Postprint: Design and Implementation of an SDR-Based Noise Aggregation Physical Layer Security Transmission Scheme

Authors: Qin Pengxiang, Pinyi Ren, Du Qinghe, Sun Li

Date: 2018-12-13T00:00:00+00:00

Abstract

Noise aggregation physical layer security schemes, through coding design combined with feedback control, can fully exploit the inherent noise resources introduced in wireless links, thereby degrading the eavesdropper' s channel quality and enhancing the security performance of communication systems. To verify and evaluate the performance of this scheme in practical systems, transmitter and receiver schemes integrating noise aggregation anti-eavesdropping functionality were designed and implemented based on a software-defined radio platform; on this basis, an anti-eavesdropping test environment comprising a source node, destination node, and eavesdropping node was constructed. Using image transmission service as a test case, objective metrics such as frame error rate and peak signal-to-noise ratio, as well as subjective image quality, were evaluated. The test results demonstrate that the legitimate receiver can obtain favorable signal-to-noise ratio gains compared to the eavesdropper under the same frame error rate conditions; under the same signal-to-noise ratio conditions, it achieves high peak signal-to-noise ratio and clear, distinguishable received images, thereby verifying the effectiveness of the noise aggregation scheme.

Full Text

Design and Implementation of Noise Aggregation Scheme in Physical Layer Security Based on Software Defined Radio

Qin Pengxiang[1],[2], **Ren Pinyi**[1],[2], **Du Qinghe**[1],[2], **Sun Li**[1],[2] 1. School of Electronics & Information Engineering, Xi' an Jiaotong University, Xi' an 710049, China 2. Shaanxi Intelligent Network & Ubiquitous Interconnection Engineering Technology Research Center, Xi' an 710049, China

Abstract: The physical layer security scheme via noise aggregation can degrade the eavesdropper' s channel quality and enhance the security performance of communication systems by fully extracting the resources of inherent noise in wireless links through coding design combined with feedback control. To validate and evaluate the performance of this scheme in practical systems, this paper designs and implements transmitter and receiver schemes with anti-wiretapping capabilities integrated with noise aggregation based on a software defined radio platform. Furthermore, an anti-wiretapping test environment comprising a source node, destination node, and eavesdropping node is constructed. Using image transmission as a test case, objective metrics such as frame error rate and peak signal-to-noise ratio, as well as subjective image quality, are evaluated. Test results demonstrate that the legitimate receiver achieves significant SNR gain compared to the eavesdropper under the same frame error rate conditions, and receives clear, recognizable images with high peak signal-to-noise ratio under the same SNR conditions, thereby verifying the effectiveness of the noise aggregation scheme.

Key words: software defined radio; wireless physical layer security; noise aggregation; image transmission

0 Introduction

With continuous innovation in wireless communication technology, diverse mobile services have become integrated into daily life. However, the inherently open nature of wireless propagation environments exposes communication systems to persistent security threats such as data eavesdropping and privacy protection challenges [1]. Traditional security mechanisms based on cryptography ensure secure transmission through secret key encryption. Their fundamental principle is to impose extremely high computational complexity on eavesdroppers attempting to decrypt information, making decryption infeasible or too time-consuming to be useful. However, the rapid development of high-performance chips in recent years has placed enormous pressure on traditional encryption mechanisms that rely on computational complexity.

Physical layer security technology [2] explores secure transmission in wireless communications from a different perspective. Unlike traditional security mechanisms, physical layer security is based on Shannon' s information theory and exploits the physical characteristics of wireless channels to degrade eavesdropper channel quality without relying on computational complexity, thereby enhancing security. He Hongliang et al. [3,4] combined network coding with ARQ feedback to correlate data packets and enhance file transmission security, investigating the critical role of noise feedback in improving physical layer security performance. Xu Hongbin et al. [5,6] proposed constellation rotation-assisted and constellation overlapping methods for bidirectional cooperative systems to prevent untrusted relays from decoding confidential information. Ding Zhiguo et al. [7] studied the impact of antenna selection on system security performance.

The noise aggregation [8] physical layer security scheme is a novel physical layer security technology proposed in recent years that can degrade eavesdropper channel quality by utilizing inherent noise in wireless links. Combined with feedback retransmission mechanisms, it can ensure reliable transmission for legitimate receivers while allowing eavesdroppers to decrypt minimal or no confidential information, thereby achieving secure transmission. The noise aggregation physical layer security scheme leverages inherently harmful noise without introducing artificial noise, ensures security through simple feedback retransmission mechanisms, and can be combined with most physical layer security technologies to further enhance security levels.

Current research on noise aggregation physical layer security schemes remains in the theoretical analysis and simulation evaluation stage. Reference [8] elaborated on the principles of the noise aggregation physical layer security scheme and simulated and compared the bit error rate and frame error rate of legitimate receivers and eavesdroppers under different channel qualities when applying the noise aggregation scheme. Reference [9] analyzed the average secrecy rate of legitimate receivers and eavesdroppers in binary symmetric channels when applying the noise aggregation scheme. To date, no related research has validated or evaluated the noise aggregation physical layer security scheme in practical systems, resulting in limited practical significance.

Based on the above concepts and previous research, this paper utilizes NI' s Universal Software Radio Peripheral (USRP-RIO) [10] to design and construct a communication system oriented toward the noise aggregation security scheme. Using image transmission as an example, the effectiveness of the noise aggregation physical layer security scheme is tested and verified.

1 System Model

The system model for noise aggregation is shown in [Figure 1: see original paper], which includes a single source node Alice, a single destination node Bob, and a single eavesdropping node Eve. Compared with the Wire-tap model [11], this network features not only a legitimate link but also a feedback link between Bob and Alice. In the presence of Eve, Alice needs to transmit confidential information to Bob.

In Figure 1, X represents the confidential information to be transmitted, which becomes the transmitted information Z after security scheme processing; h_B and h_E denote the channel gains of the legitimate channel and eavesdropping channel, respectively; n_B and n_E represent the noise at Bob's and Eve's receivers, respectively; Y_B and Y_E denote the information received by Bob and Eve; and $\hat{X}_B$ and $\hat{X}_E$ represent the confidential information recovered by Bob and Eve, respectively.

When Alice transmits confidential information to Bob, due to the open nature of the wireless propagation environment, Alice' s transmitted signal is received by Bob through the legitimate channel and by Eve through the eavesdropping

channel. Assuming that Bob' s and Eve' s receivers are identical, and that both the legitimate and eavesdropping channels are quasi-static fading channels that are independent of each other. Since a feedback link exists between Bob and Alice, when Bob experiences frame loss, it can promptly inform Alice through feedback and request retransmission of the lost frame. However, no feedback link exists between Eve and Alice, so when Bob receives a correct frame, Eve may still not have correctly received that frame. At this point, Eve permanently loses the confidential information contained in that frame, preventing Eve from receiving complete information and thereby achieving secure transmission.

In the above system model, without a security scheme, Bob' s only advantage over Eve is the feedback link. Furthermore, when the legitimate channel quality is comparable to the eavesdropping channel quality and both frame error rates approach 1, the probability that Eve has not correctly received a frame after Bob has correctly received it is only 50%. In this scenario, Eve can correctly receive approximately half of the confidential information, resulting in poor confidentiality.

2 Principles of Noise Aggregation Scheme

The noise aggregation scheme can degrade channel quality by utilizing inherent noise in the channel. Combined with feedback mechanisms, it significantly increases the probability that Eve has not correctly received a frame after Bob has correctly received it, ensuring that Eve receives minimal or zero effective information, thereby guaranteeing information security. The principle of the currently proposed noise aggregation scheme is shown in [Figure 2: see original paper].

Consider a binary symmetric channel with error probability ε. The original frame is formed by equally-divided pre-transmitted bit data. When sending the t-th frame: if t is odd, send X_t directly; if t is even, send $X_{t-1} \oplus X_t$. W_i is the noise accompanying the i-th received frame.

The noise aggregation scheme requires even-numbered frames to be decoded together with the previous odd-numbered frame. If Eve loses an even-numbered frame, it cannot decrypt the information it contains. Even if Eve correctly receives an even-numbered frame but loses the previous odd-numbered frame, decryption is still impossible. This demonstrates that the noise aggregation scheme increases the frame loss rate of even-numbered frames, effectively degrading the even-numbered frame channel. Although both Bob' s and Eve' s even-numbered frame channels are degraded, the feedback link between Bob and Alice enables reliable transmission through feedback protocols.

3.1 Overview of Verification System

This paper designs and constructs a wireless communication system and test scenario oriented toward noise aggregation using USRP-RIO equipment based

on the system model and noise aggregation scheme principles described above.

The network topology of the test scheme is shown in Figure 3: see original paper, and the test scenario is shown in Figure 3: see original paper. In Figure 3: see original paper, h_b, h_e, and h_b' represent the channel gains of the legitimate transmission channel, eavesdropping channel, and feedback channel, respectively.

The hardware components of the system mainly consist of three PCs, three USRP-RIO devices, and an external clock source. The three devices represent Alice, Bob, and Eve, respectively. The USRP-RIO devices, primarily composed of RF circuits, implement wireless signal transmission/reception, mixing, digital-to-analog/analog-to-digital conversion, and digital up/down conversion. The three devices use the same external clock source and are each connected to a PC via a PCIe bus for high-speed data transmission, enabling real-time acquisition and baseband processing of wireless signals. The software component processes baseband digital sampling signals using LabVIEW and MATLAB software on the Windows platform. Additionally, LabVIEW implements human-computer interaction through the front panel of .VI files. By calling MATLAB scripts and writing code in LabVIEW, the noise aggregation physical layer security scheme and other baseband data processing functions can be implemented. Leveraging LabVIEW' s multi-threading and modular characteristics, editing the block diagram in .VI files enables simultaneous frame assembly and disassembly, thereby achieving real-time data transmission or feedback between nodes.

3.2 Link and Frame Structure Design

Based on the analysis of application scenarios and functional requirements, the digital communication link and frame structure design oriented toward noise aggregation is shown in Figure 4. [Figure 4: see original paper] Digital communication link and frame structure for noise aggregation

3.3 Transmitter Design

The transmitter oriented toward the noise aggregation scheme consists of a baseband component and an up-conversion component. The baseband component includes noise aggregation, channel coding, interleaving, digital modulation, and pulse shaping filtering, implementing baseband processing of data. The up-conversion component includes digital up-conversion, DAC (digital-to-analog converter), and mixer, implementing up-conversion processing of data. Bit data is transformed into wireless RF signals after baseband and up-conversion processing and is transmitted through the antenna.

3.3.1 Frame Structure Design

The frame structure of the link references the 802.11 standard. Based on the frame aggregation mechanism in 802.11n [12], the link employs a modified A-

MPDU (MPDU aggregation) frame as the physical frame structure, as shown in Figure 4.

Considering the channel delay spread, time-varying characteristics, and baseband rate of the communication system in practical scenarios, the designed physical frame consists of a 544-symbol physical frame header and a 44,928-symbol aggregated physical service data unit.

The physical frame header includes a synchronization header, frame length, and FCS (frame check sequence). Since it affects bit synchronization, BPSK modulation is adopted. An excessively long synchronization header reduces the proportion of effective data in the physical frame, decreasing efficiency, while an excessively short one reduces synchronization accuracy. Therefore, a moderately long 512-bit m-sequence is selected. The excellent correlation properties of the m-sequence enable precise bit synchronization. The 16-bit frame length indicates the number of valid subframes contained in the physical frame. The FCS of the physical frame header uses 16-bit CRC checksum.

The aggregated physical service data unit consists of 18 subframes, each 2,496 symbols long. Each subframe includes a 64-symbol pilot and a 2,432-symbol MAC protocol data unit. Considering indoor channel coherence time and transmitter baseband rate, the pilot interval length (i.e., subframe length) should be approximately 2,500 symbols. Additionally, considering that pilots must satisfy the principles of equal probability of 0 and 1 occurrence and moderate length, a 64-bit m-sequence is selected as the pilot for DC offset elimination and channel estimation.

The MAC protocol data unit consists of a MAC frame header, MAC service data unit, and FCS after convolutional coding and interleaving. The MAC frame header occupies 112 bits, the FCS occupies 32 bits, and the length of the MAC service data unit is determined by the modulation scheme. For QPSK modulation, the MAC service data unit occupies 2,288 bits; for 16QAM modulation, it occupies 4,720 bits. The 32-bit FCS uses CRC checksum for error detection of the MAC service data unit.

The MAC frame header consists of an 8-bit destination address, 8-bit source address, 32-bit total byte count, 32-bit subframe number, 16-bit valid bit count, and 16-bit FCS. The 32-bit total byte count represents the total byte size of the transmitted file. The 16-bit valid bit count indicates the number of valid information bits in the MAC protocol data unit of that subframe. The FCS uses 16-bit CRC checksum for error detection of the MAC frame header.

3.3.2 Source Data Processing

Images are common transmission objects in wireless secure communications, and comparing image quality between Bob and Eve can intuitively demonstrate the security effectiveness of the scheme. Therefore, images are selected as the data source. To prevent Eve from being unable to display images due to loss of

image configuration information, the image file is pre-split into configuration information and pixel information. During testing, Alice only transmits the pixel information. After reception, Bob and Eve combine the received information with the known configuration information to generate image files.

If Alice transmits pixel data in row order, when Eve completely loses a frame, it only loses the row-direction pixel information contained in that frame. Since losing non-adjacent row-direction information does not affect overall image recognition, and the probability of simultaneously losing adjacent row-direction information is extremely small, transmitting in row order cannot achieve image confidentiality. The same applies to column-order transmission.

To address this issue, when parsing image pixel information, the image is divided into appropriately sized rectangular blocks, which are then randomly sorted and framed for transmission. If Eve experiences frame loss, since each frame contains pixel information from many adjacent rows and columns, Eve will lose the image block information contained in that frame. Consequently, Eve cannot recognize the image, achieving the image confidentiality effect.

3.4 Receiver Design

The receiver oriented toward the noise aggregation scheme consists of a down-conversion component and a baseband component. The down-conversion component includes a mixer, ADC (analog-to-digital converter), and digital down-conversion, implementing down-conversion processing of data. The baseband component includes bit synchronization, matched filtering, channel estimation, digital demodulation, deinterleaving, channel decoding, and noise aggregation removal, implementing baseband processing of data. Wireless RF signals received by the antenna are transformed into bit data after down-conversion and baseband processing. Eve' s receiver is identical to Bob' s but without a transmitter.

The experimental USRP-RIO device is a direct-conversion receiver [13], also known as a zero-IF receiver. Unlike superheterodyne receivers, its local oscillator frequency is approximately equal to the carrier frequency, which simplifies the receiver structure but introduces additional DC offset.

Bit synchronization requires selecting correlation peaks, and the presence of DC offset can cause "false peaks" in the correlated sequence. Moreover, DC offset alters the Euclidean distance between decision variables and standard constellation points, thereby affecting symbol decision. Without DC offset elimination, operations such as bit synchronization and symbol decision cannot function properly.

The Hanning window can separate most AC energy from the DC region, thereby eliminating "false peaks" during bit synchronization. However, the Hanning window also eliminates the impulse of the baseband signal at zero frequency, so this method is only used to assist bit synchronization. After bit synchronization is

completed, the baseband signal without Hanning window after matched filtering is as follows:

$$y_k = \sum_l h_k s_{k-l} + \sum_l n_{k-l} + C$$

where S is the joint gain of transmission and reception, h is the channel coefficient, m is the transmitted waveform sampling, N is the noise variance, Z is the noise, C is the DC component, and H is the unit impulse response of the matched filter.

Sampled at the moment of maximum SNR:

$$y_k = a_n w_n + ...$$

where n is the noise sampling and a is the transmitted symbol. Based on the characteristic that m-sequences have equal numbers of 0s and 1s, pilots are BPSK modulated, and the noise is zero-mean Gaussian white noise, taking the average of y_k only leaves the C term, achieving the purpose of eliminating the DC component without losing impulse information of the baseband signal at zero frequency.

3.4.2 Feedback Protocol Design

In the system model described above, the feedback link is a crucial aspect that distinguishes Bob from Eve, ensuring Bob' s reliable transmission. The feedback link requires support from feedback protocols, and the choice of feedback protocol affects Eve' s reception performance and consequently the system' s security performance. Currently, most feedback protocols in practical communication systems adopt ARQ (automatic repeat request) protocols. Common ARQ protocols include stop-and-wait ARQ, continuous ARQ, and selective repeat ARQ.

If stop-and-wait ARQ is adopted, the transmitter continuously retransmits a frame until it receives the corresponding ACK (acknowledgement) frame. However, when channel quality is poor, the transmitter spends excessive time retransmitting the same frame, resulting in very low transmission efficiency.

If continuous ARQ is adopted, due to the sliding window, the transmitter can continue sending the next frame without receiving an ACK frame. However, when channel quality is poor, Go-back-N occurs. In this case, Alice retransmits frames that Bob has already correctly received, increasing the probability that Eve correctly receives frames and thereby reducing system security performance.

If selective repeat ARQ is adopted, the transmitter can continuously send multiple frames without waiting for receiver acknowledgment and only retransmits lost frames. Compared with stop-and-wait ARQ, transmission efficiency is greatly improved; compared with continuous ARQ, it does not retransmit frames that Bob has already correctly received due to Go-back-N.

4.1 Experimental Parameters

In the actual wireless communication system, Alice and Bob communicate using frequency-division half-duplex with single-carrier modulation, with a transmission band of 5 GHz and a feedback band of 2.4 GHz. Since Eve has no transmitter, Eve can only passively eavesdrop on the transmission band. The indicator parameters of the wireless digital communication link are shown in and .

Table 1 Indicators and methods in digital communication link - Pulse shaping (matched) filter: Root-raised cosine filter - Correlation peak threshold setting: Maximum likelihood delay estimation [14] - 1/2 convolutional coding: Mean method [15] - QPSK; 16QAM: Maximum likelihood decision - Viterbi decoding

Table 2 Parameters and corresponding values in digital communication link - Convolutional coding octal generator matrix: [133, 171] - Block interleaving depth: 100 kHz - Root-raised cosine filter correlation symbol length: 300 ksps - Root-raised cosine filter roll-off factor: 1 Msps - Transmitter oversampling rate - Receiver oversampling rate

Since channel coding employs 1/2-rate convolutional coding and the physical frame includes redundant information such as headers and pilots, the actual transmission rate is approximately 10 kBps under QPSK modulation and approximately 20 kBps under 16QAM modulation.

4.2 Observation Interface

Since Alice, Bob, and Eve implement different functions, their human-computer interaction interfaces are slightly different but generally similar. Taking the Eve node as an example, the LabVIEW-based human-computer interaction interface is shown in [Figure 5: see original paper]. The interface is mainly divided into three parts: RF configuration, baseband configuration, and real-time observation.

In the RF configuration module, users can easily configure the transceiver antenna port, oversampling frequency, transmission or reception gain, generation or capture method, and oversampling rate.

In the baseband configuration module, users can set parameters such as the number of subframes, subframe length, digital modulation method, number of correlation symbols and roll-off coefficient of the pulse shaping filter, reception sequence length, and baseband rate.

In the real-time observation module, users can observe in real time the baseband waveform of the received signal, power spectrum, power level, real-time reception progress of files, current lost frame numbers, average reception power, and other information. After reception is complete, indicators such as peak signal-to-noise ratio and frame error rate of the received image compared to the original image can also be read.

In addition to the main modules described above, the human-computer interaction interface also includes clock source selection, transmitted file selection, reception address selection, comparison file selection, and other components.

4.3 Test Results

Since the three USRP-RIO devices are identical, the noise variance of Bob and Eve can be considered approximately the same, and the average reception SNR is determined solely by the average reception power. By adjusting the average reception power of Bob and Eve, their average reception SNRs can be ensured to be identical.

Using image transmission as an example, experiments recorded the frame error rates of Bob and Eve under different modulation methods and different average reception power conditions, as shown in and .

Table 3 Frame error rate at Bob and Eve in QPSK modulation **Table 4** Frame error rate at Bob and Eve in 16QAM modulation

Comparing Table 3 and Table 4 reveals that under both QPSK and 16QAM modulation, Bob always achieves significant average reception power gain compared to Eve under the same frame error rate conditions, demonstrating that the eavesdropper' s channel has been degraded.

To more intuitively illustrate the advantages of the noise aggregation scheme, [Figure 6: see original paper] shows the images transmitted by Alice and received by Eve and Bob at an average reception power of 373 W under 16QAM modulation.

As can be seen, under the same average reception power and channel quality conditions, Eve' s received image is severely corrupted and completely unrecognizable, while Bob can recover the original image, achieving secure transmission.

Objective evaluation of image quality is equally important as subjective evaluation. By calculating the PSNR (peak signal-to-noise ratio) of images, an objective assessment of image quality can be obtained, reflecting the similarity between images. A smaller PSNR value indicates greater distortion.

Since Bob receives reliably, only Eve has PSNR values. Experiments recorded the PSNR values of Eve' s received images compared to the original image under different modulation methods and different average reception power conditions, as shown in .

Table 5 PSNR of received image at Eve

Table 5 shows that under both QPSK and 16QAM modulation and different average reception power conditions, the PSNR values of Eve' s received images compared to the original image are all below the common benchmark of 30 dB. Therefore, Eve' s images can be considered significantly degraded compared to Bob' s, confirming the effectiveness of the noise aggregation scheme.

5 Conclusion

Based on the software defined radio platform, this paper designs transmitter and receiver schemes with integrated noise aggregation anti-wiretapping capabilities and constructs a corresponding anti-wiretapping test environment. Using image transmission as an example, the confidentiality performance of the noise aggregation physical layer scheme is verified with measured data. Building upon existing theoretical analysis and simulation evaluation, this work provides practical evidence for the effectiveness of the noise aggregation scheme. Additionally, the digital communication link and frame structure design based on software defined radio provides a reference for subsequent improvements and prototype implementation of other physical layer security schemes.

References

[1] Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. Summary of information safety [J]. Scientia Sinica: Technologica, 2007, 37(2): 129-150.

[2] Bloch M, Barros J. Physical-layer security: from information theory to security engineering [M]. Cambridge: Cambridge University Press, 2011.

[3] He Hongliang, Ren Pinyi. Secure ARQ protocol for wireless communications: performance analysis and packet coding design [J]. IEEE Trans on Vehicular Technology, 2018, PP(99): 1-1.

[4] He Hongliang, Ren Pinyi, Sun Li, et al. Secure communication using noisy feedback [C]//Proc of Global Communications Conference. IEEE, 2016: 1-6.

[5] Xu Hongbin, Sun Li, Ren Pinyi, et al. Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach [J]. IEEE Communications Letters, 2015, 19(12): 2270-2273.

[6] Xu Hongbin, Sun Li, Li Fan. Towards enhanced security for two-way untrusted relaying systems: a constellation overlapping scheme [C]//Proc of IEEE International Conference on Communications. IEEE, 2018: 1-7.

[7] Ding Zhiguo, Ma Zheng, Fan Pingzhi. Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise [J]. IEEE Trans on Wireless Communications, 2014, 13(4): 2189-2203.

[8] Hussain Mukhtar, Du Qinghe, Sun Li, et al. Security enhancement for video transmission via noise aggregation in immersive systems [J]. Multimedia Tools & Applications, 2016, 75(9): 5345-5357.

[9] Xu Qian, Ren Pinyi, Du Qinghe, et al. On achievable secrecy rate by noise aggregation over wireless fading channels [C]//Proc of IEEE International Conference on Communications. IEEE, 2016: 1-6.

[10] Xiang Xin. Principle and technology of software radio [M]. Xi' an: Xidian University Press, 2008.

[11] Wyner A D. The wire-tap channel [J]. Bell Labs Technical Journal, 1975, 54(8): 1355-1387.

[12] Liu Weimu, Liu Houquan. Analysis of WLAN IEEE 802.11n standard [J]. Information & Communications, 2008, 21(4): 36-39.

[13] Razabi B. Design Consideration for Direct-Conversion Receivers [J]. IEEE Trans. on Circuits Syst. ii, 1997, 44(6): 428-435.

[14] Forney G. Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference [J]. IEEE Trans on Information Theory, 2003, 18(3): 363-378.

[15] Wang Sen. Design and implementation of communication system based on Software Radio [D]. Xi' an: Xidian University, 2015.

Note: Figure translations are in progress. See original paper for figures.