current access point, each access point must meet all of the following conditions:

1) Signal intensity of the potential new AP is at least 20%. If signal is more than 20% weaker than the current one, signal intensity must be 50% or more.
2) If the potential new AP is in repeater mode, and it's distance from the backbone, in radio hops, is larger than the current AP, it must have 20% more signal intensity than the current base station.
3) The transmitter load of the roaming target AP can be at most 10 % higher than the current AP's load. The mobile client compares the access points that meet the base conditions with the current access point. If an accepted AP fulfills any of the following conditions, the terminal selects it as the new AP, henceforward the next AP of the list is compared to this new one: signal intensity is 20% higher than current, smaller hop distance to the backbone, at least four fewer clients associated to it than current access point, transmitter load is at least 20% less.

From 12.2.(11)JA IOS version, Cisco's "fast secure roaming" implementation has two additional features: more efficient 802.11 channel scanning during physical roaming, and an effective re-association mechanism applying more advanced encryption key management. The improved channel scanning results in faster L2 roam irrespective of the authentication method.

The key management speeds up the Cisco LEAP authentication process, therefore roam will be faster and safer. Both on Cisco terminals and base stations the channel scanning is enabled by default. Fast secure roaming is preceded by a channel scanning.

Before 12.2.(11)JA IOS version for a client station it took 37 ms to check a channel that took 431 ms total for 13 channels in case of European standards. For each channel the mobile client executes the following steps: when the radio hardware of the client tuned to the given WLAN channel, listens to avoid collision, then sends "probe" frames and waits for "probe response" or "beacon".

The channel scanning of fast secure roaming is more efficient: Re-associating clients now communicate information to the new access point such as the length of time since they lost association with the previous access point, channel number, and SSID. Using the information from client associations, an access point builds a list of neighbour access points and channels these access points were using. If the client reporting an neighbour access point was disassociated from its previous access point for more than 10 seconds its information is not added to the new access points list. Access points store a maximum list of 30 neighbour access points. This list expires over a one-day period. When a client associates to an access point, the associated access point sends the adjacent access point list to the client as a unicast packet.

When a client station needs to roam, it uses the list of neighbour APs it received from its current AP to reduce the number of channels it needs to scan. There are three roam types. Client uses them according to its activity.

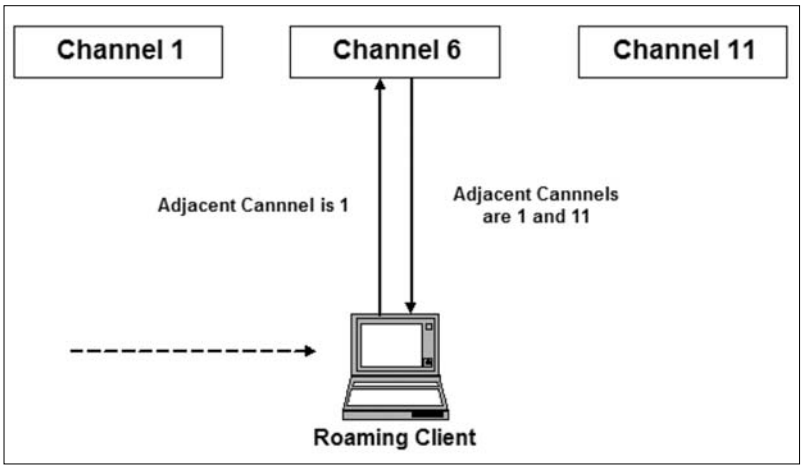
– *Normal Roam:* The client has not sent or received a unicast packet in the last 500 ms. The client does not use the neighbour access point list obtained from the previous access point. Instead it scans all channels valid for the operating regulatory domain.

– *Fast Roam:* The client has sent or received a unicast packet in the last 500 ms. The client scans the channels on which it has been told there is an adjacent access point. If no new access points are found after scanning the adjacent access point list, the client reverts to scanning all channels. The client limits its scan time to 75 ms if it is able to find at least one better AP.

– *Very Fast Roam:* the client has sent or received a unicast packet in the last 500 ms, and the client increases the load of the cell with a non-zero percentage. Same as Fast Roam except the scan is terminated as soon as a better AP is found.

Devices used in our test environment can operate in all of these three roaming modes.

Figure 3. Channel management of the fast roaming



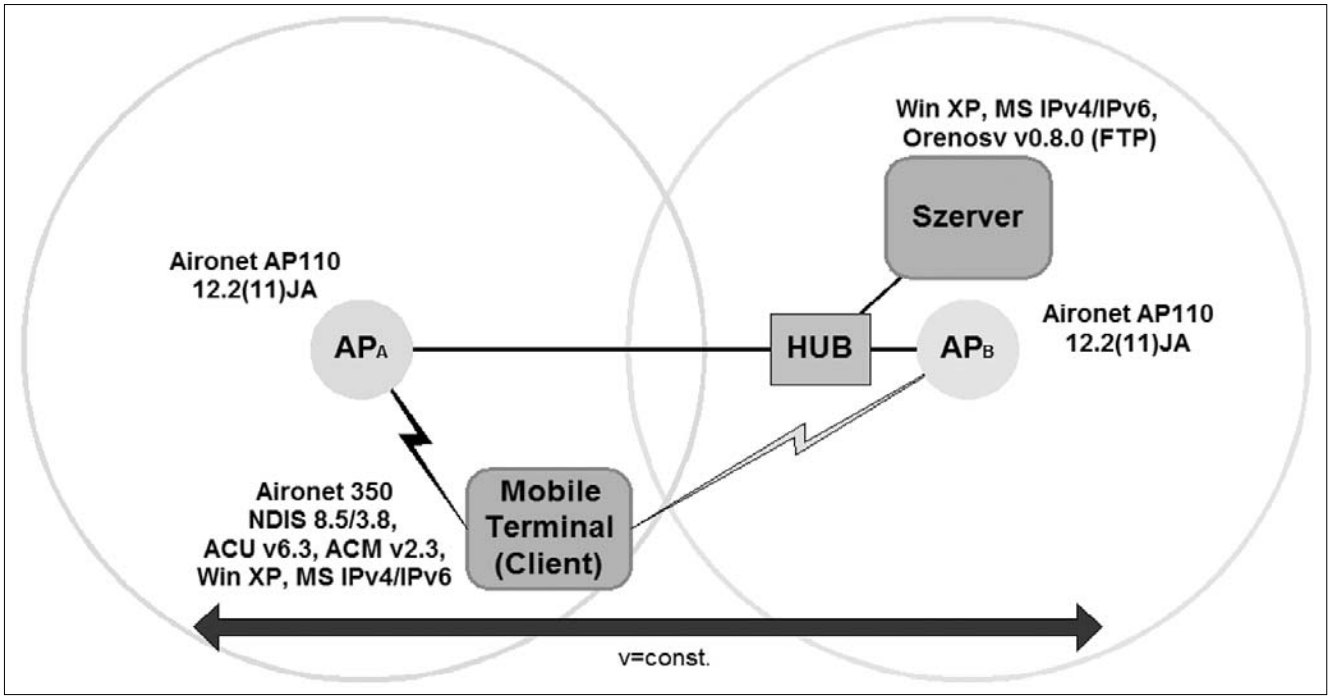


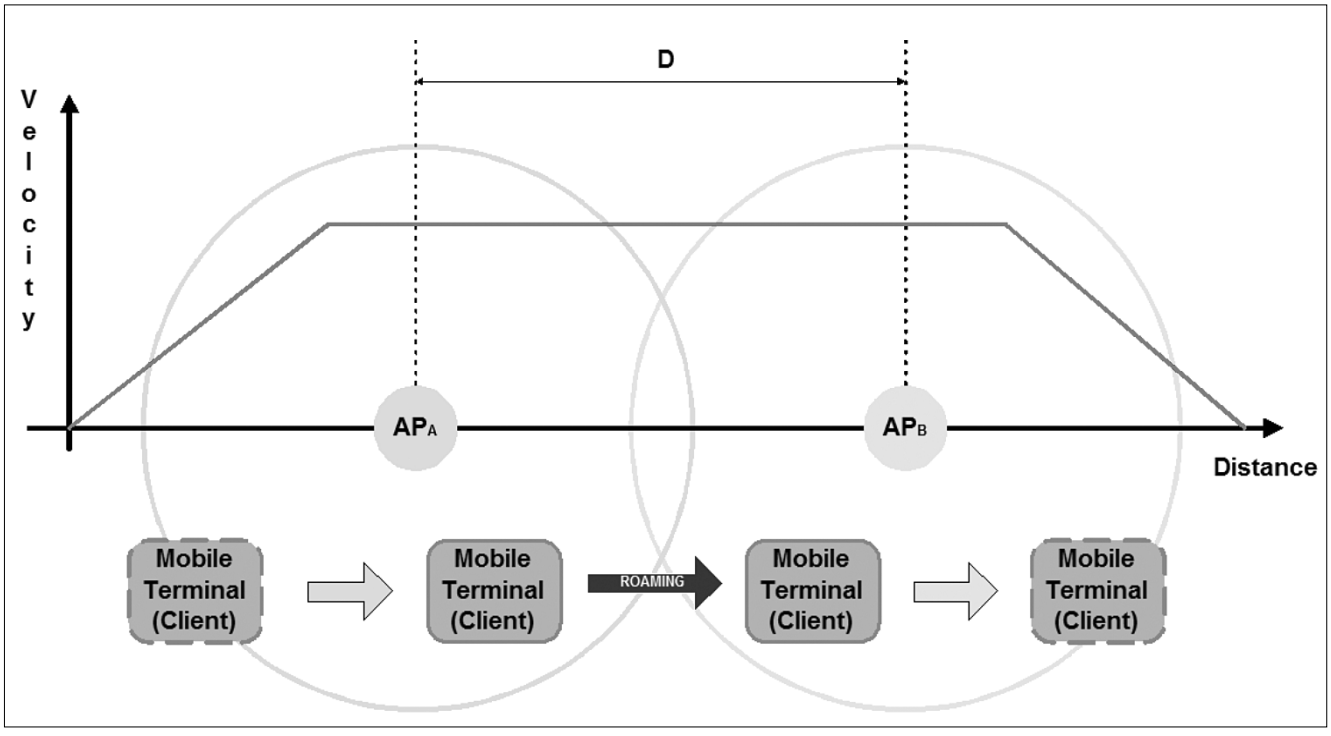
Figure 4. The measurement environment

4. Test environment

We set up an outdoor test WiFi system in order to study the behavior of the IPv4 and IPv6 protocols in mobile environment. The test is based on two APs operating according to the IEEE 802.11b standard, placed in 100 m distance from each other, linked with wired Ethernet connection, and a mobile terminal. As we know roaming is supported in the 11 Mbps WiFi standard. Whereas the speed of data transmission is strongly depend on the distance between the AP and the client station. During movement the client approaches to and diverges from the access point that causes the alteration of transmission speed in the data link layer.

In our measurements we fixed the transmission rate to 11 Mbps, this way the alteration of the radio signal strength forces the client station to initiate the roam process. We studied the behavior of the different transport layer protocols while the client station was moving on a vehicle (with constant speed during the roaming) paral-

Figure 5. The roaming process



Parameters		Independent measurements	
Access Point	Cisco Aironet AP1120	L4 protocol	TCP (FTP), UDP (Spray)
Mobile Terminal	Cisco Aironet 350 series	L3 protocol	IPv4, IPv6
AP IOS (1 mW)	12.2(11)JA	TCP traffic	MT > Server (Up) Server > MT (Down)
MT and server OS	Windows XP	UDP message [B]	18, 1472, 31970
MT Radio Firmware	Win/NDIS Driver 8.5/3.8, ACU v6.3, ACM v2.3	Speed [Km/h]	10, 30, 50
FTP server (IPv4/IPv6)	Orenosv v0.8.0	D(APA,APB)	100 m

Table 3.

lel to the line between the two access points. On the server side, the Ethereal snoop program was run, storing all of the L2's frames with unique timestamps for further analysis. During roaming the direction of data stream is important, because due to roaming, buffering is needed on the wired side (down) or on the wireless side (up) which significantly affects the operation of TCP connections.

We've selected three different sizes of ICMP message according to 64 bytes, 1500 bytes data link frame and 32 Kbytes in multiple frames. It's important for the minimal and maximal size of frame (MTU), and for the segmentation of IP packet. The speed of the vehicle was constant between the two APs, we were driving according the normal traffic rules applied for built-in areas (10 Km/h, 30 Km/h, 50 Km/h).

5. Measured parameters and evaluation

Using the frame sequence captured by Ethereal, we can interpret the signals of the roaming process, furthermore the traffic of the transport layer. So thus the roaming R[ms] and the traffic's drop out T[ms] became measurable.

FTP transmission of large files is realized based on the TCP's "Slow Start" and "Windowing" algorithms. The regulation of the window size is made necessary by the data rate alteration of the data link layer. The duration of the WiFi transmission's roaming phase strongly influences the efficiency of TCP.

UDP transport is much more adaptive by nature. We were sending 100 packets with spray ping which loaded the radio channel by 0.93, 21.82 and 100.0 percent depending on the packet size. Based on the measured parameters we can make the following observations *(see Figures 7-14)*:

• In case of ICMPv4 the time required for roaming is decreasing with the speed when frame size is under the default Ethernet MTU (1500 bytes), while with frames above the MTU it shows an increasing tendency. In case of segmentation it takes more time to reorder the packets. The ICMPv6 roaming time is decreasing with the speed at all frame size due to the medium sensing feature of the IPv6.

• Under the default Ethernet MTU frame size the loss of ICMPv4 traffic doesn't depend on the speed, whereas the delay is reduced by the segmentation. This virtual inconsistency is due to the persistent load of the radio channel. Strong fluctuation can be experienced with ICMP v6 in function of the speed, because IPv6 disconnects from the data link layer. The IPv4 doesn't perform this disconnection, so the ICMPv4 is less sensitive.

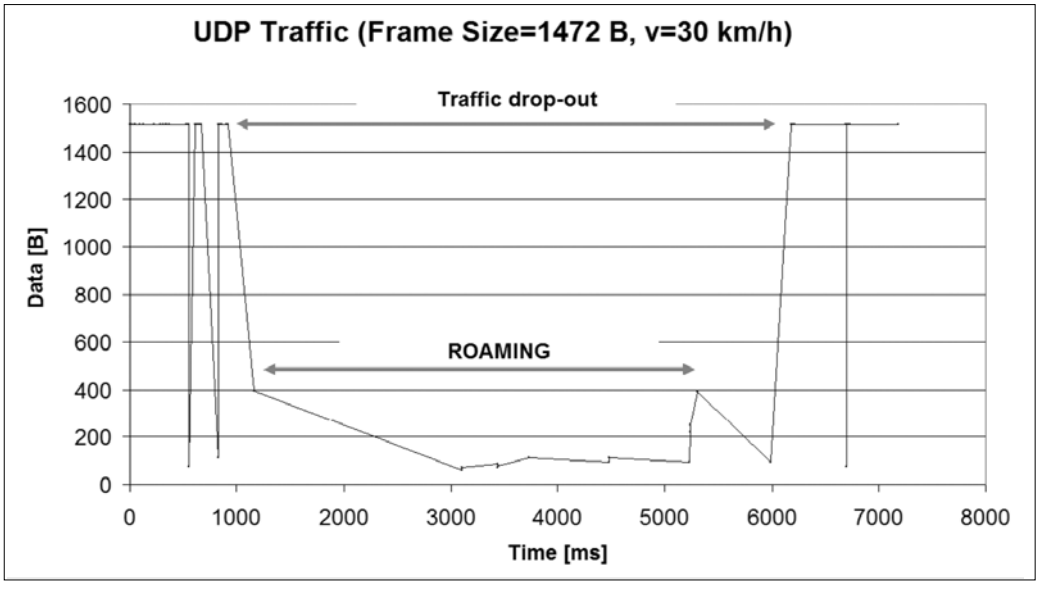


Table 6.
Measured parameters (R[ms], T[ms])

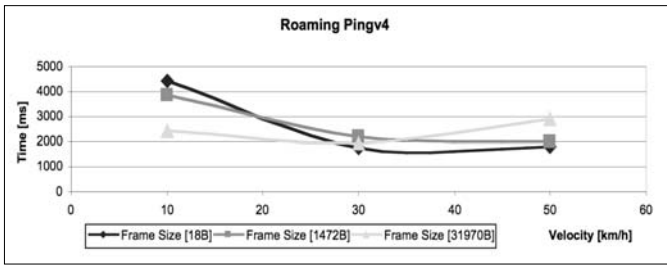


Figure 7.
Effect of the frame size to the roaming (ICMPv4)

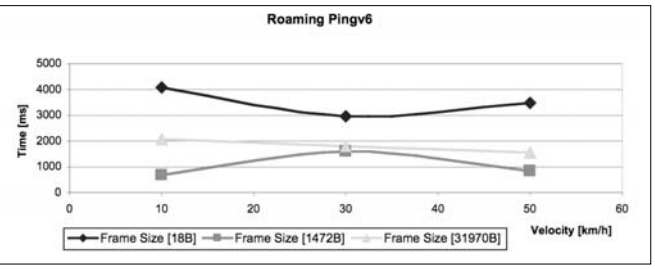


Figure 8.
Effect of the frame size to the roaming (ICMPv6)

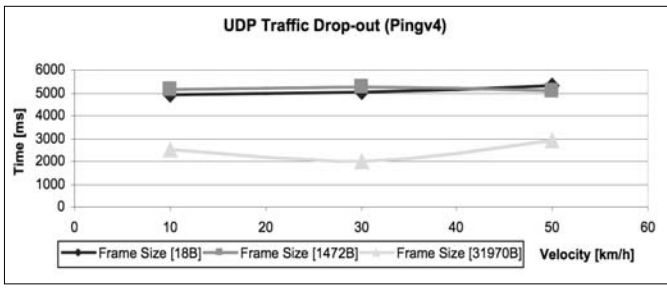


Figure 9.
Effect of the roaming to the UPD v4

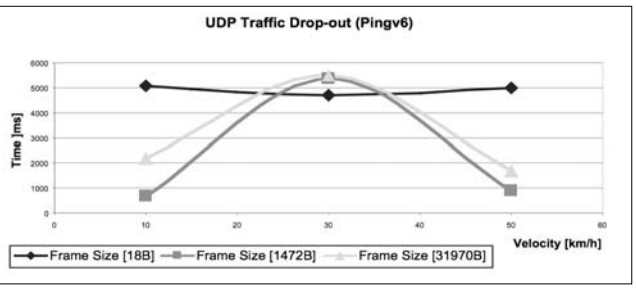


Figure 10.
Effect of the roaming to the UPD v6

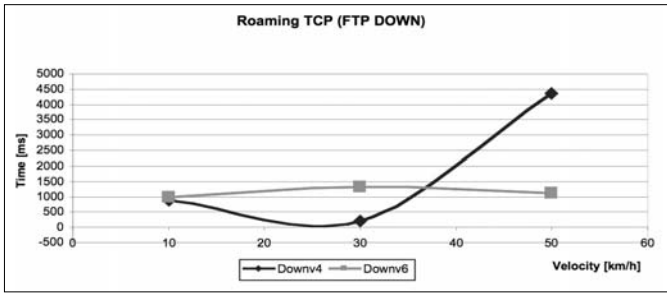


Figure 11.
Effect of the roaming (TCP download traffic)

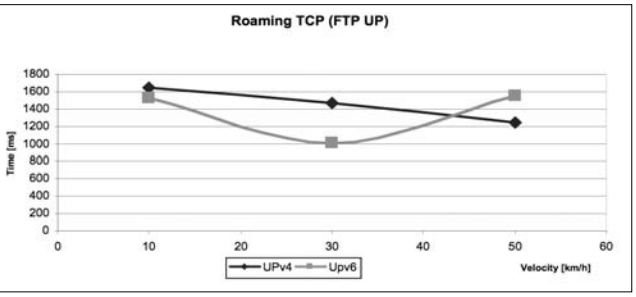


Figure 12.
Effect of the roaming (TCP upload traffic)

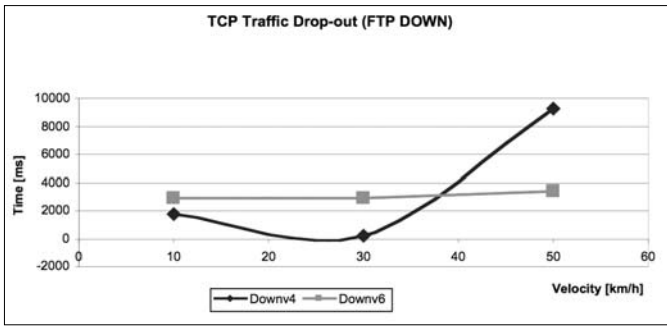


Figure 13.
Effect of the roaming (TCP download traffic)

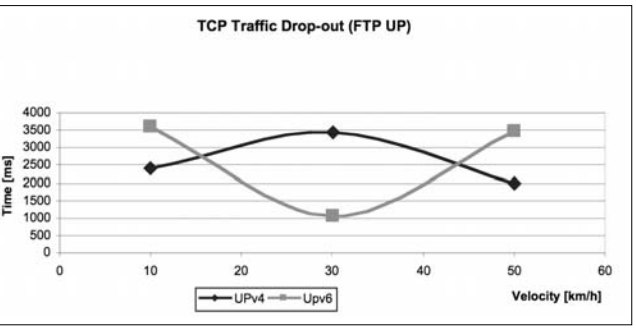


Figure 14.
Effect of the roaming (TCP upload traffic)

• The traffic dropout of ICMPv4 is 1.5 second longer, while the ICMPv6 dropout is 1 sec. longer than the roaming time. With smaller frame size the dropout depends less on speed, whereas at larger frames only IPv6 is sensitive to the speed.

• The dropout of TCPv6 is independent of the direction of data stream. In case of TCPv4 the download bears significantly more data loss than the upload. This is due to the quick window size alteration of the IPv4, therefore at download there's a high data loss because a great number of frames are sent to the previous AP.

• TCPv4 uses larger window size and slow dynamics, while TCPv6 applies smaller windows that are controlled quickly. Thus the IPv6 tolerates the roaming events of WiFi environment, resulting in the decrease of traffic loss.

• In case of download the loss of TCPv4 traffic strongly depends on the speed of the moving terminal station. It can produce a 9.2 seconds of dropout at speed of 50 Km/h that makes impossible to communicate from fast moving vehicle. In case of TCPv6 download this value doesn't depend on speed and can be

kept under 3.6 seconds. The dropout of TCPv4 upload traffic changes little with speed, while TCPv6 produces significant alterations.

6. Summary

TCP connections are affected significantly, while UDP connections are affected less significantly by the interaction between the mobile station's relative speed and the roaming execution [5],[6]. The results gained statistically from the comparative measurements provide us with a practical view on the behavior of IPv4 and IPv6 protocols in mobile environment, furthermore we can answer the question if the performance of IPv6 over wireless data link layer is really higher compared its predecessor IPv4.

The conventional applications provide slower transmission over mobile links due to the best effort nature of IPv4, while IPv6 assures effective data transfer because of its quick adaptation to lower layers. Time sensitive applications (IP phone, video conference) suffer significant dropouts due to the limitations of IPv4's QoS in mobile WiFi environment therefore the provided quality is unacceptable. The quick adaptation of IPv6 decreases the interval of dropouts [4].

A possibility for further investigation may be the analysis of quality influencing factors for communication services of mobile stations that move outside of built-up areas, at higher speed (on highways, train, etc.). Now we can also clearly see the necessity of future development: speeding up the roaming phase and development of IPv6 specific applications.

References

[1] Microsoft TechNet, The Cable Guy – Sept. 2004, "Introduction to Mobile IPv6": http://www.microsoft.com/technet/community/columns/cableguy/cg0904.mspx
[2] Charles E. Perkins (Sun Microsystems), "Nomadicity: How mobility will affect the protocol stack", http://www.computer.org/internet/v2n1/nomad.htm
[3] Microsoft Corporation, "Understanding Mobile IPv6", http://www.microsoft.com/downloads/details.aspx?FamilyID=f85dd3f2-802b-4ea3-8148-6cde835c8921&displaylang=en
[4] Ye Tian, Kai Xu, Nirwan Ansari, "TCP in Wireless Environments: Problems and solutions" IEEE Radio Communications, March 2005.
[5] Zoltán Gál, Andrea Karsai, "Videokonferencia rendszerek minőségi garancia jellemzőinek elemzése", NetworkShop 2004 – konferenciakiadvány, Széchenyi István Egyetem, Győr, 2004. április 5-7.
[6] Zoltán Gál, György Terdik, "Multifractal Study of Wireless and Wireline Datanetworks", 8th International Conference on Advances in Communications and Control, Telecommunications/Signal Processing – Proceedings, Crete, Greece, 25-29. June 2001.
[7] Cisco Systems, Inc., "Cisco Fast Secure Roaming"