ATINER CONFERENCE PAPER SERIES No: COM2013-0593

Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
COM2013-0593

# Latency Evaluations and Reduction Techniques in Authentication Phase of Centralized WLAN Hotspot Networks

**Hasbullah Mazlan**
**Universiti Teknologi Malaysia (UTM)**
**Johor, Malaysia**

**Shariq Haseeb**
**MIMOS Berhad**
**Kuala Lumpur, Malaysia**

ATINER CONFERENCE PAPER SERIES No: COM2013-0593

**Mohammed Abobakr Ahmed Balfaqih**
**International Islamic University Malaysia**
**Selangor, Malaysia**

**Siti Norhaizum Mohamad Hasnan**
**International Islamic University Malaysia**
**Selangor, Malaysia**

**Muhammad Faheem Mohd Ezani**
**MIMOS Berhad**
**Kuala Lumpur, Malaysia**

ATINER CONFERENCE PAPER SERIES No: COM2013-0593

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209
Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm



ISSN **2241-2891**
1/10/2013

# An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. The papers published in the series have not been refereed and are published as they were submitted by the author. The series serves two purposes. First, we want to disseminate the information as fast as possible. Second, by doing so, the authors can receive comments useful to revise their papers before they are considered for publication in one of ATINER's books, following our standard procedures of a blind review.

Dr. Gregory T. Papanikos
President
Athens Institute for Education and Research

This paper should be cited as follows:

**Mazlan, H., Haseeb, S., Abobakr Ahmed Balfaqih, M., Norhaizum Mohamad Hasnan, S. and Faheem Mohd Ezani, M.** (2013) **"Latency Evaluations and Reduction Techniques in Authentication Phase of Centralized WLAN Hotspot Networks"** Athens: ATINER'S Conference Paper Series, No: COM2013-0593.

# Latency Evaluations and Reduction Techniques in Authentication Phase of Centralized WLAN Hotspot Networks

**Hasbullah Mazlan**
**Universiti Teknologi Malaysia (UTM)**
**Johor, Malaysia**

**Shariq Haseeb**
**MIMOS Berhad**
**Kuala Lumpur, Malaysia**

**Mohammed Abobakr Ahmed Balfaqih**
**International Islamic University Malaysia**
**Selangor, Malaysia**

**Siti Norhaizum Mohamad Hasnan**
**International Islamic University Malaysia**
**Selangor, Malaysia**

**Muhammad Faheem Mohd Ezani**
**MIMOS Berhad**
**Kuala Lumpur, Malaysia**

**Abstract**

Centralized Wireless Local Area Networks (WLANs) are becoming increasingly popular in public hotspot deployments. This is because centralized networks make use of a single infrastructure network where several Access Points (APs) connect to the network for services such as Quality of Service (QoS), traffic control, access control, roaming, SNMP and billing. Even though centralized network deployments are robust, secure and easily expandable, they pose high handover latency for mobile clients that move from one AP to another. While roaming, mobile clients have to perform scanning, authentication and association, 802.1x authentication and key management processes. These processes take a long time and pose a challenge for real-time applications that are sensitive to network latencies. This paper aims to experimentally evaluate the latencies involved in different processes of roaming under erroneous and non-erroneous conditions. The paper further proposes a mechanism to reduce the overall handoff latency by 260 times for real-time applications by eliminating the 802.1x authentication latency.

**Keywords:** Real-time applications, roaming, authentication, association, 802.1x.
**Corresponding Author:**

## Introduction

Typical Wi-Fi hotspot deployments in the past were autonomous, consisting of a single AP connected to a single backhaul network with pre-shared key for authentication. This type of AP is known as full MAC or fat AP because the entire MAC layer is built into the AP. The AP packs enough processing and storage capacity to manage network processes within itself. However, this increases the cost of deployment and is not scalable.

A modern Wi-Fi hotspot deployment consists of a central core network that is connected to at least one backhaul network. Several APs are then connected to the central network for utilizing services such as authentication, association, accounting, QoS, network management and bandwidth control. In a centralized network, AP does not need to implement all the functionalities of the MAC. It may choose to only implement the real-time MAC for packet processing and hence, it does not need high CPU or memory resource. This makes centralized network architectures ideal for campuses, shopping malls, enterprise and even small towns or villages.

Centralized networks are cheaper and more robust compared to autonomous architectures. However, they implement several latency inducing protocols during the roaming process when a mobile client moves from one AP to another. During initial connection, mobile clients scan for APs and then initiate a connection with the selected AP. The AP then authenticates the clients with a RADIUS server before serving the clients. However, during roaming, when mobile clients move to another AP, they have to re-authenticate themselves with the RADIUS server. The authentication and re-authentication process takes a long time and during this process, no communication can take place.

Continuous Internet connection is a requirement for Real-time Applications (RTAs) such as gaming, audio, video and voice. They require low latency, real-time frames, seamless connectivity and fast data transfer. VoIP can be categorized as the most latency constrained application because voice is very sensitive to missing, deformed or delayed frames during communication. The minimum latency for most constrained RTA is strictly not more than 150ms [1] while, the centralized WLAN architecture has much higher latency than that.

This paper aims to characterize the handover latencies in a centralized WLAN deployment architecture. It further aims to identify the latency components and implements mechanism to eliminate high latency components for reduced overall handoff latency. This paper briefly describes the WLAN architectures, current WLAN authentication mechanism, and the evaluation of latency during the roaming process. Latency during roaming is extracted from a centralized WLAN test-bed developed by us. The rest of the paper is organized as follows. The next section explains the related work, followed by the WLAN deployment architectures. Section 4 discusses the roaming latencies. Following section highlights our proposed solution. Test-bed setup is

discussed in section 6. Results are discussed in section 7 followed by a conclusion.

## Related Works

Previous works on WLAN network architectures focused mostly on autonomous and distributed architectures [2, 3]. This is because autonomous architecture can configure devices independently while distributed architecture can delegate all decisions on mobility management to the access points like a mesh network. However, previous studies have revealed that centralized architecture is suitable for enterprise Wi-Fi network due to the simplicity in handling different kinds of AP vendors [4].

The previous works on different types of APs have focused on "Thin" AP and "Fat" AP since both APs have 802.11 MAC Layer inside Access Controller (AC) for managing and controlling a collection of heterogeneous Wireless Termination Points (WTPs). Besides, both APs are easy to use especially for enterprise Wi-Fi planner to deploy enterprise Wi-Fi with secured connection [5].

There have been many studies comparing latencies for open-system and secure authentication mechanisms during roaming in IEEE 802.11 [6,7,8]. However, no research has been done on the effects of wireless error on re-authentication latency during handover process. The wireless errors occur because of packet loss during transmission due to collision or weak signal cause by attenuation, fading and multipath [9].

There is no past work on eliminating authentication latency to reduce the overall handoff latency in a centralized WLAN architecture and this can be considered as a major contribution of this paper to the research community.

## WLAN Deployment Architectures

Autonomous, centralized and distributed architectures, are the three types of WLAN deployment architectures in existence today. These architectures can be individually deployed in a variety of places to suit the need of the scenario [3, 5].

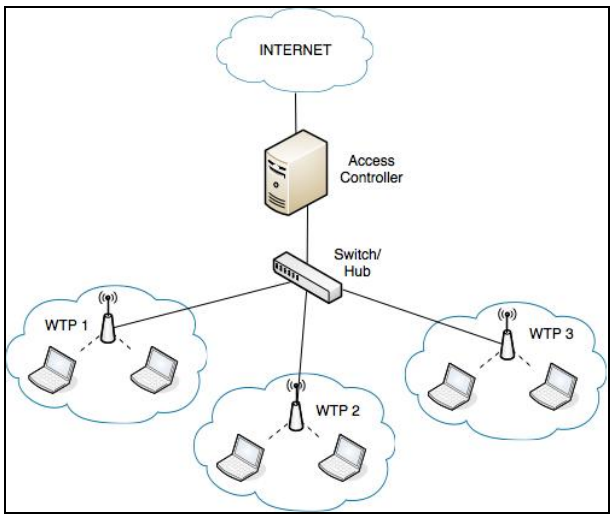
In an autonomous architecture, all 802.11 MAC functions and necessary core network functions are implemented directly into the APs. APs operating in autonomous mode are referred to as "Fat" APs [5]. "Fat" APs have many enterprise features such as identity and Simple Network Management Protocol (SNMP)-based management. From 802.11 MAC layer concepts, "Fat" AP uses local MAC implementation involving all 802.11 functions implemented in WTP/AP [3].

Distributed architecture is implemented in mesh network where the network intelligence is distributed between the nodes that form the network. The nodes exchange information with each other to perform network services

such as bandwidth control, routing, Virtual Local Area Networks (VLANs) and QoS. This paper does not discuss Autonomous and Distributed architectures, as they are not popular architectures for hotspots.

Fig. 1 illustrates the centralized architecture that requires an AC, which acts as a central point for handling several APs. In this architecture, most of the core network functions reside on the AC and the APs are reduced or no MAC devices. No MAC APs are known as "Thin" APs because their only function is to transmit and receive packets to and from wireless clients like a smart antenna system [10]. Reduced MAC APs are known as "Fit" APs because real-time functions of the MAC are implemented on the AP while the non real-time functions of the MAC are implemented on AC. Both "Thin" and "Fit" APs are much cheaper than "Fat" APs [11,12,13,14].

**Figure 1.** *Centralized Architecture*




## Roaming Latencies

Upon successful connection between the AP and the AC, clients are allowed to connect to the AP and roam between APs for accessing the network services. However, client connection and roaming between the APs is governed by the IEEE 802.11 scanning, authentication and association protocols.

During roaming, when a mobile client detects weak signal from its current AP, it starts to perform the scanning phase. In the scanning phase, mobile client waits for beacon frames to identify potential APs on each channel. It then sends a series of probe request and waits for responses before making a physical connection with an AP. The scanning phase usually takes between 400ms and 600ms. Although this is too high a latency for real-time applications like voice, there have been several studies in the past on reducing the scanning phase latency. Some of the studies propose the use of dual radio where one radio scans while the other transmits and receives. Other studies propose the use of selective scanning where only a selected group of channels are scanned for

determining the next AP. There have also been proposals on geo-location based scanning. Reduction of scanning phase latency is a very well researched area and is not the focus of the paper. This paper aims to reduce the latencies during the authentication and association process.

There are many secured authentication mechanisms defined by IEEE 802.11, such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA) and WPA2. These mechanisms offer varied degree of security. WPA2 was introduced to replace WEP and WPA due to their security weaknesses. WPA2 can either operate in personal mode or enterprise mode. WPA2-Personal authentication scheme, it is designed for small networks such as home and small buildings because their ease of deployment [15]. WPA2-Personal also refers to WPA2-PSK (Pre-Shared Key) scheme. In WPA2-Personal authentication, the AP sends a challenge to the client and requires the client to encrypt and send it back to the AP. The AP will decrypt and encrypt the challenge response by the client. If the challenge matches the response, the AP will grant the connection to the client.

WPA2-Enterpise authentication, also known as WPA2-802.1x or WPA2-EAP (Extensible Authentication Protocol) scheme is deployed in a centralized WLAN architecture. This authentication scheme requires external authentication server like RADIUS for secure authentication process and is considered to be extremely secure [16]. Fig. 2 shows the timing diagram of WPA2-Enterprise authentication process in centralized WLAN deployment architecture. This authentication scheme requires three major phases during authentication process, which are authentication and association phase, 802.1x authentication phase and key management phase. A client can only connect to the AP after completing all the three phases. During roaming, mobile clients need to repeat the three phases each time they connect to a new AP.

## Proposed Solution

From previous work in the area of roaming, and our experimental results, it was determined that there are four major latency-causing phases. These phases are the scanning, authentication and association, 802.1x authentication and key management. Scanning phase is out of scope of this paper because it is a very well researched area. Hence, the concentration of this paper is on the other three phases.

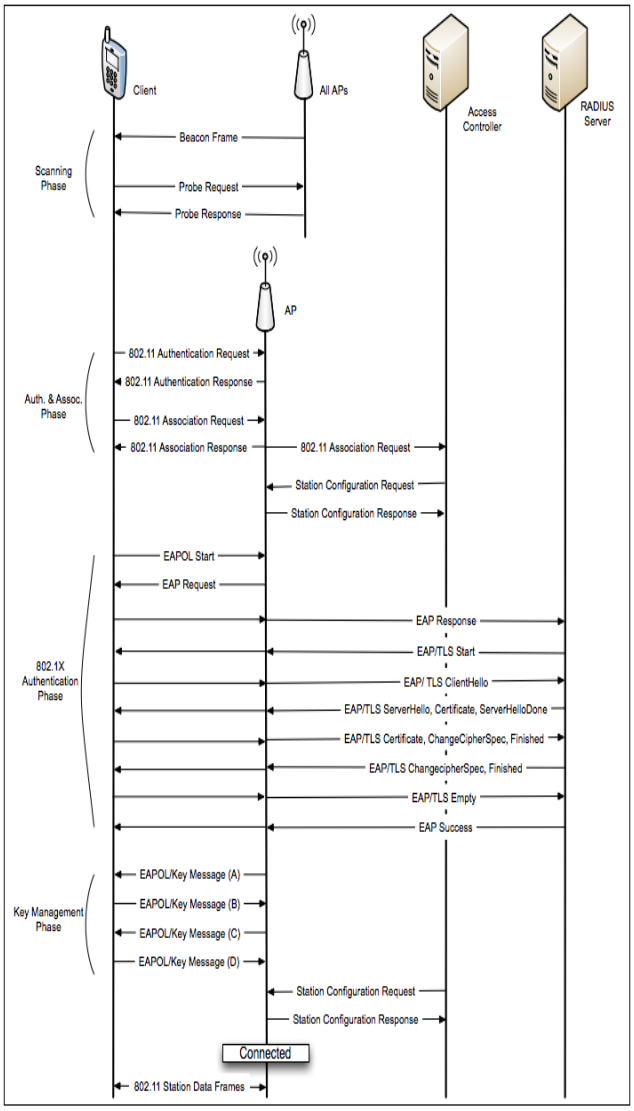
Experiments where then conducted to determine the exact latency values of each phase. The results of these experiments will be further discussed in the results and discussion section of this paper. However, it was determined from the experiments that highest latency component amongst the three phases is the 802.1x authentication phase.

In order to reduce the latency induced by 802.1x phase, a predictive context transfer protocol was proposed, where it is assumed that the AP deployments in the network are usually in 3D. A mobile user moving from one AP to another can only connect to the neighboring APs that are either beside

the current AP that is serving the mobile client or above and below the current AP. In a centralized network, all the APs connect back to the AC and hence AC is able to determine the neighbors of any AP.

When a mobile client's signal starts to drop at its current AP, the AC is triggered of a potential handoff. AC then requests the current AP to provide the 802.1x authentication context information. Once the context information is received, AC determines the neighboring APs of the current AP and forwards the context information to them. Therefore, when the client connects to any of the new neighboring APs, the AP believes that the RADIUS server has already authenticated the client and it does not need to perform the 802.1x phase anymore.

**Figure 2.** *Timing Diagram for handover process for WPA2-Enterprise in Centralized WLAN Architecture*



This process speeds up the authentication phase during roaming. Hence allowing real time applications to thrive in a centralized WLAN deployment environment.

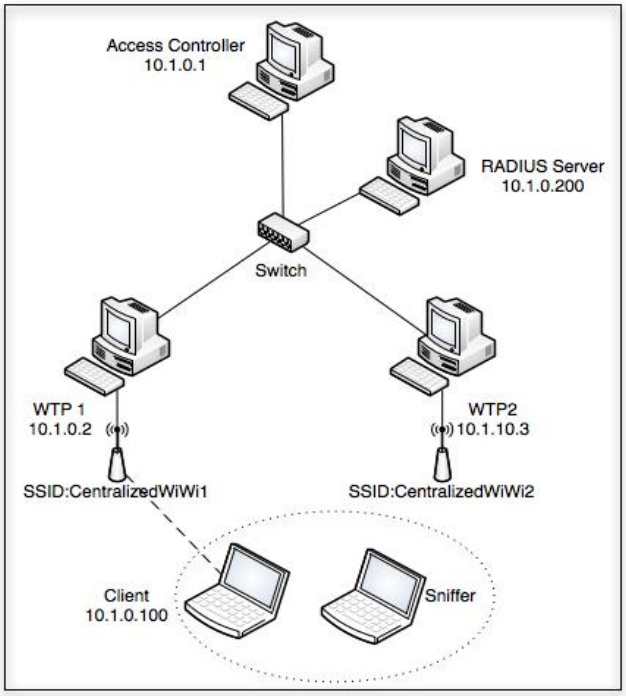
## Test-bed Setup

In order to study the handoff latencies of 802.1x phase, in erroneous and non-erroneous states, a test-bed shown in Fig. 5 was developed. The test-bed consisted of an AC for controlling the APs, RADIUS server for authenticating the clients and 2 APs named at WTP1 and WTP2. A client performed roaming between WTP1 and WTP2. A sniffer was also employed in the test-bed to capture the message exchange between the client and the AP. For without error scenario, experiments were conducted in the close range of 1m between the APs and client. While for the error scenario, experiments were conducted in the range of 10m between the APs and client. This allowed the signal to noise ratio to be at a level where controlled errors could be introduced in the authentication phase.

Proposed context transfer protocol was then enabled on the test-bed in Fig. 5 and experiments were repeated to study the effects of predictive context transfer protocol.

Both the scenarios were repeated several times and the erroneous results were discarded before average was derived. The results are discussed in the next section.

**Figure 3.** *Test-bed setup*



## Results and Analysis

The results of the test-bed experiment are discussed in two parts. First part discusses the authentication phase latency without context transfer and second part discusses the authentication phase latency with predictive context transfer protocol.

## Without Predictive Context Transfer Protocol

Fig. 4(a) shows the authentication, association, 802.1x and key management latencies in an error free scenario. It can be observed that the overall latency can go in excess of 160ms, which is already beyond the VoIP requirements of 150ms. It can also be observed from the figure that the highest latency is observed during the 802.1x phase of the authentication protocol. 802.1x phase contributes to 86% of the overall authentication protocol latency.

Fig. 4(b) shows that during error, authentication protocol latencies can go up to 6 seconds. This is a 39 times increase as compared to error free scenario. It was very obvious from the results that the highest contributing factor behind such high latencies was the 802.1x phase of the authentication protocol. Upon further investigation, it was determined that the main contribution factor behind the dramatic increase in 802.1x latency is the back-off algorithms that require the client and APs to wait for a fixed period of time before retrying during the erroneous scenario.

**Figure 4(a).** *Latency of WPA2-Enterprise Authentication Protocol without Error Scenario and Predictive Context Transfer Protocol*

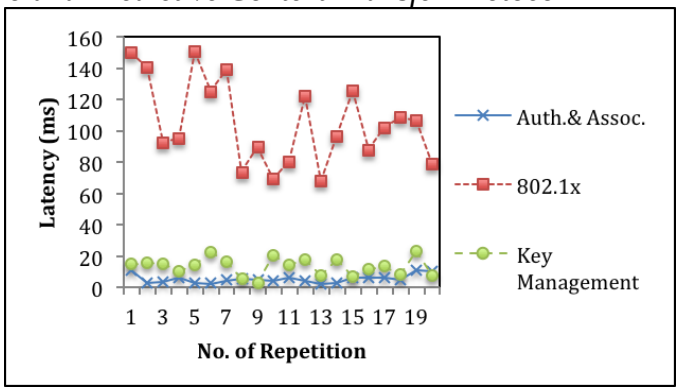
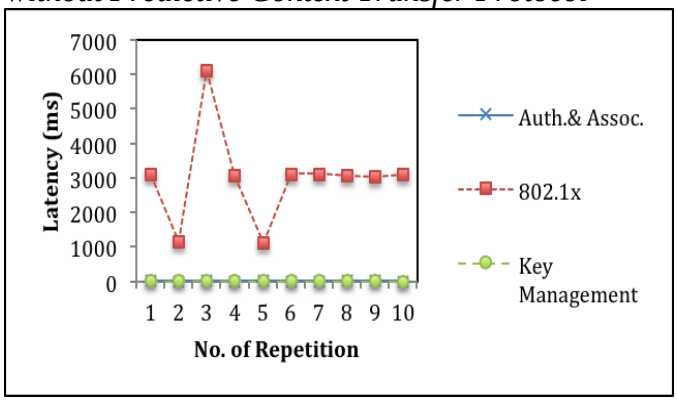


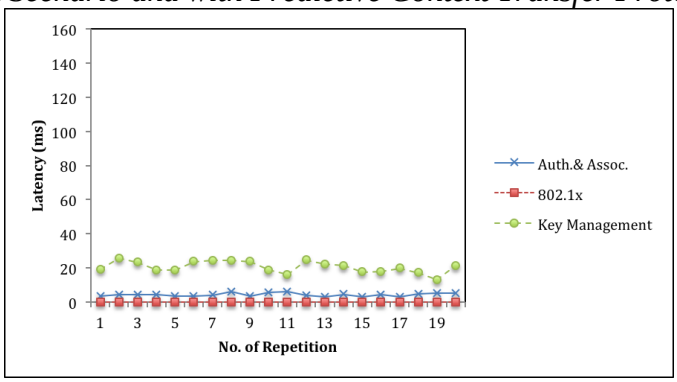
**Figure 4(b).** *Latency of WPA2-Enterprise Authentication Protocol with Error Scenario and without Predictive Context Transfer Protocol*




**With Predictive Context Transfer Protocol**

Fig. 5 shows the authentication, association, 802.1x and key management latencies after implementing context transfer protocol. It can be observed from the results that the 802.1x authentication latency has been totally eliminated because of predictive context transfer since the mobile client does not need to perform the 802.1x phase anymore. This reduces the overall authentication protocol latency to around 30ms. Additionally, this is also an 81.25% improvement compared to the error free scenario and 99.5% improvement compared to the erroneous scenario.

**Figure 5.** *Latency of WPA2-Enterprise Authentication Protocol with error/without Scenario and with Predictive Context Transfer Protocol*




**Conclusion and Future Work**

Authentication protocol latencies play an important role in the overall mobile user handoff experience. During the authentication protocol phases, clients are unable to connect to the AP for communication. The longer the

latency observed during authentication, the poorer is the Quality of Experience (QoE) of the network.

In this paper we studied the latency of the authentication protocol phases in erroneous and error free scenario with and without predictive context transfer protocol. Important conclusion from the experiment was that authentication latency is already above the real time application requirements and with the introduction of errors, authentication latencies can increase by 39 times. It was also conclusive that the biggest contributor to the authentication protocol latency is 802.1x phase. It can also be concluded from the experiments that, by introducing the predictive context transfer protocol, overall authentication protocol latency can be reduced by 81.25% in error free scenario and 99.5% in erroneous scenario.

In the next part of this project, we plan introduce more intelligence into the predictive protocol by implementing location based prediction in the predictive context transfer protocol.

## References

[1] N. Seitz. "ITU-T QoS Standards for IP-Based Networks", IEEE Communication Magazines, pp 82-89, 2003.

[2] J. Wang, L. Bao. "Mobile Context Handoff in Distributed IEEE 802.11 Systems", in Proceeding of International Conference on Wireless Networks, Communications and Mobile Computing (WIRELESSCOM), pp. 1-6, 2005.

[3] L. Chai, S. Machiraju, H. Chen. "CapAuth: A Capability Based Handover Scheme", in Proceeding of 29th Conference on Information Communications (INFOCOM'10), pp. 1-5, 2010.

[4] C. M. Huang, J. W. Li. "A Context Transfer Mechanism for IEEE 802.11r in the Centralized Wireless LAN Architecture", in Proceeding of 22nd International Conference on Advanced Information Networking and Applications (AINA'08), pp. 1-7, 2008.

[5] G. Conradi. "Current Status and Overview of the CAPWAP Protocol", Available on http://www1.cse.wustl.edu/~jain/cse574-10/ftp/capwap/index.html, pp. 1-20, 2010.

[6] A. H. Mir, G. R. Beigh, S. Ahmad. "Latency Evaluation of Extensible Authentication Protocols in WLANs", IEEE 5th International Conference on ANTS, 2011.

[7] B. Singh, P. Bachan. "Performance Evaluation of Authentication Protocols for IEEE 802.11 Standard", 2010 International Conference on ICCCT, 2010.

[8] H. Fathi, H. Imai, K. Kobara, R. Prasad, S. S. Chakraborty. "On the Impact of Security on Latency in WLAN 802.11b", IEEE GLOBECOM '05, 2005.

[9] A. Mishra, D. Agrawal, S. Banerjee, S. Rayanchu, S. Saha."Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal", IEEE The 27th Conference on INFOCOM 2008, 2008.

[10] L. Yang, P. Zerfos, E. Sadot. "Architecture Taxonomy for Control And Provisioning of Wireless Access Points (CAPWAP)", IETF, RFC4118 (Informational), Available on http://tools.ietf.org/rfc/rfc4118.txt, pp. 1-41, 2005.

[11] D. Stanely, M. Montemurro, P. Calhoun. “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification” RFC 3990, 2005.
[12] D. Stanely, M. Montemurro, P. Calhoun. “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11” RFC 4118, 2005.
[13] E. Sadot, L. Yang, P.Zerfos. “Architecture Taxonomy for Control and Provisioning of Wireless Access Points” RFC 4564, 2005.
[14] Ed, L. Yang, S. Govindan, WH. Zhou, ZH. Zhou. “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification” RFC 3990, 2006.
[15] F. C. Kuo, F. Meyer, H. Tschofenig, X. Fu. “Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security”, 25th IEEE International Conference on INFOCOM 2006, 2006.
[16] A. Chiornita, D. Rosner, L. Gheorghe. “A Practical Analysis of EAP Authentication Methods”, 2010 9th Roedunet International Conference (RoEduNet), 2010.