Real-time FPGA-based Non-Cryptography System for Wireless Network

Ali M. Allam and M. M. Abutaleb

Electronic, Communication and Computer Engineering, Helwan University
Cairo, Egypt

Abstract

Traditional privacy techniques for wireless communications are facing great challenges, due to the open radio propagation environment and limited options of transmission techniques. A new bilateral pilot aided protocol is presented, with single-tone based burst transmission over slow time varying flat fading wireless channels, and is investigated to enhance the security of quadrature amplitude modulation (QAM) system. In this paper, a real-time and link privacy method with FPGA-based design is proposed, which is based on the characteristics of radio channel including randomness and privacy. For the proposed approach, the unique instant channel state information (CSI) of channel can be estimated in real-time by a proposed FPGA-based circuit to be used in giving confidentiality for transmitted data. The proposed approach is adequate for most real-time wireless communication systems.

Keywords: *Physical-layer security, Channel State Information, Channel Estimation, FPGA.*

1. Introduction

Confidentiality is the process where only the authorized parity can read the transmitted information. The broadcast nature of the wireless channel exposes the transmission to eavesdropping. Securing the wireless channel is commonly done by implementing enciphering and deciphering algorithms in software, and is usually detached from the physical layer of communication. Most mechanisms of confidentiality of mainstream wireless communication systems, such as cellular mobile communication systems [1], wireless broadband access systems [2] and wireless sensor networks (WSN) [3][4], are based on traditional cryptography encryption and functioned at high layer. The confidentiality is set up by invoking the higher layer protocol stack at call establishing, location updating, and other value-added service.

There are some encryption methods which rely on the physical layer of communication for their implementation, such as spread spectrum Frequency Hopping (FH) and Direct Sequence (DS) [5]. In FH and DS a key has to be distributed securely to set the FH hopping pattern or DS spreading sequence. Many key distribution methods rely on the Diffie-Hellman algorithm [6].
Encryption, decryption and key distribution impose overheads on memory, computation power, energy consumption and data throughput. These overheads are a crucial implementation issue for low complexity systems with strict constraints on system resources [7], such as Wireless Sensor Networks (WSN) and ad-hoc networks [8-9].

Recently channel-like fingerprint has been used to enhance the security in physical layer (PHY) [10]-[16]. Besides the broadcast feature, the radio channels feature randomness and privacy as well due to the multipath propagation effect of radio waveform [17]. That is to say, (1) randomness means the channel state information (CSI) varies rapidly and randomly. (2) privacy means the CSI of the link between communication pair is unique due to the CSI decorrelates rapidly in space and time if the paths are separated by the order of an RF wavelength or more in scatter rich environments. Based on the randomness and privacy features of channel, Faria et.al firstly proposed a scheme in [10] to detect identity-based attacks by using the signal strength information, namely, the instantaneous signal-to-noise ratio (SNR). G. Tsouri and D. Wulish proposed the confidential method using the CSI information in [20].

In this paper, we propose both a bilateral pilot protocol and a real-time FPGA-based confidentiality method in physical layer based on instantaneous CSI. Our method differs with the existed methods on that we estimate the CSI, and then modulate the transmitted signal with it to compensate the effect of channel between transmitter and receiver. The estimation and compensation of the channel phase-shift and attenuation are mandatory components of this system and pose the most significant implementation challenge. The VHDL modules provide a proof of concept

and a framework unto which more sophisticated algorithms can be later developed and tested.

Our method can be reliably used as PHY encryption is due to the observation that the CSI changes continuously in time- and frequency domain, and is unique for each link. It is commonly accepted that a distance of a few wavelengths of carrier frequency is enough to have practically no correlation with eavesdropper link. Since the pilot-aided channel estimation and simple prediction methods are widely applied to obtain the CSI in all kinds of wireless communication systems including single carrier (SC)/multiple carrier (MC) systems and single-input single-output (SISO)/multiple-input multiple-output MIMO systems in all sorts of selective fading channels, the proposed method needs no complicated channel modeling and parameters identification as done in [13], and can be easily applied without introduction of extra complexity, which is of importance for energy-constraint networks like WSN. Since the simplicity of our method, real-time per message encryption is easily realized.

The main contributions of the proposed privacy method are listed below.

- CSI estimation based real-time encryption method is developed in PHY. This method facilitates application in wireless communication systems due to the widely used pilot-aided CSI estimation and simple CSI estimation method without induction of extra complexity or any changes to the exist systems.
- Two-way privacy is achieved when the proposed method is implemented at both sides of the communication pair, and also no extra complexity is introduced due to the CSI estimation is widely applied to obtain CSI in current wireless communication networks.

The rest of the paper is organized as followed. System model is introduced in Section II, and the proposed method is presented in detail in Section III. In Section IV, FPGA-based design is proposed to implement the proposed method, and we conclude the paper in Section V.

2. Bilateral Pilot Protocol

The objective of this protocol is to provide the privacy between transmitter and receiver in full duplex communication mode, beside that we wish to deprive the eavesdropper from immediate estimation of the channel forms the transmitter to itself and also update the pilot signal for privacy. The suggested protocol is modification for reverse piloting protocol in [20] which is used only for simplex transmission mode. We propose the following bilateral piloting protocol for accessing the wireless channel:

1. A local oscillator (LO) at the transmitter is synchronized with a LO at the receiver.
2. The receiver sends a pilot signal, and starts sensing for a received signal.
3. The transmitter estimates the channel from the receiver and deduces the channel from itself to the receiver, based on channel reciprocity.
4. The transmitter sends a burst of QAM data symbols, compensated for channel phase and attenuation.
5. The transmitter stores the last 8 bits of each transmitted data, to be used as updated pilot signal by the receiver.
6. The receiver senses a received signal, and decodes the data symbols based on the a-priory known signal constellation.
7. The receiver tracks the time varying channel phase using some decision feedback method, and after a channel de-correlation period steps 2-6 are repeated, in step 2 receiver use updated pilot.
8. When the receiver needs to transmit a new pilot signal, it will use the last 8 bits of last received data to be used as a pilot and repeats the same steps from 2-7.
9. Repeats the steps from 2-8 according to a flow control mechanism in case of changing the transmission role between parities.

Assuming the channel phase from the transmitter to the receiver is uncorrelated with the channel phase from the transmitter to the eavesdropper, the eavesdropper would receive data symbols with unknown phase shift and attenuation. Beside that we assuming a flow control mechanism to manage the flow between parties.

2.1 Coherence time vs. de-correlation time

Usually the channel coherence time is assumed to be short enough to have a quasi-static channel, so that the channel wouldn't vary significantly during the data burst, and decoding would be unaffected by outdated channel estimates. For our purposes we define a channel de-correlation period, which is set to have the channel de-correlate as much as possible between pilots. This insures that successive channels are uncorrelated, and is also the reason why the receiver needs to track the time varying phase.

2.2 Implementation issues

Since we are interested in evaluating security properties of the proposed bilateral piloting protocol, we assume errorless synchronization of LOs, errorless channel estimates, perfect tracking of channel phase by the receiver, and perfect detection of a received signal at the receiver. We assume the same for the eavesdropper. Note that these assumptions are not a prerequisite for implementing the protocol. Effects of synchronization, estimation and tracking errors on decoding performance are the same as those for a system with conventional pilot signaling. Methods for synchronization of LOs, channel tracking using decision feedback, and the impact of channel estimation errors may be suggested in section four, when we design a FPGA-based circuit for the suggested encryption scheme.

3. Secrecy System Model

In this section we will discuss the mathematical model for physical layer privacy which we will suggest a FPGA-based design for it in the following section. The mathematical model used is following the Shannon's communication theory [19] and assuming the reciprocal property of the channel characteristics.
The low pass equivalent model (baseband model) of the received data symbols $r(t)$ at the receiver may be written as:

$$r(t) = s_D(t) * h(t) + n(t) \quad (1)$$

where $s_D(t)$ is the transmitted information bearing complex symbol, $h(t)$ is a complex random variable representing channel attenuation a_{ch} and phase φ_{ch}, and $n(t)$ is some complex additive noise at the receiver. We write the impulse response $h(t)$ as:

$$h(t) = a_{ch}\delta(t - \tau_{ch}) \quad (2)$$

and the transfer function $H(\omega)$ of this channel as:

$$H(\omega) = a_{ch}\, e^{-j\omega\tau_{ch}} \quad (3)$$

where the phase-shift due to the delay τ_{ch} in the channel ~~is~~ can be represented as:

$$\varphi_{ch} = \omega\tau_{ch} \quad (4)$$

The attenuation and phase-shift of the path between transmitter and receiver is the channel status information (CSI) for the path between the transmitted and the receiver. This CSI is unique for each path, even if with the transmitter and the eavesdropper. It is commonly accepted that a distance of a few wavelengths of carrier frequency is enough to have practically no correlation at all between paths CSI's. For example, for wireless systems working in the frequency range of a few GHz this translates to a distance of a few centimeters [18]. The eavesdropper and receiver are reasonably much farther apart than that.

So the CSI of path can be used as symmetric secret key between transmitter and receiver and it is updated for each coherent period. So the data signal is compensated by reciprocal of transfer function of signal as shown in Fig. 1, then transmitted.

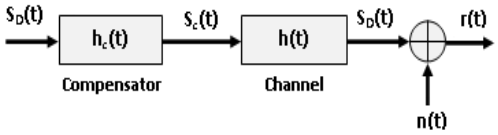

Fig. 1. System Model

The transfer function of the compensator is:

$$H_c(\omega) = \frac{1}{a_{ch}}\, e^{j\omega\tau_{ch}} \quad (5)$$

and its impulse response is:

$$h_c(t) = \frac{1}{a_{ch}}\, \delta(t + \tau_{ch}) \quad (6)$$

So that the cascaded network of compensator and the channel to be:

$$h_c(t) * h(t) = \delta(t) \quad (7)$$

Therefore the transmitted signal at the output of this cascaded network will be:

$$s_D(t) * \delta(t) = s_D(t) \quad (8)$$

and the received signal at the authenticated receiver will be:

$$r(t) = s_D(t) + n(t) \quad (9)$$

Of course, if the eavesdropper received this signal, he will have other impulse response channel $h'(t)$. Therefore the received signal by eavesdropper will be:

$$r(t) = s'_D(t) + n(t) \quad (10)$$

where

$$s'_D(t) = s_D(t) * h_c(t) * h'(t) \quad (11)$$

Since the eavesdropper has no prior knowledge on the compensated parameters, it cannot readily decode its received data symbols, because it has no prior knowledge

of the bit mapping of its received constellation. In [20] proved that this system which modeled as Shannon secrecy system is analogous to a shift cipher.

4. Design Channel Estimator and Compensator (CEC) in FPGA

FPGA technology is being widely used for accelerator control owing to its fast digital processing capability. This work is purely a model to determine the design circuit to implement Channel Estimator and Compensator (CEC) in FPGA technology. It is used to detect the phase-shift and attenuation of pilot signals that are transmitted wirelessly, and then compensate the transmitted signals by the channel effects to be secured.

The main task of the CEC design is to track the channel phase-shift and attenuation via comparison between the pilot and reference signals in transmitting section, and then compensate the transmitted data signals. The input signal is assumed as a series of numerical values (digital signal) via 8-bit of analog to digital conversion (ADC) circuit. The CEC circuit gets the 8 bit signal every clock cycle. The fixed point data representation is used in this work.

The CEC circuit is designed using VHDL, and then simulated and synthesized using ModelSim SE 6.2b simulator and Xilinx ISE 12.2, respectively. The CEC architecture is composed of three basic parts: Channel Phase Compensator (CPC), Channel Attenuation Compensator (CAC), and Transmission Data Compensator (TDC). The complete block diagram of the system is shown in Fig. 2.

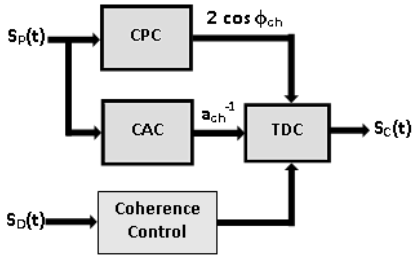

Fig. 2. Block diagram of CEC

In this work, the timing signal of Coherence Control is assumed to be '0' through the processing period and '1' through the data transmission period between pilots as shown in Fig. 3.

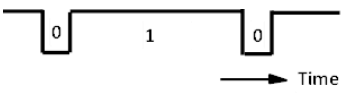

Fig. 3. Coherence Control Signal

4.1 Channel Phase Compensator (CPC)

The architecture of Channel Phase Compensator (CPC) consists of the Synchronization Block (SB) and Generator Block (GB) as shown in Fig. 4.

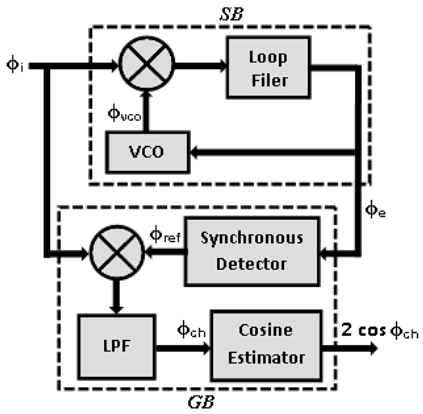

Fig. 4. Block diagram of CPC

Synchronization Block (SB) is a circuit which synchronizes the phase (ϕ_{vco}) of the output signal generated by a voltage controlled oscillator (VCO) with the phase (ϕ_i) of the input signal. The phase difference between the input signal and VCO signal is called phase error (ϕ_e) and the control mechanism acts on the oscillator in such a way to reduce the phase error. Therefore, it is similar to the system PLL.

Multiplier has two inputs and produces the output voltage that mixes the two input signals. This mix produces the sum and difference phases. Booth's multiplication algorithm [21] is used here instead of simple signed arithmetic multiplier. Arithmetic multiplier will consume large area, while Booth's multiplication algorithm for 8-bit multiplication only needs eight 8-bit adders which is much save in area consumption.

The loop filter removes the high-frequency component and produces the output voltage that contains only a DC component. VCO will take this voltage which is proportional to the phase difference and then shift its output signal. It is a simple integrator which accumulates the input value and maps it into predefined cosine ROM; there are 1024 sampling points per cycle. Since one cycle can be divided to four quarter, we only need to define the first quarter with 257 values. The remains quarters are duplicated form the first quarter, where the opposite sign is applied to second and third quarter.

Generator Block (GB) is a circuit which generates the cosine value of channel phase (ϕ_{ch}) with gain of 2. The phase difference between the synchronized input signal

and reference signal is called channel phase ϕ_{ch}. The reference phase (ϕ_{ref}) signal will be generated from the Synchronous Detector depending on the least phase error (ϕ_e) in the synchronization block. The synchronized input signal will multiply with reference signal. Low pass filter (LPF) is used to reject the high frequencies of this signal and then the channel phase (ϕ_{ch}) can be obtained in its cosine value with gain of 2 using the Cosine Estimator.

Finite Impulse Response (FIR) filter is use here to perform digital LPF. This filter is essentially average filter since its output is equal to the average value of its input over the last *n*-tap samples [22], where the tap weights determine the type of the filter whether it is Low-pass or High-pass. It can be implemented by just the right shift operations.

4.2 Channel Attenuation Compensator (CAC)

The architecture of Channel Attenuation Compensator (CAC) is shown in Fig. 5. The CAC system is an automatic system that can detect the peak value of the input signal, and then estimate the inverse value of channel attenuation that is used as compensator for the channel attenuation.

The function of the Peak Detector is to detect the peak value (a_P) of the input signal $S_P(t)$. It means that if the amplitude of input signal increases, the peak detector searches about the maximum (peak) value while if the amplitude of input signal decreases, the peak detector keeps the last peak value in its output and so on. The divider is used to calculate the channel attenuation (a_{ch}) by dividing the peak value (a_P) of the input signal by the peak value (a_{ref}) of the Reference. The channel attenuation (a_{ch}) can be compensated by inverting its value using the Inverse Estimator.

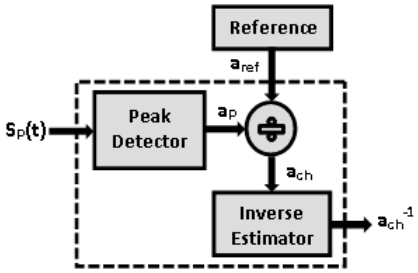

Fig. 5. Block diagram of CAC

4.3 Transmission Data Compensator (TDC)

The architecture of Transmission Data Compensator (TDC) is shown in Fig. 6. It is used to compensate the transmission data (M-ary QAM) signal that has amplitude a_i and phase φ_i:

$$s_D(t) = a_i \cos(\omega t + \varphi_i) \quad (12)$$

to generate the compensated signal:

$$s_c(t) = \frac{a_i}{a_{ch}} \cos(\omega(t + \tau_{ch}) + \varphi_i) \quad (13)$$

which can be written as:

$$s_c(t) = \frac{a_i}{a_{ch}} \cos(\omega t + \varphi_{ch} + \varphi_i) \quad (14)$$

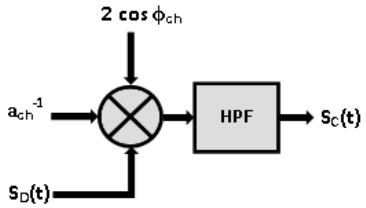

Fig. 6. Block diagram of TDC

Here, multiplier produces the output voltage that contains the sum and difference phases. The high-pass filter (HPF) is used to pass the high-frequency component and produce the compensated signal $S_C(t)$ for secure transmission.

4.4 Simulation and Synthesis Results

A simulation is performed to test the logic function of the hardware design and it is presented to verify the correctness of the architectures implemented in the proposed system. The part of the simulation result is shown in Fig. 7 during the estimation and compensation of channel phase-shift and attenuation.

The first three rows show the system clock, the coherence control signal ('0'), and the pilot signal, respectively. The fourth row and the fifth row are the generated reference-phase signal and the estimated cosine-value of channel phase with gain of 2, respectively. The last three rows show the detected peak-value of pilot signal, the reference peak-value, and the inverting-value of channel attenuation, respectively.

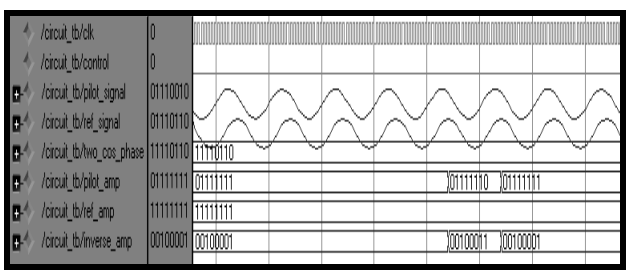

Fig.7. The simulation of the proposed system.

In regard to the designated hardware realization, the VHDL code is synthesized by considering Spartan-3E Xilinx chip XC3S500E. Design is synthesized with Xilinx Synthesize Tool (XST), here we conclude that the total critical path delay is 39.384ns and the total circuit area is 1144 slices with 24% utilization.

5. Conclusion

Lower/physical layer characteristics have been considered as potential alternatives/complements to provide security services in wireless networks. A bilateral piloting protocol based on synchronization and channel phase tracking at the receiver has been presented for securing single-tone transmission over SISO channels. This system has been designed and simulated on a FPGA-based circuit to provide light weight encryption scheme for wireless communication. Real-time performance and efficient hardware are achieved by this method.

References

[1] 3GPP, TS33.102 v5.1.0, ”Technical specification group services and system aspects; 3G security; Security architecture (Release 5),” Dec., 2002.

[2] IEEE 802.16-2009, ”Air interface for broadband wireless access systems,” May 29, 2009.

[3] IEEE 802.15.4, ”Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs),” 2003

[4] ZigBee specification v1.0, ”ZigBee Specification,” 2005.

[5] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill 2002.

[6] W. Diffie and M. E. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, vol. 22, Nov. 1976, pp. 644–54.

[7] N. R. Potlapally, S. Ravi, A. Raghunath and N. K. Jha, “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,” IEEE Transactions on Mobile Computing, vol. 5, no. 2, Feb. 2006, pp. 128-143.

[8] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” IEEE Transactions on Wireless Communications, vol. 11, issue 1, Feb. 2004, pp. 38-47.

[9] G. Guimaraes, E. Souto, D. Sadok, J. Kelner, “Evaluation of security mechanisms in wireless sensor networks,” Proceedings of IEEE Systems Communications, Aug. 2005, pp. 428-433.

[10] D. Faria and D. Cheriton, ”Detecting identity-based attacks in wireless networks using signalprints,” in Proc. ACM Workshop on Wireless Security (ACM WiSe), Los Angeles, CA, Sept. 29, 2006, pp. 43-52.

[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, ”Fingerprints in the ether: Using the physical layer for wireless authentication,” in Proc. IEEE Int. Conf. Commun. (ICC), Glasgow, Scotland. Jun. 24-28, 2007, pp. 4646-4651.

[12] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, ”Using the physical layer for wireless authentication in time-variant channels,” IEEE Trans. on Commun, vol. 7, no.7, 2008, pp. 2571-2579.

[13] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, ”A physicallayer technique to enhance authentication for mobile terminals,” in Proc. IEEE Int. Conf. Commun. (ICC) Beijing, China. May 19-23, 2008, pp. 1520-1524.

[14] Goergen, N., Lin, W.S., Liu, K.J.R., Clancy, T.C., ”Authenticating MIMO Transmissions Using Channel-Like Fingerprinting,” In Proc. IEEE Global Commun. Conf. (GLOBECOM). Miami, Florida, USA. Dec. 6-10, 2010, pp. 1-6.

[15] Fangming He, Hong Man, Wei Wang, ”Physical layer assisted security for mobile OFDM networks,” in Proc. Vehicular Networking Conference (VNC). Jersey City, New Jersey, USA, Dec. 13-15, 2010, pp. 346-353.

[16] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, ”Channel-Based Detection of Sybil Attacks in Wireless Networks,” IEEE Trans. Commun., vol.4, no.3, 2007, pp. 492-503.

[17] A. Goldsmith, ”Wireless Communications,” Cambridge Press, 2005.

[18] W. C. Lee, Mobile Communication Engineering, McGraw-Hill, 1982.

[19] C. E. Shannon, “Communication theory of secrecy systems,” Bell Systems Technical Journal, vol. 28, Oct. 1949, pp. 656-715.

[20] G. R. Tsouri and D. Wulich, "Reverse Piloting Protocol for Securing Wireless Time Varying Channels", IEEE Wireless Telecommunications Symposium (WTS), Apr. 2008.

[21] Douglas J. Smith, HDL Chip Design, Doone Publication, 1996.

[22] Meyer-Baese Uwe, Digital Signal Processing with Field Programmable Gate Arrays (FPGA), 3rd Edition, Springer 2007.