Journal of Computer and Communications, 2014, 2, 64-75
Published Online June 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.28007

Multilayer Authentication for Communication Systems Based on Physical-Layer Attributes

Ahmed Refaey[1], Weikun Hou[1], Khaled Loukhaoukha[2]

[1]Department of Electrical and Computer Engineering, University of Western Ontario, London, Canada
[2]Department of Electrical and Computer Engineering, Université Laval, Québec, Canada
Email: ahusse7@uwo.ca, whou5@uwo.ca, khaled.loukhaoukha.1@ulaval.ca

Received 10 March 2014; revised 10 April 2014; accepted 7 May 2014

Abstract

In this paper, a multilayer security solution is introduced, in order to accord the required end-to-end security blanket to the heterogeneous networks by considering the properties used by authentication at the physical-layer in transport-layer authentication. In particular, after achieving an authentication level based on the estimated channel impulse response (CIR) at the physical-layer, these CIRs are exploited at the transport layer, adding more randomness to the generated sequence numbers used in the 3-Way TCP/IP handshake authentication. Furthermore, in order to enhance the authentication at the physical layer, the estimated CIR is quantized into two domains: amplitude and phase. The quantizer's output is used to differentiate between the legitimate transmitters and intruders using binary hypothesis testing. Eventually, generating a unique sequence numbers is granted due to the increased randomness offered by the quantizer outputs. In order to verify the effectiveness of the proposed scheme, simulation results are shown based on an orthogonal frequency division multiplexing (OFDM) system. Additionally, a logarithmic likelihood ratio test is used to evaluate the authentication performance.

Keywords

Physical Layer Authentication, Channel Impulse Response, TCP, Hypothesis Testing

1. Introduction

In recent years, the secure transmission in the Internet protocol (IP) wireless networks has received a significant amount of research attentions by addressing the security weaknesses of these networks. The topologies of such

How to cite this paper: Refaey, A., Hou, W.K. and Loukhaoukha, K. (2014) Multilayer Authentication for Communication Systems Based on Physical-Layer Attributes. *Journal of Computer and Communications*, **2**, 64-75.
http://dx.doi.org/10.4236/jcc.2014.28007

networks are composed of a wired, packet-switched, backbone network, and a wireless network. The wireless network is organized into geographically defined cells, with a control point called a base-station (BS) in each of these cells. The base-stations are also directly connected to the wired network, routing packets between the wireless and the backbone network. In these networks, a mobile host (MH) receives data from a fixed host (FH) via internet routed through the BS of the cell that it is stationed in and vice-versa. Due to the movement of the MH between wireless cells, the task of securing the data transmission between the wired network and the mobile host has received a significant amount of research attention by addressing the security weaknesses of wireless systems and networks. In fact, the security in these particular networks is traditionally addressed on the upper layers of protocol stack through cryptography and IPSec which bring on an unprotected communications environment at the physical-layer. In addition, these upper layer security protocols run into an isolated environment from the physical-layer, while in the upper layer security there are many unique attributes that can be exploited, which lead to wireless networks with strong end-to-end security properties. The physical layer authentication has been formulated as binary hypothesis testing by exploiting the unique attributes related to the signal propagation environment such as, received signal strength (RSS) [1] and the channel state information (CSI) [2]. Indeed, the performance of these attributes is limited by the communication's noise as well as the channel stability, therefore, investigation on channel characteristics such as, the channel frequency response (CFR) has been conducted in [3], while considering the mobility of wireless terminals and/or the multiple antennas. It is noteworthy that, the physical layer authentication based on the CFR is suffering from the high complexity in broadband systems, as well as, the omission of spatial information related to the signal propagation environment. Eventually, the channel impulse response (CIR) has been investigated in [4] and [5] to be used in the physical-layer authentication, in order to overcome the drawbacks of the CFR. Herein, considering the wireless part of the IP wireless network, the quantization of the CIRs is employed as a pre-processing procedure for physical-layer authentication. In particular, a quantization algorithm for the amplitude as well as the channel path delay is applied to the estimated CIRs to mitigate negative impact of the channel noise and estimation error, as well as, the mobility induced channel variation and path arrival time [6] [7]. In addition to the physical-layer authentication, recently there is an undeniable temptation to use the Internet Protocol (IP) address in a transmission control protocol (TCP) connection for authentication [8]. Unfortunately, TCP was not designed to be used in this manner, consequentially, this authentication method is not secure enough. However, it still provides an interesting network security issue [9] [10]. As a matter of fact, this authentication method is based on the initial SEQ numbers which are supposed to be generated in a random manner. Therefore, the randomness of the initial SEQ numbers is considered as a keyword for this method of authentication. Unfortunately, in the current networks they are often not very random at all [11]. In this paper, in addition to the authentication method that we offer to the wireless part of the network based on the quantization of the channel impulse response (CIR), we propose generating the initial SEQ numbers from the quantization of the CIRs. As a result, we then do not need any of the authentication protocols such as, pesky or troublesome keys, as well we will offer an end-to-end authentication technique to the IP wireless networks.

2. Proposed System Model

To visualize the proposed communication scenario we demonstrate an IP wireless network as shown in **Figure 1**. In the wireless connection side, to address the physical-layer authentication, a channel impulse response (CIR)-based authentication scenario for a simple time-invariant wireless environment is considered. This authentication scheme is based on quantization algorithm as it will be shown in the next section. Furthermore, in the wired connection, we use the TCP/IP protocol architecture as the starting point for our solutions to security problem in

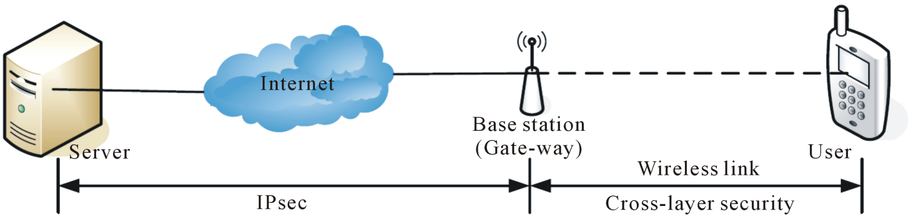


Figure 1. Overview for the network topology.

IP wireless networks rather than designing new protocol architecture completely from scratch.

2.1. Wireless Connection

In fact, the channel impulse responses needed for the authentication process are estimated from the received signal based on a noise-eliminated channel estimation method. A quantization scheme is applied to estimated CIRs as shown in the next section in details, and the outputs are used for decision-making based on likelihood test ratio under a binary hypothesis testing. An OFDM system is employed here for theoretical analysis and numerical simulation. Additionally, we consider "Mobile-1, Base Station-A, Mobile-2" scenario is used to explain the concept of authentication, where Mobile-1 and Mobile-2 are at different locations in space as shown in **Figure 2**. Mobile-1 as the legitimate user, require secure communications, while Mobile-2 represents an eavesdropper to intend spoofing the Base Station-A. The objective of the proposed authentication is to determine if a spoofing attack is occurred in the wireless part of the network.

2.2. Wired Connection

Although TCP was not designed as a security protocol, it is tempting to use the IP address in a TCP connection for authentication. In this section we will demonstrate how TCP is used for authentication through an assumed scenario as follows:

First we need to quickly review the TCP three-way handshake, which is illustrated in **Figure 2** (blue messages). The first message is a synchronization request (SYN), whereas the second message, which acknowledges the synchronization request (SYN-ACK), and the third message which can also contain data acknowledges the previous message, and is simply known as an (ACK).

Now, suppose that the Server relies on the completed three-way handshake to verify that it is connected to a specific IP address, which is it knows that it belongs to Base Station-A. In effect, the server is using the TCP connection to authenticate Base Station-A. Since the Server sends the SYN-ACK to Base Station-As IP address, it is tempting to assume that the corresponding ACK must have come from the Base Station-A. In particular, if the Server verifies that ACK b + 1 appears in message three, it has some reason to believe that the Base Station-A, at its known IP address, has received and responded to message two, since message two contains SEQ b. An underlying assumption here is that Base Station-F cannot see the SYN-ACK packet otherwise the Base Station-F would know b and it could easily forge the ACK. Clearly, this is not a strong form of authentication, but it is often used in practice [11].

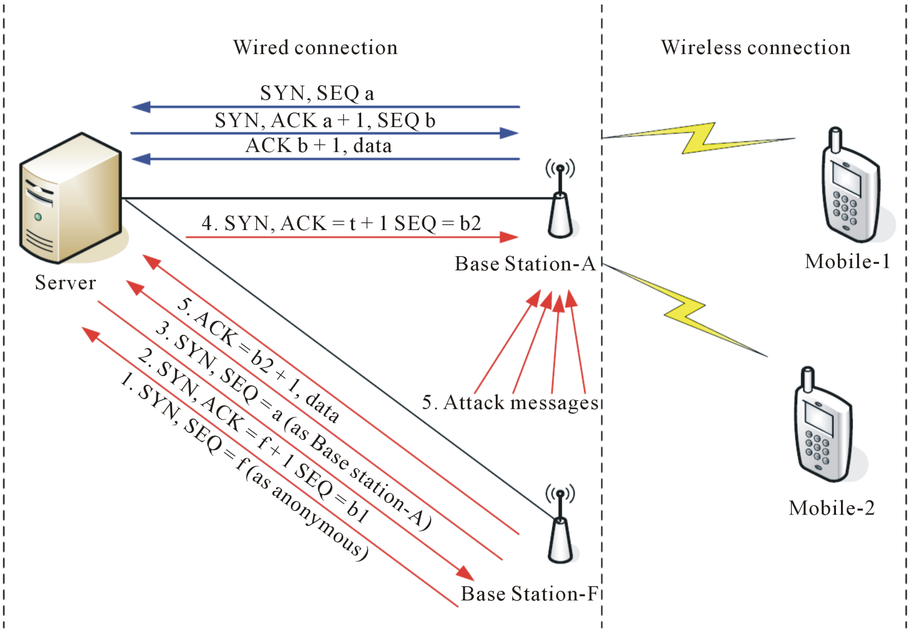


Figure 2. Proposed communication scenario.

Possible Attacks

Unfortunately, one serious flaw with this TCP authentication scheme occurs if Base Station-F can predict the initial SEQ number sent by the Server. Herein, we provide two possible attacks to the TCP authentication. The first attack in the Berkeley systems, the initial sequence number is incremented by a constant amount once per second and by half that amount each time a connection is initiated. Thus, what a hacker needs to do is just initiate a normal connection and keep the ISN received from destination host, then calculate the ISN for the next connection attempt, based on the round-time delay, number of connections after the first connection. Usually, it has high possibility to succeed.

The second possible attack scenario is illustrated in **Figure 2** (red messages). In this attack, Trudy first sends an ordinary SYN packet to Bob, who responds with a SYN-ACK. Trudy examines the SEQ value b1 in this SYN-ACK packet. Suppose now that Base Station-F can use b1 to predict Servers next initial SEQ value b2. Then Base Station-F can send a packet to the Server with the source IP address forged to be for example, Base Station-As IP address. Then the Server will send the SYN-ACK to Base Station-As IP address which, by assumption, Base Station-F cannot see. But since the Base Station-F can guess b2, it can complete the three-way handshake by sending ACK b2 + 1 to the Server. As a result, the Server will believe that data from Base Station-F on this particular TCP connection actually came from the Base Station-A.

Note that the Server always responds to Base Station-As IP address and, by assumption, Base Station-F cannot see his responses. But the Server will accept data from Base Station-F, thinking it came from Base Station-A, as long as the connection remains active. However, when the data sent by the Server to Base Station-As IP address reaches Base Station-A, Base Station-A will terminate the connection since it has not completed the three-way handshake. In order to prevent this from happening, Base Station-F could mount a denial of service attack on Base Station-A by sending enough messages so that

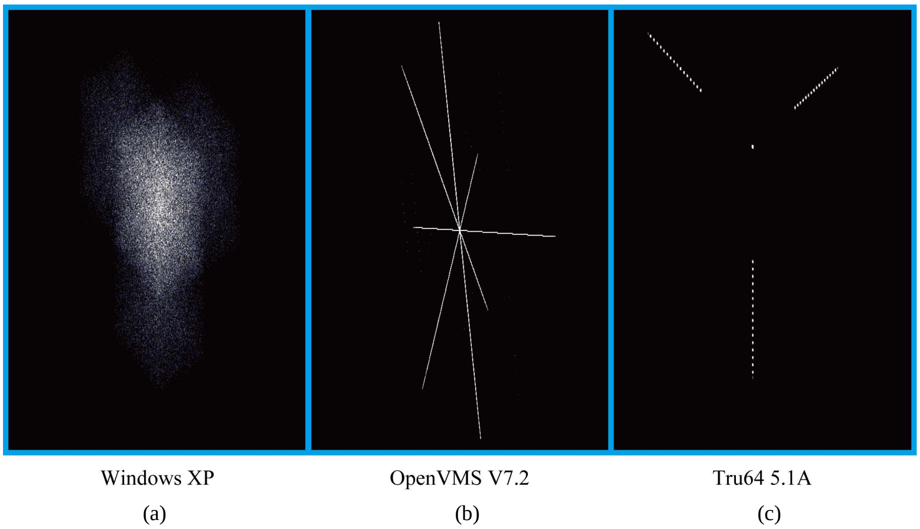
The Server s messages cannot get through or, even if they do get through, Base Station-A cannot respond. This denial of service is illustrated by the messages labeled with 5s from Base Station-F to Base Station-A. If Base Station-A happens to be offline, Base Station-F could conduct the attack without this denial of service phase.

This attack is well known, and as a result it is known that initial SEQ numbers must be random [12].

As a matter of fact, the initial sequence numbers are often not very random at all which increase the possibility to such the above attack to success.

For example, **Figure 3** provides a visual comparison of random initial SEQ numbers in three different operating systems, Windows XP, OpenVMS V7.2, and Tru64 5.1A. This figure shows how the initial sequence numbers' generated in these operating systems are highly biased. Notwithstanding, the TCP authentication method is often used in practice for security purposes due to it is convenient.

As a consequence, in order to employ a secure authentication using the TCP, it is highly recommended to



Windows XP (a)

OpenVMS V7.2 (b)

Tru64 5.1A (c)

Figure 3. The randomness of initial sequence number for different operating systems.

introduce an better approach would be to employ a secure authentication.

3. Proposed Authentication Scheme

The flowchart of the proposed authentication scheme is illustrated in **Figure 4**. First of all, CIRs needed for the proposed authentication process are estimated from the received signal based on a noise-eliminated channel estimation method. A quantization scheme is applied to estimated CIRs, and the outputs are used for decision-making based on likelihood test ratio under a binary hypothesis testing. Furthermore, the output of the quantization operation is stored in a database to be used in the decision-making. An OFDM system is employed here for theoretical analysis and numerical simulation. Consequently, the output of the quantization step each time is 64-bit (64 tabs). Therefore, in order to use the quantized CIRs as a initial sequence number we need a puncturing step. This puncture step not only assist to adjust the required number of bits for the initial sequence number (32-bits) but also it increase the randomness of these numbers and consequently add to the security operation. The objective of the proposed authentication is to determine if a spoofing attack is occurred in either the wireless part or the wired part. In the following subsections, the operation steps in shown in details.

3.1. Quantization

The physical-layer authentication based on the channel impulse response (CIR) has been proposed in [13], where the unique characteristics of CIR are exploited and the difference between two adjacent CIR estimates is used to develop test statistics for evaluating the authentication performance. Unfortunately, the proposed CIR-based authentication scheme in [13] cannot guarantee a robust performance at low SNR due to large overlapped portion under a binary hypothesis testing (H_0 and H_1). Since the overlapping parts are caused by the presence of noise, channel estimation error and terminal movement, the quantization scheme to be applied to CIR estimates will tolerate these negative impacts on CIRs. The quantized CIR estimates are represented in two dimensions, *i.e.*, amplitude $\hat{a}_q^t$ and channel path delay $\hat{\tau}_q^t$,

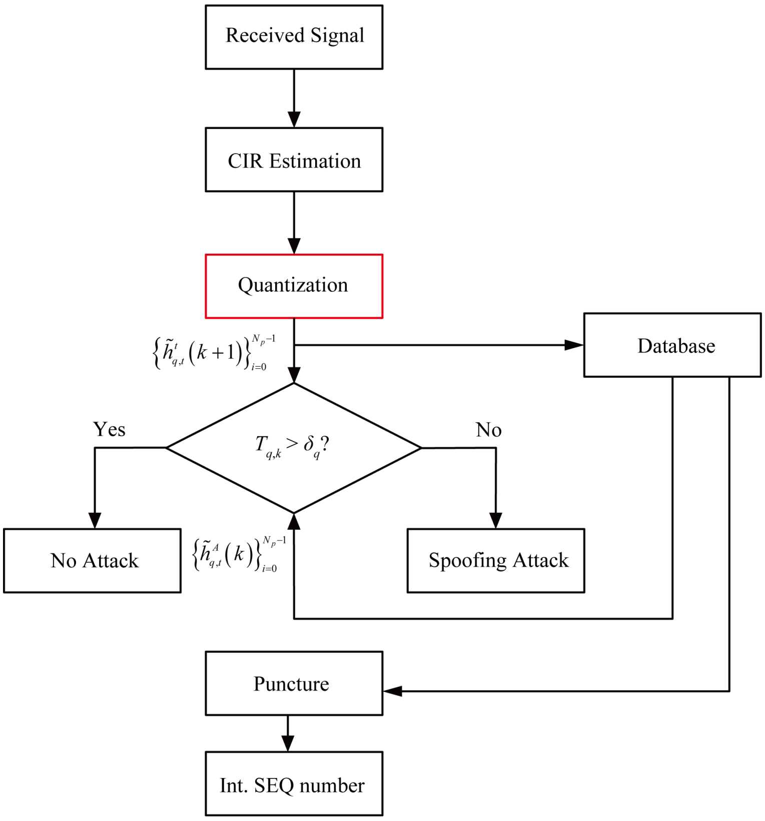


Figure 4. The flowchart of the proposed authentication scheme.

$$\hat{a}_{q,i}^{t}(k)=\begin{cases}\left\lfloor \dfrac{\hat{a}_i^t(k)}{\Delta x_i}\right\rfloor\cdot\Delta x_i+\dfrac{\Delta x_i}{2}, & \text{if } \hat{a}_i^t(k)\neq 0\\ 0, & \text{if } \hat{a}_i^t(k)=0,\end{cases}\tag{1}$$

$$\hat{\tau}_{q,i}^{t}(k)=\begin{cases}\left\lfloor \dfrac{\hat{\tau}_i^t(k)}{\Delta y_i}\right\rfloor\cdot\Delta y_i+\dfrac{\Delta y_i}{2}, & \text{if } \hat{\tau}_i^t(k)\neq 0\\ 0, & \text{if } \hat{\tau}_i^t(k)=0,\end{cases}\tag{2}$$

where $\hat{a}_i^t$ is the estimated amplitude on the i^{th} path, and $\hat{\tau}_i^t$ is the i^{th} estimated path delay. Δx_i and Δy_i are step sizes of quantization in the dimensions of amplitude and path delay respectively. The superscript "*t*" indicates the identity of the transmitter is uncertain.

Due to the existence of quantization noise, an additive noise model is used to represent the output of the quantization. Thus, the quantizer output can be represented as

$$\hat{a}_{q,i}^{t}=\hat{a}_i^t+e_{x,i},\tag{3}$$

$$\hat{\tau}_{q,i}^{t}=\hat{\tau}_i^t+e_{y,i},\tag{4}$$

where $e_i=e_{x,i}+je_{y,i}$ is the quantization noise and assumed as additive Gaussian noise with variance of $\sigma_{e,i}^2$. Herein $e_{x,i}$ and $e_{y,i}$ are real and independent random variables, uniformly distributed between $\pm\dfrac{\Delta x_i}{2}$ and $\pm\dfrac{\Delta y_i}{2}$ respectively. Thus, the variance of the quantization noise, $\sigma_{e,i}^2$, can be derived as

$$\sigma_{e,i}^2=\frac{(\Delta x_i)^2}{12}+\frac{(\Delta y_i)^2}{12}.\tag{5}$$

Considering those difficulties on CIR-based authentication, the objective of the proposed quantization scheme is to minimize the variation between two adjacently quantized CIR estimates from the same transmitter, but still maintain the difference between them from disparate transmitters. In particular, training symbols from the authenticated terminal (Mobile-1) are initially observed at receiver. Then, after channel estimation, CIR estimates in the dimensions of amplitude $\left\{\hat{a}_i^m 1\right\}_{i=0}^{N_p-1}$ and path delay $\left\{\hat{\tau}_i^M 1\right\}_{i=0}^{N_p-1}$ are correspondingly achieved, where the superscript "*m*1" stands for the legitimate transmitter Mobile-1.

Therefore, the proposed quantization algorithm can be formulated in two aspects applying to the CIR estimates. First of all, on the i^{th} path, two mean square errors (MSEs) are denoted as $MSE_x^{m1}(i)$ and $MSE_y^{m1}(i)$ in the two dimensions respectively, which describe the difference of two consecutively quantized CIR estimates. For authentication enhancement, these two MSEs are minimized, *i.e.*,

$$MSE_x^{m1}(i)=\min_{\Delta e_{x,i}}\frac{1}{M}\sum_{k=0}^{M-1}\left[\hat{a}_i^{m1}(k+1)-\hat{a}_i^{m1}(k)-\Delta e_{x,i}\right]^2 p_{x,i}^{m1}(k),\tag{6}$$

$$MSE_y^{m1}(i)=\min_{\Delta e_{y,i}}\frac{1}{M}\sum_{k=0}^{M-1}\left[\hat{\tau}_i^{m1}(k+1)-\hat{\tau}_i^{m1}(k)-\Delta e_{y,i}\right]^2 p_{y,i}^{m1}(k),\tag{7}$$

where $\Delta e_{x,i}$ and $\Delta e_{y,i}$ are the differences of two successive quantization noises in the corresponding dimensions, and expressed as $\Delta e_{x,i}=e_{x,i}(k)-e_{x,i}(k+1)$ and $\Delta e_{y,i}=e_{y,i}(k)-e_{y,i}(k+1)$. $p_{x,i}^{m1}(k)$ and $p_{y,i}^{m1}(k)$ are the probabilities of $\hat{a}_i^{m1}(k+1)-\hat{a}_i^{m1}(k)$ and $\hat{\tau}_i^{m1}(k+1)-\hat{\tau}_i^{A}(k)$ respectively. Since Rayleigh fading channel is employed, these two probabilities follow complex Gaussian distributions with mean zero and different variances. Based on Equation (6), $\Delta e_{x,i}$ and $\Delta e_{y,i}$ are derived as

$$\Delta e_{x,i}=\frac{\sum_{k=0}^{M-1}\left(\hat{a}_i^{m1}(k+1)-\hat{a}_i^{m1}(k)\right)p_{x,i}^{m1}(k)}{\sum_{k=0}^{M-1}p_{x,i}^{M1}(k)},\tag{8}$$

$$\Delta e_{y,i} = \frac{\sum_{k=0}^{M-1}\left(\hat{\tau}_i^{m1}(k+1) - \hat{\tau}_i^{M1}(k)\right) p_{y,i}^{m1}(k)}{\sum_{k=0}^{M-1} p_{y,i}^{m1}(k)}. \tag{9}$$

Consequently, the step sizes of quantization for all paths can be represented by $\Delta e_{x,i}$ and $\Delta e_{y,i}$, which are written by

$$\Delta x_i = \lambda \Delta e_{x,i}, \tag{10}$$

$$\Delta y_i = \mu \Delta e_{y,i}, \tag{11}$$

where coefficients λ and μ have constant values. Since the difference between two quantized CIR estimates from the legal terminal are expected to be minimized for authentication purpose, larger step sizes of quantization lead to a smaller variation. However, overly large step sizes decrease the performance of detecting spoofing attacks. Hence, the values of λ and μ should be constrained and can be determined experimentally when an eavesdropper is involved in the communication.

In the presence of Mobile-2, in order to achieve a robust performance of spoofing detection, a sum of differences between two quantized CIR estimates from unauthenticated transmitters should be at least equal to that from the legitimate transmitter, *i.e.*,

$$\begin{gathered} \sum_{k=0}^{M-1}\sum_{i=0}^{N_p-1}\left\{\left[\hat{a}_{q,i}^{t}(k+1) - \hat{a}_{q,i}^{m1}(k)\right]^2 - \left[\hat{a}_{q,i}^{m1}(k+1) - \hat{a}_{q,i}^{m1}(k)\right]^2\right\} \geq 0, \\ \sum_{k=0}^{M-1}\sum_{i=0}^{N_p-1}\left\{\left[\hat{\tau}_{q,i}^{t}(k+1) - \hat{\tau}_{q,i}^{m1}(k)\right]^2 - \left[\hat{\tau}_{q,i}^{m1}(k+1) - \hat{\tau}_{q,i}^{m1}(k)\right]^2\right\} \geq 0. \end{gathered} \tag{12}$$

Based on the proposed quantization scheme, the quantization step sizes are constrained by these two aspects given in (6) and (12).

3.2. Authentication Decision

The physical-layer authentication is generally considered as a hypothesis testing problem, therefore, in order to verify the performance of proposed authentication scheme, a binary hypothesis testing is formulated here. In particular, based on the proposed quantization scheme, the test statistic $T_{q,k}$ is compared with some threshold δ_q to determine if a spoofing attack occurs. The binary hypothesis testing problem is expressed as

$$\begin{gathered} H_0 : T_{q,k} > \delta_q \\ H_1 : T_{q,k} < \delta_q, \end{gathered} \tag{13}$$

where H_0, the null hypothesis, denotes Mobile-1 as the legitimate transmitter, while the alternative hypothesis, H_1, represents Mobile-2, the spoofing transmitter. δ_q is the threshold for decision making, and $T_{q,k}$ is given by,

$$T_{q,k} = \ln\left\{\frac{1}{2\pi N_p}\sum_{i=0}^{N_p-1}\frac{1}{\sigma_{q,i}^2}\exp\left[\frac{-1}{2\sigma_{q,i}^2}\left(\left|\hat{a}_{q,i}^{t}(k+1) - \hat{a}_{q,i}^{A}(k)\right|^2 + \left|\hat{\tau}_{q,i}^{t}(k+1) - \hat{\tau}_{q,i}^{A}(k)\right|^2\right)\right]\right\}. \tag{14}$$

Referring to the theoretical analysis in [13], the variance σ_i^2 under the two hypotheses can be expressed as

$$\begin{gathered} \sigma_{H_0,i}^2 = 2(1-\zeta)\sigma_{m1,i}^2 + 2\sigma_s^2, \\ \sigma_{H_1,i}^2 = \sigma_{m2,i}^2 + \sigma_{m1,i}^2 + 2\sigma_s^2, \end{gathered} \tag{15}$$

where the subscripts "*m*1" and "*m*2" represent the transmitters Mobile-1 and Mobile-2 respectively. Based on the expressions of variance σ_i^2 under two hypotheses, the variance $\sigma_{q,i}^2$ in (3.2) can be derived as

$$\begin{gathered} \sigma_{q,H_0,i}^2 = \sigma_{H_0,i}^2 + 2\sigma_{e,i}^2, \\ \sigma_{q,H_1,i}^2 = \sigma_{H_1,i}^2 + 2\sigma_{e,i}^2. \end{gathered} \tag{16}$$

Additionally, the false alarm rate (FAR) P_{fa} (*i.e.*, the probability of declaring Mobile-1 as intruder by mistake), and the probability of detection (PD) P_d (*i.e.*, the probability of detecting spoofing attacks) are utilized to analyze the authentication performance of our proposed scheme. These two metrics are denoted as

$$P_{fa} = P_r\left\{T_{q,k} < \delta_q \middle| H_0\right\}, \tag{17}$$

$$P_d = P_r\left\{T_{q,k} < \delta_q \middle| H_1\right\}. \tag{18}$$

Neyman-Pearson test is considered here, where the PD is maximized according to a minimum tolerable constraint on FAR. Before establishing communication links, training symbols are sent from Mobile-1 to Base Station-A, and Bob can calculate FAR for several PDs in (17). Due to the gradually increase between FAR and PD, Base Station-A can find the threshold δ_q when the FAR satisfies the requirement.

3.3. Puncturing

In fact, puncturing technique is usually used in channel coding to achieve different code rates by puncturing the parity bit sequences. This has the same effect as encoding with an error-correction code with less parity bit sequences (high rates). Generally, a pre-defined puncturing array is used in the transmitter part (encoder), and the inverse operation (depuncturing) is done by the receiver (decoder). Indeed, with puncturing the same decoder can be used regardless of how many bits have been punctured, thus puncturing considerably increases the flexibility of the system without significantly increasing its complexity. Herein, we utilize the same concept to achieve the exact required number of bits for the initial sequence number (32-bits). In addition, puncturing bits from the quantized CIRs using a pre-defined puncturing array makes the authentication operation more secured anti-attackers. In this case, the attackers not only need to predict the unique initial sequence number based on the CIRs but also they need to predict which bits has been punctured which make the operation almost impossible.

The elements of the puncturing array are zeros and ones, corresponding to keeping or deleting bits respectively. The puncturing block here periodically deletes bits via a puncturing matrix from the CIRs sequences. The punctured approach can be best understood by illustration, for a detailed example see [14].

3.4. TCP Authentication

TCP/IP is the most widely used protocol suite in the IP wireless networks. In fact, this protocol is designed through a highly structured and layered approach, with each layer responsible for a different facet of communications. Unfortunately, standard TCP/IP protocol is not perfect as it does not achieve optimal performance when operated over these modern IP wireless networks. Therefore, transport-aware link layer mechanisms are often necessary to correct some problems such as non-congestion losses, latency, variable bandwidth, and dynamic changing topology which are caused because such these networks possess certain characteristics that are unfriendly to TCP. However, these performance enhancement mechanisms are conflicted with other security protocols such as Internet Protocol (IP) Sec which is almost used in all-IP wireless networks. Consequently, the modification to the TCP protocol to be used for the authentication purpose and release the conflict with other security protocols is a must. Currently, there exist a number of serious security flaws inherent in the protocol design or most of TCP/IP implementation whereas the network hackers can utilize these security holes to perform various network attacks such this Base Station-F in **Figure 2**. In **Figure 2**, a fake base station is trying to impersonate the legitimate one to establish a connection with the Server. Among the hacking techniques, two of them are commonly used and reflect some typical problems in TCP/IP protocol as shown in Section 2.

Herein, we propose an enhanced approach of the TCP/IP 3-way handshake to replace the IPsec, consequentially, offering the required security blanket and work in a friendly environment with the transport-aware link layer mechanisms. In addition, the proposed approach is generating the initial sequence number which is the core of this security mechanism based on the unique quantized CIRs which are described in the previous subsection.

Considering that the base station can inspect every TCP packets, **Figure 5** shows the proposed protection model for the TCP. The sender (Mobile-1) encrypts the TCP data while leaving the TCP header in unencrypted and unauthenticated form. As a consequence, that intermediate node (Base Station-A) can make use of the TCP state information encoded in the TCP header.

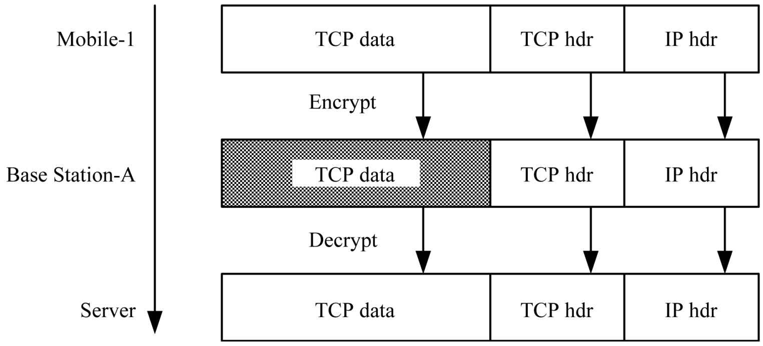


Figure 5. The protocols formats.

In fact, letting the entire TCP header appear in clear text exposes several vulnerabilities of the TCP session to a variety of TCP protocol attacks (in particular traffic analysis), because the identity of sender and receiver are now visible without confidentiality protection. However, only the legitimate base station can generate the sequence number based on the quantized CIRs. Furthermore, the connection between the base station and the server will start after the base station authenticate the sender identity

4. Discussion and Simulation Results

In this section, the effectiveness of the proposed authentication scheme is verified by numerical simulations. An OFDM system with total sub-carrier number of 1024 is employed and modulated by the QPSK technique on each sub-carrier, and the length of CP is set to be 256. Comb-type pilots with number of 64 are inserted into each OFDM symbol for channel estimation. As for the channel model, a random Rayleigh fading channel is developed with six sparse sample-spaced significant paths and uniform power delay profile. In contrast, the number of significant paths communicating between Mobile-2 and the Base Station-A is randomly chosen from 1 to 10. Additionally, different delayed paths are statistically independent of each other.

In **Figure 6**, it is shown the two averaged logarithmic likelihood ratios (L) and (L_q) versus different SNRs under two different values of quantization step size, where the intruder Mobile-2 is involved.

As in [13], the averaged logarithmic likelihood test function of the variation between estimated CIRs (L) can be formulated as

$$L = \frac{1}{M}\sum_{k=0}^{M-1} T_k, \tag{19}$$

where T_k is given by:

$$T_k = \ln\left\{\frac{1}{2\pi N_p}\sum_{i=0}^{N_p-1}\frac{1}{\sigma_i^2}\exp\left[\frac{-1}{2\sigma_i^2}\left(\left|\hat{a}_i^t(k+1)-\hat{a}_i^A(k)\right|^2+\left|\hat{\tau}_i^t(k+1)-\hat{\tau}_i^A(k)\right|^2\right)\right]\right\}, \tag{20}$$

and σ_i^2 is the variance of the difference of estimated CIRs on the i^{th} path under a certain SNR.

Similarly, a test statistic of the difference between quantized CIR estimates using the averaged logarithmic likelihood ratio (L_q) can be expressed as:

$$L_q = \frac{1}{M}\sum_{k=0}^{M-1} T_{q,k}, \tag{21}$$

where $T_{q,k}$ is given in (3.2) in the previous section and $\sigma_{q,i}^2$ is the variance of the distinction between two quantized CIR estimates on the i^{th} tap based on a given SNR.

Herein AR coefficient (ζ) under H_0 is set to be 0. **Figure 6** illustrates that the presence of the eavesdropper Eve makes the values of L_q s corresponding to Mobile-1 and Mobile-2 dramatically different, and the values of L_q observed from Alice are always larger than that from Eve. Moreover, the values of quantization step size influence less on the values of L_q from Mobile-1 than that on the values of L_q from Mobile-2.

In **Figure 7**, the performance of spoofing detection is sketched versus different SNRs based on two different step sizes of quantization in two cases (*i.e.*, $\zeta = 0$ and $\zeta = 0.4$). When the AR coefficient (ζ) under H_0 is

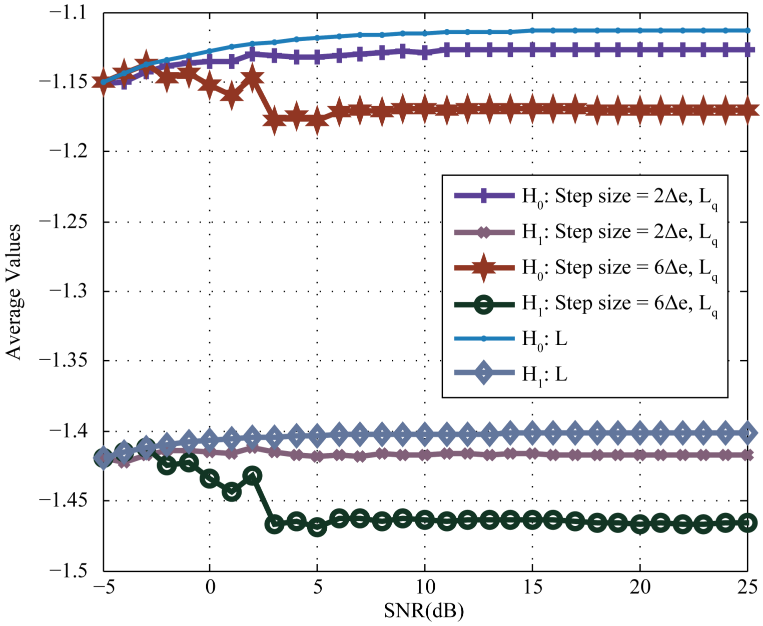


Figure 6. The randomness of estimated CIRs after quantization process.

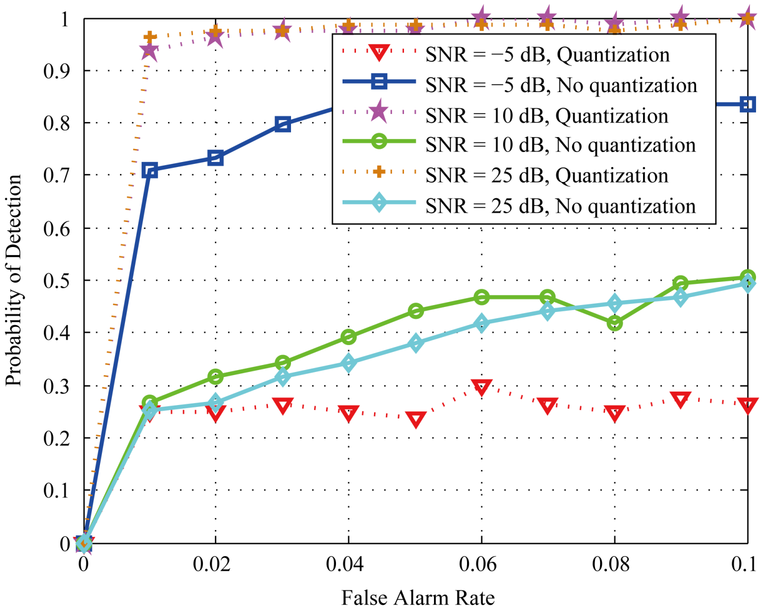


Figure 7. PD versus different SNRs using two different quantization steps sizes.

equal to 0, the probability of detection is approximately 0.5 without quantization process, whereas the probability of detection under the proposed quantization scheme is equal or higher than 0.5 even at SNR = −5 dB. When ζ increases to 0.4, the probability of detection reaches approximately to one in the two cases, where SNR is in the working range of a normal wireless system.

Figure 8 shows the difference of two quantized CIR estimates with the length of 64 bits under two different threshold values respectively. Since sparse channel is employed here and most of inherent differences between two CIR estimates from the legitimate user are removed by the process of quantization, few paths with non-zero values are remained particularly under a larger threshold value.

In **Figure 9** CIR estimates are achieved from a series of OFDM sequences with the number of 1000. Each

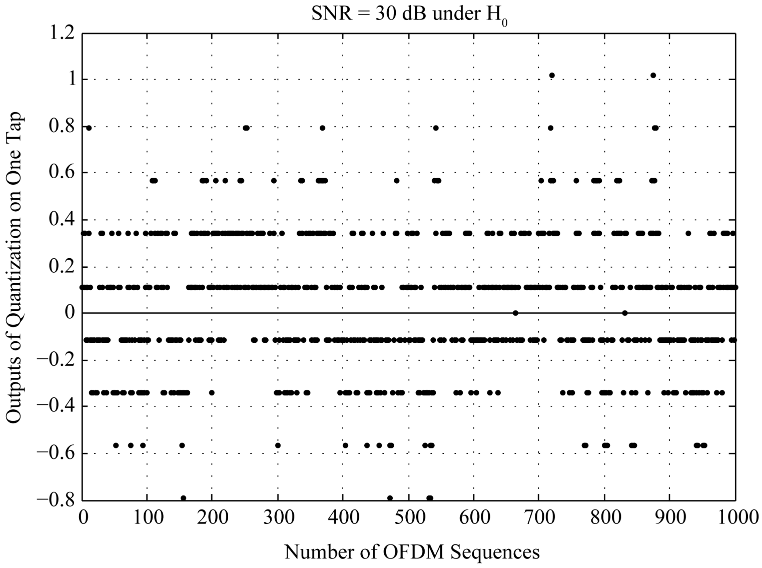


Figure 8. The randomness of estimated CIRs after quantization process.

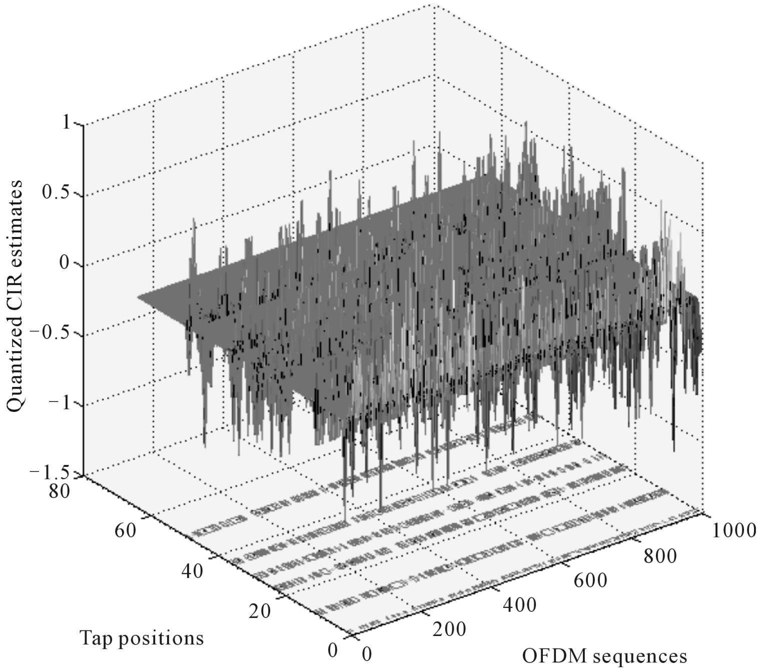


Figure 9. 3-D figure of the estimated CIRs after quantization process to generate the initial SEQ number.

CIR estimate has 64 paths, however, a few paths have non-zero values due to the assumption of sparse channel. Based on proposed quantization scheme, majority of significant variations of CIR from the legitimate transmitter is eliminated.

5. Conclusion

The end-to-end network security mechanisms are based on the layering architecture for network security protocols by considering the joint effects of physical-layer security with transport-layer authentication. In particular, considering IP wireless networks, a physical-layer authentication scheme using quantization algorithm for the amplitude as well as the channel path delay under a binary hypothesis testing has been proposed for the wireless part of the network. Additionally, the estimated channel impulse responses (CIRs) are quantized to eliminate the impacts of communications noise, channel estimation error and mobility induced channel variation and path arrival time for the CIR-based authentication. Specifically, a noise-mitigated channel estimation method is first utilized to pre-process the achieved CIRs at the base-stations. The proposed quantization algorithm is then applied to the CIR estimates in the dimensions of amplitude and channel path delay respectively, where different step sizes of quantization for all significant channel paths are derived based on a logarithmic likelihood test function by exploiting training symbols between legitimate users prior to establish a communication link. In fact, the physical-layer attribute CIR, is not only used to authenticate the legitimate transmitter to the base-stations but also to generate the random initial sequence numbers for the 3-Way TCP/IP handshake authentication protocol used in the wired part of the network (between the base-station and the servers). Consequently, we have proposed a physical-layer authentication as well as generating a unique sequence numbers related to the legitimate transmitters to be used in the 3-Way TCP/IP authentication method. The efficacy of the proposed authentication scheme has been verified by the numerical simulations.

References

[1] Zeng, K., Govindan, K. and Mohapatra, P. (2010) Non-Cryptographic Authentication and Identification in Wireless Networks. *IEEE Wireless Communications*, **17**, 56-62. http://dx.doi.org/10.1109/MWC.2010.5601959

[2] Xiao, L., Greenstern, L., Mandayam, N. and Trappe, W. (2008) MIMO-Assisted Channel-Based Authentication in Wireless Networks. *IEEE Conference on Information Sciences and Systems* (*CISS*), 642-646.

[3] He, F., Man, H., Kivanc, D. and McNair, B. (2009) EPSON: Enhanced Physical Security in OFDM Networks. *IEEE International Conference on Communications* (*ICC*), 14-18 June 2009, Dresden, 1-5.

[4] Tugnait, J.K. and Kim, H. (2010) A Channel-Based Hypothesis Testing Approach to Enhance User Authentication in Wireless Networks. *IEEE International Conference on Communication Systems and Networks* (*COMSNETS*), 1-9.

[5] Rosati, S., Corazza, G.E. and Coralli, A.V. (2009) OFDM Channel Estimation with Optimal Threshold-Based Selection of CIR Samples. *Proceedings of IEEE Global Telecommunication Conference* (*GLOBE-COM*), 1-7.

[6] Nair, S., Abraham, S. and Al Ibrahim, O. (2011) Security Architecture for Resource-Limited Environments. *International Wireless Communications and Mobile Computing Conference* (*IWCMC*), 412-417,

[7] Goergen, N., Charles Clancy, T. and Newman, T.R. (2010) Physical Layer Authentication Watermarks through Synthetic Channel Emulation. IEEE *Symposium on New Frontiers in Dynamic Spectrum*, 6-9 April 2010, Singapore, 1-7.

[8] Touch, J., Mankin, A. and Bonica, R. (2009) The TCP Authentication Option. draft-ietf-tcpm-tcp-auth-opt-05.

[9] Zalewski, M. (2012) The Tangled Web: A Guide to Securing Modern Web Applications. No Starch Press, San Francisco.

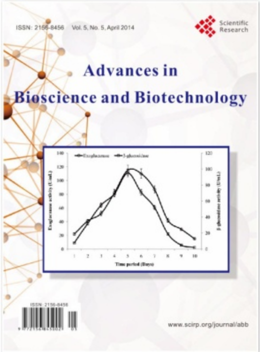
[10] Zalewski, M. (2005) Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. No Starch Press, San Francisco.

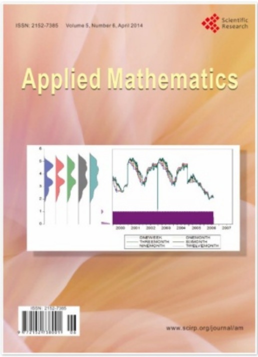
[11] Venkatraman, L. and Agrawal, D.P. (2000) A Novel Authentication Scheme for ad hoc Networks. *Wireless Communications and Networking Conference*, 23-28 September 2000, Chicago, 1268-1273.

[12] Xiao, L., Greenstein, L., Mandayam, N. and Trappe, W. (2008) A Physical-Layer Technique to Enhance Authentication for Mobile Terminals. *IEEE International Conference on Communications* (*ICC*), 19-23 May 2008, Beijing, 1520-1524.

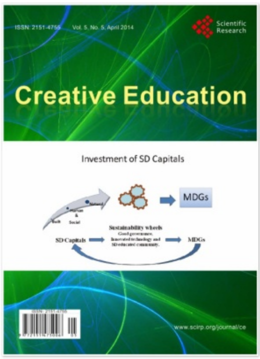
[13] Xiao, L., Greenstein, L., Mandayam, N. and Trappe, W. (2007) Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication. *IEEE International Conference on Communication*, 24-28 June 2007, Glasgow, 4646-4651.

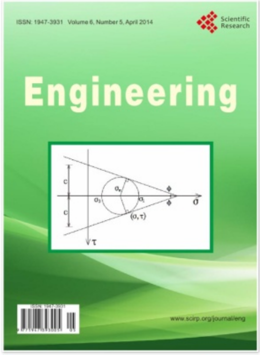
[14] Cain, J., Clark, G. and Geist, J. (1979) Punctured Convolutional Codes of Rate (n-1)/n and Simplified Maximum Likelihood Decoding. *IEEE Transactions on Information Theory*, January 1979, 97-100.


Advances in Bioscience and Biotechnology

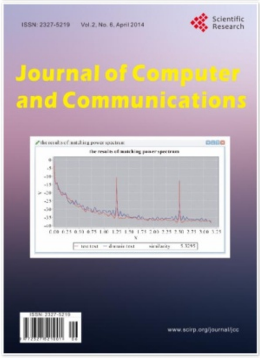

Applied Mathematics

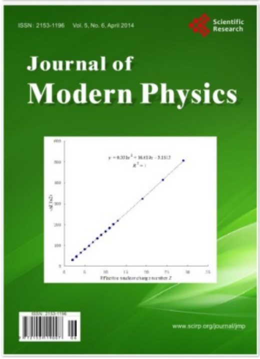
American Journal of Plant Sciences


Creative Education

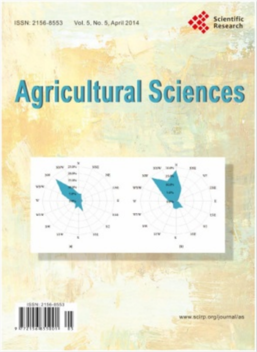

Engineering

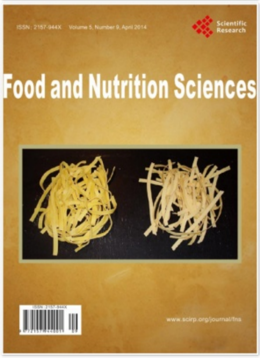
HEALTH

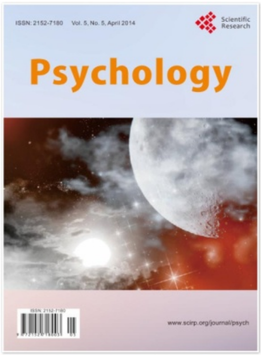

Journal of Computer and Communications


Journal of Modern Physics

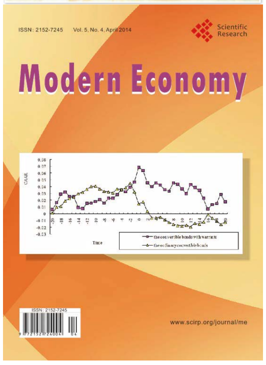
Journal of Environmental Protection


Agricultural Sciences


Food and Nutrition Sciences


Psychology

Natural Science


Modern Economy

Journal of Cancer Therapy

American Journal of Analytical Chemistry