# Performance Evaluation of Centralized IEEE802.11i-based Security Suites on Mobile WiFi Networks

Péter Orosz · János Sztrik · Seokjun Lee · Youngjin Oh · Chesoong Kim

In today's mobile wireless networks beyond the high degree of mobility, secure user authentication, data privacy and integrity are among the most important demands of advanced WiFi systems with good reason. In view of growing user demands, roaming service becomes available on wireless networks in order to provide infrastructure for mobile IP telephony, video conference and multimedia streaming applications, etc. Furthermore, private end-user data has to be protected by advanced security mechanisms that support roaming function. Accordingly, we are going to empiricaly investigate 802.11i-based security protocol suites (WPA, WPA2) in terms of performance and effectiveness in L2 roaming situations on both 802.11a and 802.11b/g systems. We separately focus on L2 roaming time, re-authentication performance of PEAP versions and encryption key exchange (TKIP, AES) and overall TCP dropout. Consequently, we intend to find a protocol combination that gives the best compromise between fast roaming time and security.

Keywords: mobility, IEEE 802.11a/b/g, roaming, IEEE 802.11i, WPA2, PEAP, TKIP, AES-CCMP, TCP

## I. OUTLINE

In the local area networking segment, the popularity of wireless transmission technology is dynamically growing due to the low cost of per-connection deployment besides mobility features. At the same time, WiFi transmission brought on complex security issues that need to be answered by network analysts. It is very important to examine how the novel security suites (WPA, WPA2) - including EAP-based authentication mechanisms (e.g. PEAPv0, PEAPv1) and data encryption protocols (TKIP, AES-CCMP) - impact the transmission parameters of the 802.11a/b/g mobile WiFi systems, especially the L2 roaming time. We already know from a previous analysis[1] that both TCP and UDP traffics are affected by the L2 roaming event that is due to happen during the physical movement of the mobile client. When data-link layer roaming evantuates, mobile terminal deassociates from the access point of the radio cell it is moving out from; and will attempt to reassociate to an access point that has the most auspicious signal parameters at its new physical position. The next essential step is the reauthentication phase that has already been effected in the latest EAP mechanisms. Thus, the following questions seem to be reasonable: How long does the reauthentication extend the traffic dropout period during roaming events? How are the upper layer protocols (TCP specially) impacted by the data loss in the wireless medium? Sophisticated data encryption mechanisms (TKIP, AES-CCMP) dynamically change the per-client unicast keys which consumes extra resources. Moreover, PMK shall be regenerated during roaming events. Consequently, key generation and exchange add some overhead on roaming time as well. By splitting the roaming event up to sub-

Peter Orosz, Janos Sztrik: University of Debrecen, Hungary
Seokjun Lee, Youngjin Oh and Chesoong Kim: Sangji University

processes (L2 LLC (Layer2 Logical Link Control) activity, re-authentication, re-keying) we are able to analyse protocol overheads in detail.

## II. INTRODUCTION - WiFi SECURITY OVERVIEW

### 1. WPA

The original security mechanism of IEEE 802.11b (WEP - Wired Equivalent Privacy) may be actually left out of consideration when secure encryption is required on our WiFi network [4]. IEEE 's network security task group aimed to design a new, advanced security suite to replace WEP. Therefore, 802.11i has been created. WiFi Alliance adopted an early version of the standard (draft 3.0) that is actually a special subset of the 802.11i security suite that can co-operate with legacy 802.11 hardwares. This is WPA (WiFi Protected Access) technology[3]. The original WEP uses 40-bit RC4 keys with 24-bit Initialization Vector (IV), furthermore, it gives protection against packet forgery by its CRC32 algorithm. Whereas, all of these solutions are not proven strong enough to achieve the desired wired-level privacy. An example of RC4 flaws in WEP is the small size of IV. Therefore a certain value is likely to be regenerated within a short period of time. This security vulnerability helps attackers in real-time decoding. Additionally, replay protection is not implemented within the algorithm.

WPA actually brings an intermediate solution for wireless security. Two types of its key management schemes are the followings: 1. WPA supports external authentication server (e.g. RADIUS) and EAP mechanisms[5]. 2. Authentication with pre-shared keys. The former is called WPA-Enterprise while the latter is WPA-PSK or Personal. Both generate master keys for each supplicant/authenticator communication session. It defines TKIP (Temporary Key Integrity Protocol) to replace WEP that may come into consideration as a compromise between secure communication and hardware compatibility. TKIP adapts RC4 stream cipher algorithm and generates 128-bit per-packet RC4 key to prevent key recovery attempts, moreover, it uses Michael MIC integrity algorithm against replay attacks.

WPA introduces a new 4-way key handshake algorithm for generating and exchanging the per-packet encryption keys between the access point and the mobile client. This mechanism can be also used to verify that both the access point and the client have already acquired the master key (PMK).

### 2. WPA2 & IEEE 802.11i

By June 2004, the development of missing parts of IEEE 802.11i was finalized. Hence, WiFi Alliance created an advanced WPA suite called WPA2 based on the final version of 802.11i. WPA2 supports the more complex and much stronger AES-CCMP (AES in Counter Mode with CBC-MAC Protocol) cryptographic algorithm that is a special block-mode version of AES-128. Besides the stronger encryption requirements, WPA2 also introduces two enhancements to support fast roaming between access points. By caching the PMK, WPA2 allows users to reconnect to an access point that they have recently connected to without re-authentication. Pre-authentication is also a novel feature of WPA2 that allows clients the pre-authenticate to the new access point they are moving towards without de-associating from the previous access point they are moving away from.

## III. DATA ENCRYPTION PROTOCALS

### 1. TKIP

TKIP is defined by IEEE 802.11i standard. Protocol designers had to find an intermediate solution combining high security level and functionality on legacy wireless hardwares. Accordingly, the new protocol uses the same RC4 algorithm as WEP. However, RC4 in TKIP operates with 128-bit keys. The most obvious change is the per-packet keying mechanisms where a unique key is generated for each data packet. These keys are derived from the mixture of some specific data, such as the source MAC address of the sender and packet id. Each packet contains a 48-bit sequence number that increases by 1 as soon as a new packet is transmitted. This value is used by the algorithm in the Initialization Vector (IV). Thus, this sequence number guarantees unique keys for each inidivdual packets.

TKIP specifies a set of four keys for each client/access point unicast communication instance and two additional keys for multicast and broadcast traffics[2]. PMK is determined during EAP authentication by the authentication server (RADIUS) together with the wireless client. Afterwards, it is propagated to the access point by the server encapsulated in an *Access-Accept* message. Thereafter, AP initiates 4-way key handshake so to

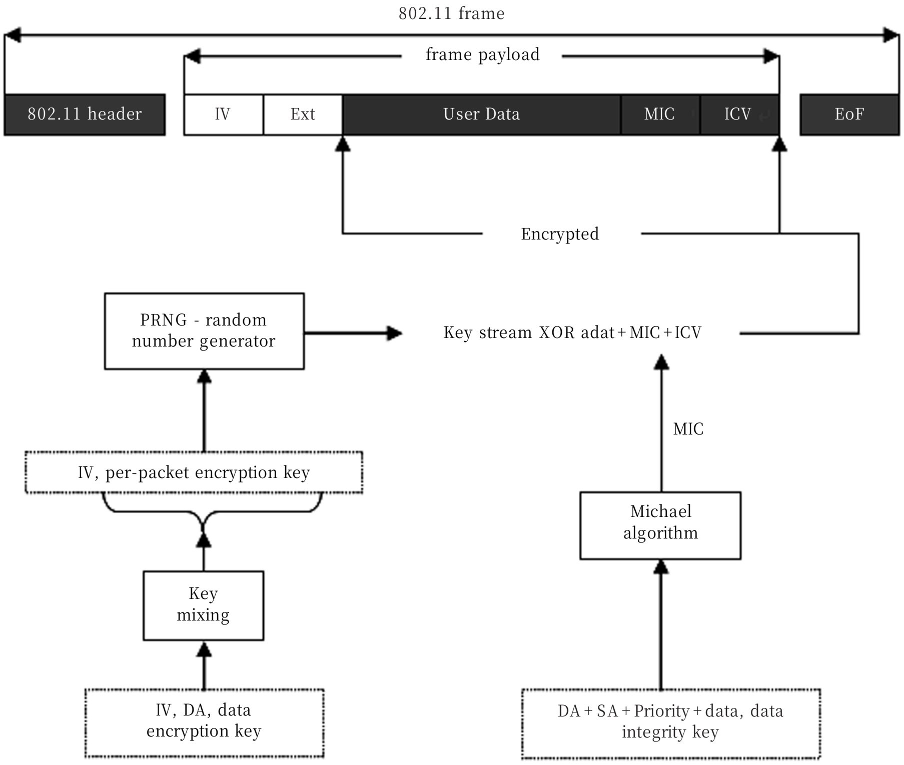

802.11 frame
frame payload
802.11 header
IV
Ext
User Data
MIC
ICV
EoF
Encrypted
PRNG - random number generator
Key stream XOR adat+MIC+ICV
MIC
IV, per-packet encryption key
Michael algorithm
Key mixing
IV, DA, data encryption key
DA+SA+Priority+data, data integrity key

Figure 1. The block scheme of TKIP

generate and exchange the temporary keys. The algorithm calculates these keys (PTK) and derivates the MIC value in order to verify the existence of PMK at both the access point and the client(See. Figure 1).

*The following components required to encrypt data frames:*

- Inicialization Vector (IV).
- Data Encryption or Group Encryption Key of the PTK
- Source and destination address of the frame (DA, SA).
- Value of the priority field, it is set to 0 by default.
- Data Integrity or Group Integrity Key of the PTK.

*TKIP Encryption Algorithm:*

① The IV, DA and Data Encryption Key will be applied as inputs of the WPA mixing function that calculates per-packet keys.

② Inputs of Michael data integrity algorithm for MIC generating are DA, SA, priority value, unencrypted data and data integrity key.

③ ICV is determined from the CRC-32 checksum.

④ Inputs of programmed random number generator of RC4 are the IV and the per-packet key to produce a key stream that has the same size as the data field, MIC and ICV values together.

⑤ Execute a logical XOR operation on the combination of key stream, data, MIC and ICV to generate encrypted 802.11 data.

⑥ Finally, it adds IV to the encrypted data and encapsulates the result between an 802.11 header and an End of Frame field.

## 2. AES-CCMP

Similarly to TKIP, CCMP specifies temporary keys (PTK) to encrypt data and the same 4-way key handshake algorithm to calculate keys. Data integrity protection has already been implemented within the protocol (both key management and integrity are handled by CCMP), therefore it can repace both TKIP and Michael. AES-CCMP applies counter mode AES to encrypt the 802.11 payload and MIC value, the latter is calculated by the CBC MAC algorithm. It operates on 4 x 4 array of bytes and has a fixed block size of 128 bits and key sizes of 128, 192 and 256 bits.

Table 1. Security solutions

| Technology | *Authentication* | *Encryption* |
|---|---|---|
| WPA | PEAP-MSCHAPv2 | TKIP |
| | PEAP-GTC | TKIP |
| WPA2 | PEAP-MSCHAPv2 | AES-CCMP |
| | PEAP-GTC | AES-CCMP |

Table 2. Notation

| Moments | Event Description |
|---|---|
| T1 | Last important TCP packet sent by the MT before L2 roaming |
| T2 | Begining of re-authentication phase |
| T3 | End of re-authentication phase |
| T4 | First important TCP packet sent by the MT after L2 roaming |

## IV. MEASUREMENT TEST-BED AND PARAMETERS

All of the wireless types of hardware used in our test-bed support communication according to IEEE 802.11a/b/g standards, as well as investigated security technologies. As some access points may have advanced vendor specific features we set all configuration parameters according to the transmission standard without any vendor extension. We focused on the combined effect of the mentioned transmission and security mechanisms on the physically moving wireless client. We measured and examined the effects that impact the roaming process of the moving client. Whereas, the QoS of the networking applications depends on the traffic dropout. The mobile client moved at 5-6 km/h (1,4-1,7 m/sec) in parallel with the virtual line that connects the APs. During one measurement period (TSi) MT associated to AP2 from AP1 afterwards it moved back and re-associated to AP1 as soon as it got back to its scope. The mobile terminal (MT) was a P4 PC laptop equipped with 512MB of RAM on which an FTP client was running. The wired side of the TCP session was a Linux based machine running a glFTP server. Large binary data files were moved from the FTP server to the client and back. Transfer rate was limited to 256KByte/sec which is a good approximation of the effective user bandwidth of a moderately loaded (12-15 clients) access point. We performed tests for both download and upload, whereas, the access point showed different behaviors depending on the direction of TCP flow.

Both access points were members of the same L2 VLAN and they were placed at 50 meters physical distance from each other in indoor environment. On wired side the traffic of the APs was mirrored to a SPAN VLAN and was captured and stored by tcpdump on the Linux machine. We used Ethereal version 0.10.14 to analyze the measurement data. Emitted radio power of the access points was set to 5mW for 802.11b/g communication and 12mW for 802.11a considering the optimal radio cell size for our measurements. As reference, measurements were performed with open authentication first, afterwards, we set different authentication (PEAPv0 that stands for PEAP-MSCHAP *Microsoft Challenge Handshake Authentication Protocol*, PEAPv1 - PEAP-GTC *Generic Token Card*) and encryption (TKIP - *Temporal Key Integrity Protocol*, CCMP - *Counter Mode CBC MAC Protocol*) combinations as shown in Table 1.

MT was passing from point A to point B and back. Distance between point A and B was 50 meters. We defined four moments in time to measure the effect of the above protocol combinations on roaming time and TCP dynamics. Roaming performance was severely affected by the beacon period set on the access points. We know from our previous analysis[1] that a relatively optimal L2 roaming performance for IEEE 802.11b/g transmission can be achieved with a beacon period set to <50ms. Accordingly, we performed the measurements with 40ms beacon period for both 802.11b and 802.11g communication. However, we must consider that a too low beacon period may cause multiple roaming events within the route from A to B in indoor environment due to the reflexion effect of the walls. For IEEE 802.11a we get acceptable result with a period of approx. 50ms, therefore, we fixed its value to 50.

As Table 2 shows, important TCP packets (LIP, FIP)

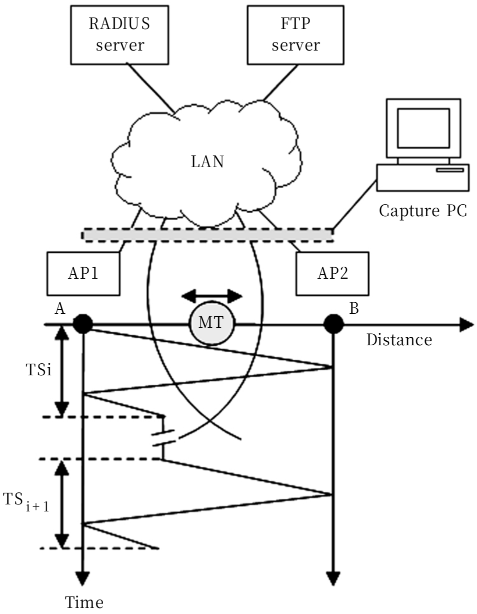


Figure 2. Test-bed

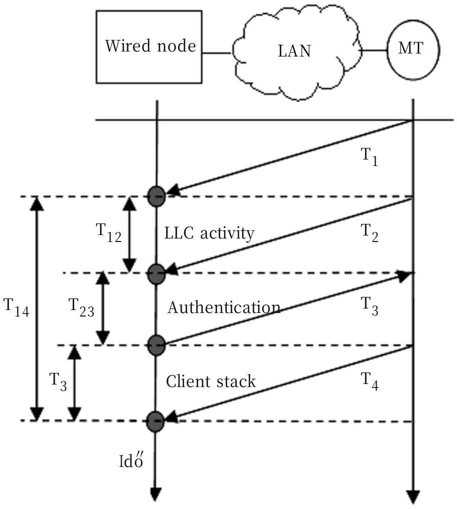


Figure 3. Measured periods

belong to the FTP session. Accordingly, we found it essential to differenciate them from other types of TCP traffic that may be generated by the client within the capture period. The first $T_{12}$ time interval is the time required for L2 roaming which has been already discussed in our previous paper[1]. $T_{23}$ is the re-authentication interval when 802.1x authentication eventuates between the RADIUS server and the wireless client. In this phase, PMK has to be determined and 4-way key handshake has to be initiated in order to generate temporary keys(See. Figure 2~3).

Straight after passing through these phases, encrypted data communication is due to begin between the client and the access point. During roaming, TCP connection is not dropped in most of the cases however, we experienced significant traffic dropout at the data link layer. $T_{34}$

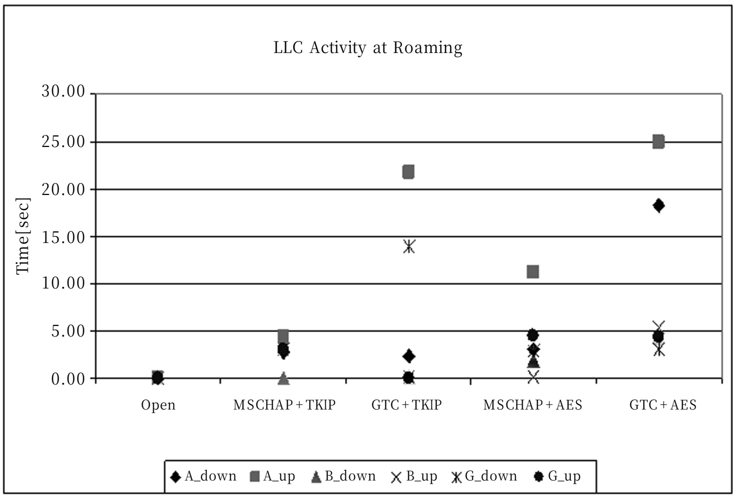


Figure 4. L2 Roaming period

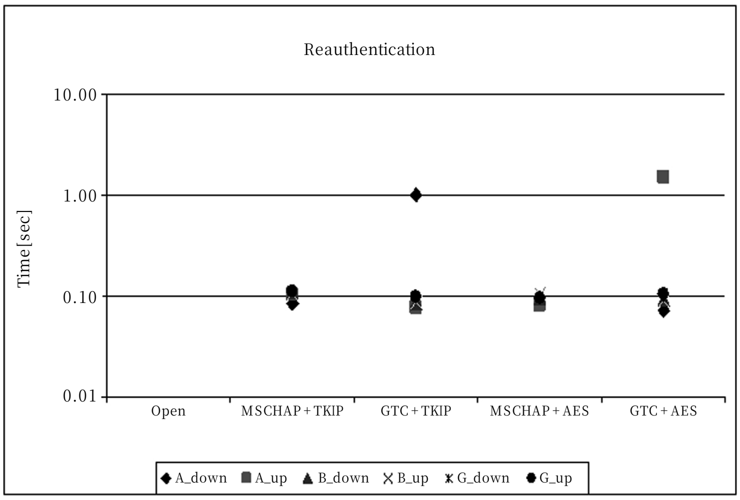


Figure 5. Re-authentication period

values indicate that TCP connection does not come up immediately, there is a noticeable time difference between the re-authentication phase and the first important TCP packet (FIP) which may depend on the TCP variant used on the mobile client.

## V. RESULTS AND CONCLUSIONS

The entire traffic stream was captured and stored at the wired side of the network to provide enough information about the roaming process for our in-depth analysis. During L2 roaming, the mobile client sends a well defined packet sequence towards the new access point, whereby we could easily determine the exact time of the roaming event in all measurement files. Since, we investigated on TCP traffic the most interesting questions remaining are how roaming sub-processes (L2 LLC activity, re-authentication, re-keying) affect the TCP data-flow and what differences are shown in time intervals of the different 802.11 technologies? On the following graphs, we splitted the roaming process up into four phases keeping the focus on the traffic direction. If we observe

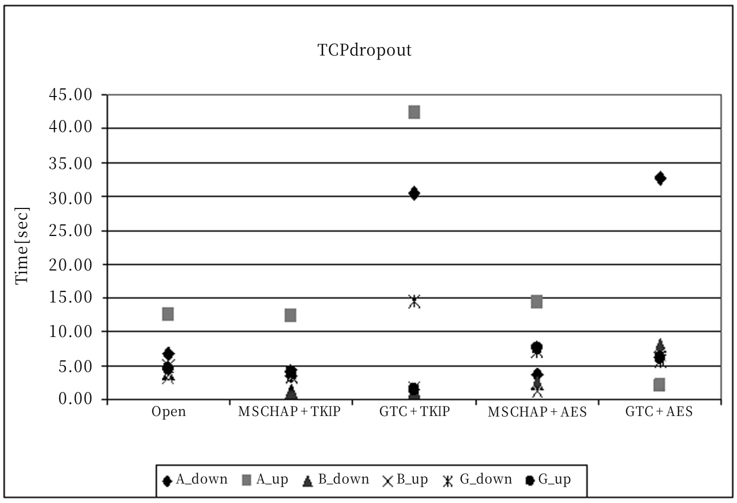


Figure 6. Overall TCP drop-out

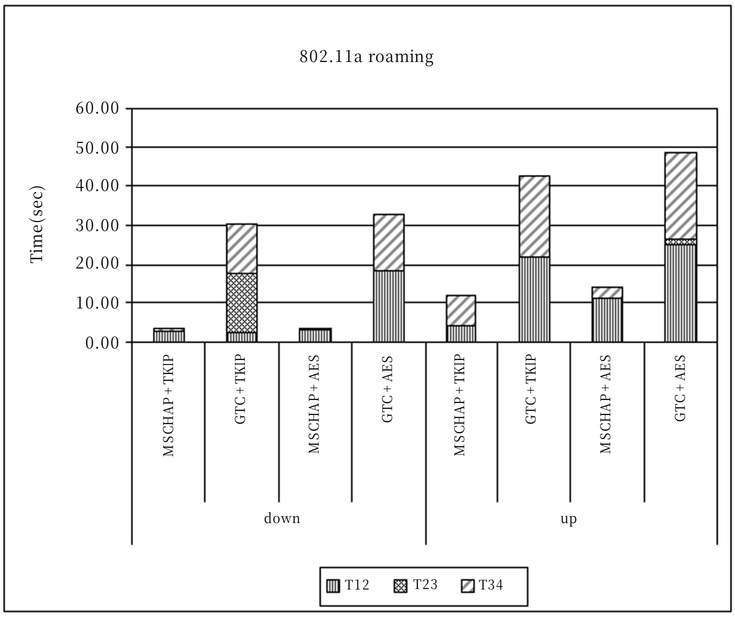


Figure 7. Authenticaton and encryption: 802.11a

any roaming phase, significant differences arise between authentication mechanisms (MSCHAP, GTC) as well as WiFi technologies (IEEE 802.11a/b/g). Time of the LLC activity actually depends on the applied PEAP version (See. Figure 4). At this point L2 roaming was faster with MSCHAP in all cases. Time interval is the function of TCP flow direction as well. If roaming occurs while client is performing a file download, some packets may have already arrived to the buffer of the access point the client is currently moving away from and initiates association to the new access point. Therefore, those packets have to be re-transmitted towards the new AP straight after the L2 switch updated its CAM table with the MAC address of the mobile client. Accordingly, the longer the overall roaming period, the higher number of TCP packets need to be re-transmitted which degrades TCP throughput as well

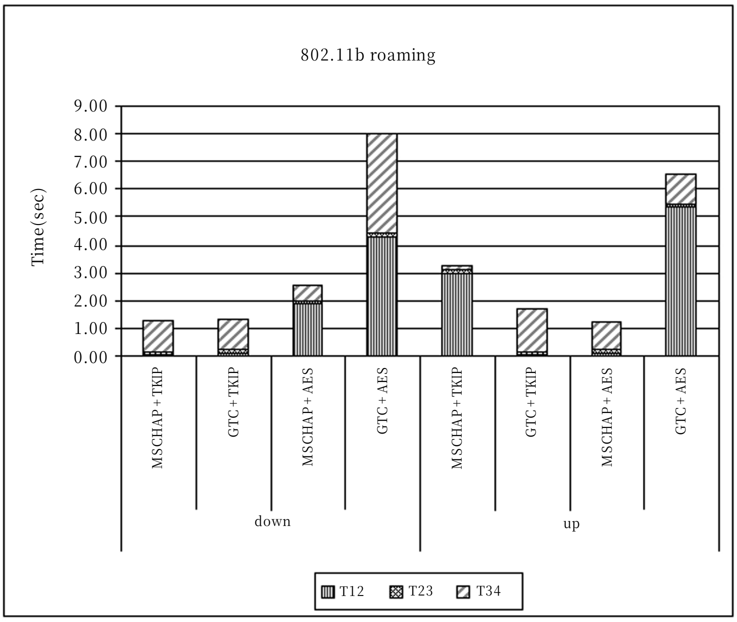


Figure 8. Authenticaton and encryption: 802.11b

as quality of service for networking applications. In the following graphs (Figure 4-6.) we noted the 802.11 communication types with a capital letter (stands for the 802.11 type) and a suffix (_up and _down) indicates the traffic direction on the mobile client.

In the re-authentication phase the difference has a much smaller order (<20ms) between the authentication mechanisms (See. Figure 5). Each authentication period is floating around 100ms. Extreme alterations on the graphs actually display the differencies between 802.11 technologies. IEEE 802.11a produced the worst roaming performance compared to 802.11b/g in all measurement phases. In extreme cases (802.11a+GTC+TKIP, 802.11a+GTC+AES) the time of re-authentication (approx. 1000ms) is one order higher than the average 100ms measured value. The reason why TCP has direction sensitivity is that the access point buffers the incoming packets, which may cause retransmission towards the new access point after the roaming event terminated. Furthermore, it connects two significantly different types of network medium.

Overall TCP drop-out is shown on Figure 6. This graph presents intervals between the last important packet (LIP) sent by the client to the previous access point and the first important TCP packet (FIP) sent towards the new access point. Unfavourable values are performed by the combination of 802.11a and PEAP-GTC. Whereas, we achieved especially good results with the combination of 802.11g/b and PEAP-MSCHAP, where in some cases (MSCHAP+TKIP, MSCHAP+AES), measured values are close to open authentication values due to the PMK-caching function.

When we compare the roaming performance of 802.11 technologies (See. Figures 7, 8 and 9) we can assume that the highest measured values are presented by 802.11a IEEE standard[6]. In this technology the physical size of the micro cells is smaller than that of the 802.11b/g access point transmitting with the same radiation power. Consequently, cells of the 802.11a access points located at 50 meters distance from each other are less overlapping. In order to compensate this phenomenon, we can increase the emitted radio power. Whereas, we need to consider the 40mW limitation of emitted power of the 802.11a technology operating in the 5.4GHz frequency range and the wave reflexion effect of the walls[6].

# VI. SUMMARY

In this paper we have investigated the performance of IEEE802.11i-based security suites on IEEE802.11a/b/g mobile WiFi systems. We have focused on L2 roaming events. We found that the 802.11a standard cannot prove its efficiency in terms of mobility. Obviously, apart from presenting longer intervals for all measured phases,

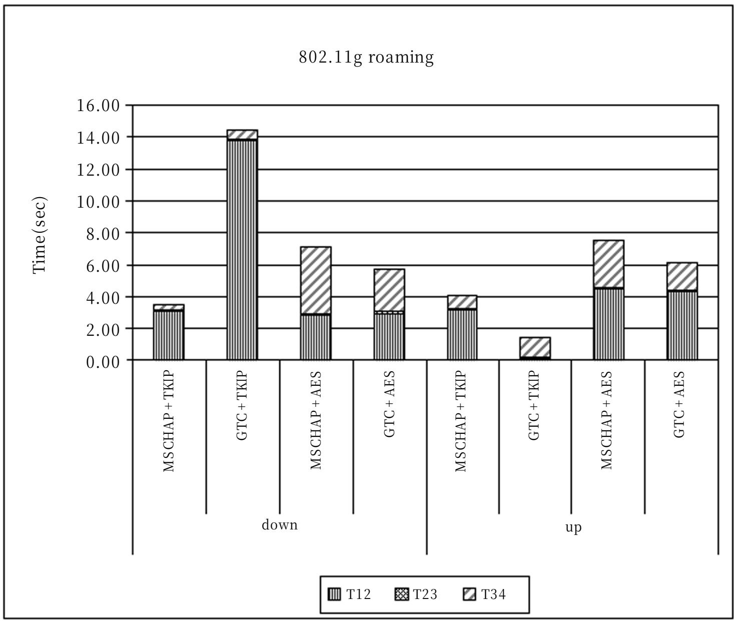


Figure 9. Authenticaton and encryption: 802.11g

roaming events produced disconnection of the TCP session in several cases. However, 802.11a operates at 5.4GHz frequency range that is less congested. All of the measured security protocol combinations added their overhead to roaming time. Therefore, the QoS parameters experienced at the application layer are declined. If we observe any roaming phase, significant differences arise between authentication mechanisms (MSCHAP, GTC) as well as WiFi technologies (IEEE 802.11a/b/g). Time of LLC activity actually depends on the applied PEAP version. At this point L2 roaming was faster with MSCHAP in all cases. However, differencies between the performance of authentication and encryption mechanisms are smaller of order compared to the transport layer latency that is in the second domain. In the re-authentication phase differences were much smaller of order between EAP types. This minor difference lies in complexity, processing time and the number of message exchanges. In mobile WiFi environment the quality of service experienced in the application layer depends on a complex roaming process, where the overall perfomance is the function of several components within the protocol stack, emphasising the importance of the applied TCP congestion control mechanism. The longer the overall roaming period, the higher number of TCP packets need to be re-transmitted which degrades TCP throughput as well as quality of service. Based on the experiences of this paper, we are going to focus on alternative TCP congestion control mechanisms that will be subject of an extensible investigation in mobile WiFi environments.

## Acknowledgements

This work was supported by Hungarian Scientific Research Fund-OTKA K 60698/2006 and KOSEF-HAS Bilateral Scientific Cooperation under grant KOSEF-F01-2006-000-1004-0. Special thanks to Zoltán Gál and Andrea Karsai for cooperating in the measurements. This research has been supported by Sangji University Research Fund 2007

## [References]

[1] Zoltán Gál, Andrea Karsai, Péter Orosz, "Evaluation of IPv6 Services in Mobile WiFi Environment," *Selected Papers of Info-Communication-Technology*, Vol. LX., 2005., pp 47-54.

[2] Wi-Fi Protected Access Data Encryption and Integrity: http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx

[3] Securing Wi-Fi Wireless Networks with Today's Technologies:http://www.wi-fi.org/files/uploaded_files/wp_4_Securing%20Wireless%20Networks_2-6-03.pdf

[4] Scott Fluhrer, Itsik Mantin, Adi shamir, "Weakness in the Key Scheduling Algorithm of RC4,"

http://www.crypto.com/papers/others/rc4_ksaproc.pdf

[5] Péter Orosz, János Sztrik, Kim Che Soong, “ Kö zpontosított EAP alapú hitelesítés vezeték nélkü li hálózatokban ”, *Informatics in Higher Education 2005 Conference, Hungary.*

[6] Zoltán Gál, Andrea Karsai, Péter Orosz, "Effect of WiFi systems on multimedia applications," *Networkshop*

**Péter Orosz**

Péter Orosz is a PhD student of Informatics Systems and Networks at the Faculty of Informatics, University of Debrecen, Debrecen, Hungary. He studied computer science at University of Debrecen 1997-2003, obtained M.Sc. in 2003, major in System Engineering. He is working as network engineer at the Directorate of Informatics at University of Debrecen. His research interests are in the fields of cross-layer protocol analysis and performance analysis of data communication networks. Last year he participated in a research project in the Network Research Laboratory at Queen Mary, University of London, UK. In recent years, he has published papers and conference presentations about TCP performance analysis on WiFi and high speed networks.

E-mail: oroszp@delfin.unideb.hu
Tel:+36-52-409-901
Fax:+36-52-416-857

**János Sztrik**

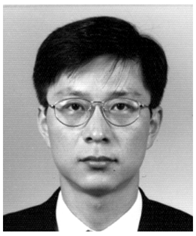
János Sztrik is a Full Professor and Head of Department of Informatics Systems and Networks at the Faculty of Informatics, University of Debrecen, Debrecen, Hungary. He studied mathematics at University of Debrecen 1973-1978, obtained the M.Sc. in 1978, Ph.D. in 1980 both in probability theory and mathematical statistics from the University of Debrecen. Received the Candidate of Mathematical Sciences degree in probability theory and mathematical statistics in 1989 from the Kiev State University, USSR, habilitation from University of Debrecen in 2000, Doctor of the Hungarian Academy of Sciences in 2002. His research interests are in the field of production systems modelling and analysis, queueing theory, reliability theory, and performance analyis of telecommunication systems. He is the leader of Applications of Queueing Methods in Reliability Theory and Computer Performance Research Group supported by the Hungarian National Foundation for Scientific Research. Main coordinator of Hungarian-German, Hungarian-Finnish, Hungarian-Korean bilateral intergovernmental scientific cooperations, participant of several national and international projects. He has published 4 theses, 3 books, 13 lecture notes, 116 papers, 38 research reports.

E-mail: jsztrik@inf.unideb.hu
Tel:+36-52-409-901
Fax:+36-52-416-857

### Seokjun Lee

Seokjun Lee received his B.S. and M.S. degree in Industrial Engineering at Sangji University, and his PhD in School of Business Administration at Sangji University in 2007. His current field of scientific interests is in e-commerce, queueing network modeling and their applications, collaborative filtering on the recommender system and data mining.

E-mail: crco909@yahoo.co.kr
Tel:+82-33-730-0460
Fax:+82-33-743-1115



### Young-Jin Oh

Young-Jin Oh received his Master degree and Doctor degree in Engineering from Department of Industrial Engineering at Hanyung University in 1988 and 1996. He is currently professor of the Department of Industrial Engineering at Sangji University. His current research interests include various aspects of system analysis and design, HCI and R&D.

E-mail: yyjjoo@sangji.ac.kr
Tel:+82-33-730-0462
Fax:+82-33-743-1115

### Chesoong Kim

Chesoong Kim received his PhD in Engineering from Department of Industrial Engineering at Seoul National University in 1993. He was a Visiting Scholar in the Department of Mechanical Engineering at the University of Queensland, Australia from September of 1998 to August of 1999. From July of 2004 to August of 2005, he was foreign scientist in the School of Mathematics & Statistics at the Carleton University, Canada. He was also a Visiting Professor in the Department of Industrial Engineering at the University of Washington, USA from August of 2005 to August of 2006. He is currently Full Professor and Head of Department of Industrial Engineering at Sangji University. His current research interests are in stochastic process, queueing theory, with particular emphasis on computer and wireless communication network, queueing network modeling and their applications, and reliability analysis. He has published around 60 papers in internationally refereed journals such as RESS, ITOR, IJRQSE, Mathematical & Computer Modeling, ANZJS, Statistics & Probability Letters, A&RC, Queueing Systems, Operations Research Letter and Annals of OR.

E-mail: dowoo@sangji.ac.kr
Tel:+82-33-730-0464
Fax:+82-33-743-1115