Multimed Tools Appl (2016) 75:5345–5357
DOI 10.1007/s11042-015-2936-3

Security enhancement for video transmission via noise aggregation in immersive systems

Mukhtar Hussain[1] · Qinghe Du[1] · Li Sun[1] · Pinyi Ren[1]

Received: 10 April 2015 / Revised: 12 July 2015 / Accepted: 1 September 2015 /
Published online: 26 September 2015

Abstract The interest in the field of immersive audio/visual systems exists for many years from both of the commercialization point of view and the research perspective. Technological advancements in the field of cameras, video display along with the processing hardware lead the way to a new generation of immersive systems. On one hand, advancement in video compression schemes like MPEG and H.264/AVC, and transmission technologies like and 3G and 4G LTE enhanced the feeling of virtual presence. However, on the other hand the secure transmission of immersive audio/visual contents over wireless networks is a challenge, as it suffers from the potential malicious attacks. One type of typical malicious attack is passive eavesdropping. The goal of this paper is to propose a solution to enhance the secure wireless transmissions of Video in Immersive Systems via simple yet effective physical-layer approach. To reduce the chance that that the passive eavesdropper extracts information, we present a physical-layer security method, termed noise aggregation, for the secure video transmission to legitimate receiver. Theoretical analyses and simulation results demonstrate that our method is able to effectively limit the amount of information eavesdropped by the unauthorized user at bit level, and thus significantly enhancing security for video distribution.

Keywords Immersive systems · Noise aggregation · Video transmission · Physical layer security

✉ Qinghe Du
duqinghe@mail.xjtu.edu.cn

Mukhtar Hussain
mukhtar.ciit@gmail.com

[1] Department of Information and Communications Engineering, School of Electronic and Information Engineering, Xi'an Jiaotong University, 28 West Xianning Road, Xian, Shaanxi 710049, China

1 Introduction

In recent years, evolution in the field of computing, networking and communications made immersive systems popular. Tele-immersion is sought after to be the next generation of communications. Immersive audio/visual systems provide the end users a level of multimodal multimedia intercommunications that cannot be achieved by conventional 2D systems.

The research projects like blue-c [10] at ETH Zurich and TEEVE (Tele-immersive Environments for Everybody) [17] at the University of Illinois and the University of California at Berkeley have provided a platform for the development real time immersive system. These projects aim to provide users an immersive environment using the existing three-dimensional (3D) capture, transmit and visualization tools. The significant challenges associated with the transmission of 3D videos have been overcome with the advancement in both video compression and transmission technologies like MPEG, H.264/AVC and 4G LTE, respectively.

The proliferation of immersive audio/visual applications, urge for the secure transmission of multimedia content, especially over the wireless networks. One of the most challenging security issues is to guarantee the integrity of media content against the malicious intruder (eavesdropper). It is very easy to eavesdrop on wireless medium due to its broadcast nature. A commonly used model to characterize physical-layer security schemes was presented in [16]. Specifically, a transmitter (called Alice) expects to transmit secret message to the legitimate receiver (called Bob), but does not want the message to be overheard by the eavesdropper (called Eve). The eavesdropper is assumed to be passive, and thus, it is hard to eliminate eavesdropper to access wireless networks.

By means of cryptographic primitives, the secure transmission of wireless multimedia content mainly depends on upper layers processing such as transport layer, network layer, and application layer, while physical layer security [18] is often overlooked. Figure 1 shows a typical example of multimedia communications over wireless channel, where the multimedia content is transmitted over the wireless channel from a transmitter to a receiver in the presence of a passive eavesdropper. Secrecy in typical wireless networks is usually achieved by key-based enciphering techniques at upper protocol layers. Particularly, a secret key is shared between the transmitter and the legitimate receiver to encrypt and decrypt the data. It is widely assumed to be computationally infeasible for the eavesdropper to decipher when lacking the knowledge of secret key. However, encryption techniques like ciphers are insufficient due to the continual growth of computational power. The main idea behind this paper is to limit the amount of information that can be extracted by unauthorized user by physical-layer techniques rather than encryption techniques. Our goal is to decrease the information leaked to the eavesdropper at bit level by means of physical-layer security, with no limitations assumed on the channel quality and computational resources of unauthorized receiver. We present a novel noise aggregation method for the secure transmission of data to legitimate user over the wireless channel. Our proposed method is able to enhance secrecy even when eavesdropper is under the same channel conditions as the intended receiver.

The rest of the paper is outlined as in Section 2, existing approaches for secure video communication are reviewed. In Section 3, we describe the system model for the noise aggregation method. Section 4, we propose the noise aggregation method, conduct the probabilistic analysis of the proposed scheme, and apply it in Immersive Systems. In Section 5, we present the simulation results for our noise aggregation scheme. The paper concludes with Section 6.

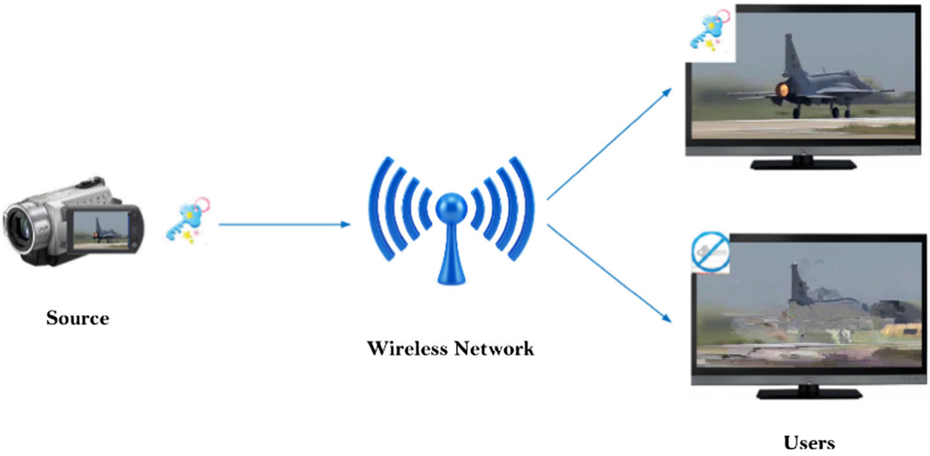

Fig. 1 Multimedia transmission over wireless channel

2 Related work

For quite a long time the major focus in the field of multimedia communication over wireless channel was to optimize the video compression algorithms. The major focus of the researchers were to meet video's Quality of Service (QoS) requirements and muddle through the copyright violations. The secure video communication over the wireless channel majorly relied on the cipher based encryption techniques at network or higher layers. Voloshynovskiy et al. [14] presented a framework for multimedia security and secure communication based on data hiding methods. They proposed visual scrambling and steganography methods for secure multimedia communication. These methods are key based enciphering methods for video communication that are error resilient to the wireless channel. However these methods can be surpassed using high computational power by eavesdropper.

Liang Zhou et al. [18] presented a cross layer architecture for secure multimedia communication as well as to cope with copyright violations. Application layer technologies like watermarking and authentication technologies [6] to cope with copyright violations and to verify the integrity of the multimedia content and source. Authentication methods aid the receiver to verify that the multimedia content is transmitted by legitimate transmitter. While Secrecy Capacity (SC) techniques [12] at physical layer provide secrecy against the passive eavesdropper. They investigated the existing application layer and physical layer technologies and presented a joint application and physical layer security mechanism. The fundamental principle behind the physical layer security is to limit the amount of information that can be extracted by unauthorized user at bit level [1]. In past, Ciphers were considered to be unbreakable without the knowledge of secret key. However with the relentless growth of computational power ciphers are continually surmounted [12].

Initial theoretical work by Shannon in [11] and Wayner in [16] for secrecy capacity (SC) has gained a lot of attention in the field of information security. Shannon describes SC as the maximum achievable transmission rate when legitimate users suffer from eavesdropping by unauthorized users. He suggested a perfect cipher, also known as one-time pad proposed by Vernam [13] can achieve perfect secrecy if secret key is as long as the plain text message. However such a cipher is completely impractical to be implemented in real time. Hence based on Shannon's assumption all presently used ciphers can be theoretically broken.

Wyner in [16] presented a concept of wiretap channel to achieve virtually perfect secrecy. The wiretap channel (eavesdropper's channel) is assumed to be noisier than the main channel (legitimate receiver's channel). Under this condition it is possible to achieve perfect secrecy without relying on ciphers. However, in wireless communication systems it is impossible to assure that eavesdropper's channel is always noisier than legitimate receiver's channel.

During 1970s and 1980s the research work in the field of physical layer security was limited due to the strict secrecy capacity defined by Shannon and classical wiretap channel by Wyner requires legitimate users to have advantage over eavesdropper. However the work of Maurer [9] cause to regain the interest in the field of physical layer security. He describe the secrecy capacity as the maximum rate at which a transmitter can send information to the intended receiver in the presence of eavesdropper, as a function of binary entropy of channel error probabilities.

Baldi et al. [2] presented a physical layer security through *Scrambled Codes and ARQ protocol.* They have proposed non-systematic channel codes (based on scrambling) over the AWGN wiretap channel. The legitimate user also have the facility of ARQ but eavesdropper cannot enjoy such facility. The secrecy is only achieved by considering limitation to the eavesdropper channel. Hence this scheme cannot work when Eve have better channel quality then Bob.

Harrison and Boyce presented a physical layer security method based on linear block codes for binary erasure wiretap channel (BEC) [7, 8]. The idea behind the proposed method is to intentionally erase certain bits from the coded message signal to weaken the corrective capability of the codes at eavesdropper end. The main channel between the legitimate users Alice and Bob is assumed to be error free whereas the wiretap channel is assumed to be BEC, hence further erasure in the transmitted bits limit the information leakage to Eve. The proposed method was tested against the maximum likelihood and maximum passing strategies that can be utilized by the eavesdropper to correct the erased bits and extract information. However this method is also impractical due to the assumption of noiseless main channel.

In [5] Bloch et al. presented the physical layer security method based on secret key agreement between the legitimate users. The key idea behind this method is to exploit the randomness of fading channel to generate a secret between the legitimate users Alice and Bob. No limitation on eavesdropper's channel is assumed, however it is presumed that transmitter have the complete information of the channel gains of legitimate receiver and the eavesdropper. The authors have also extended their work to imperfect CSI case in [3].

3 System model

The system model for this paper is shown in Fig. 2, similar to the Wyner *wiretap channel model* [16]. However in our system model the main channel is not noiseless and the addition of noiseless feedback channel for authenticated receiver. At transmitter side it is require to achieve reliable and secure communication with the legitimate receiver in the presence of passive eavesdropper. Alice is sending a video packet to a user Bob over the main channel, while Eve is also receiving data over the wiretap channel. The main and wiretap channel are assumed to be independent of each other; implies that the passive eavesdropper Eve may enjoy better channel quality than legitimate user Bob. It signifies that our proposed method is not limited to degraded scenarios. It can also be noted in Fig. 2 that Bob has the facility to request retransmission of lost packets however Eve does not have such a facility, hence Eve could only get the missing packets unless it is requested by Bob. For example, if any packet is not received by Eve however Bob successfully receive the packet, Bob will not request for Eve's lost packet.

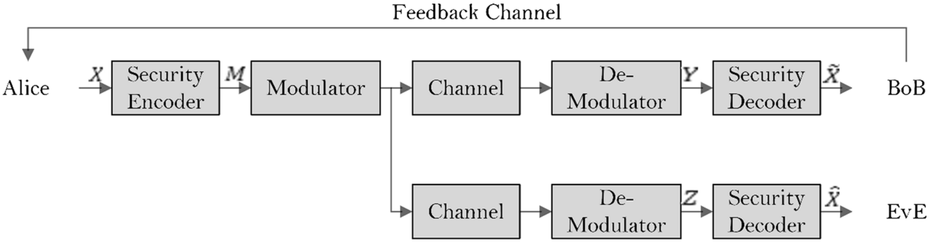

Fig. 2 System Model with feedback channel assuming the same main and wiretap wireless channel

Figure 2 shows that Alice wants to transmit private message X to the desired receiver Bob. She encodes the message X using Nosie Aggregation method and sends the encoded message M, over the wireless channel. The desired receiver Bob and a passive eavesdropper Eve receive the encoded messages as Y and Z respectively. Assuming that the passive eavesdropper already knows about the encoding algorithm, both Bob and Eve start decoding the received messages using Nosie Aggregation method and get decoded messages as $\tilde{X}$ and $\hat{X}$ respectively. Security encoding algorithm is discussed in detail in Section 4.

4 Noise aggregation approach for security enhancement in immersive systems system model

4.1 Principles of noise aggregation for security enhancement

Let's assume Alice has a collection of message packets $X=X_1,X_2,\ldots,X_N$ to be transmitted. The security encoder at the transmitter side performs bitwise exclusive-or (XOR) operation on even packets with odd ones. However odd packets are transmitted without encoding. To decode the message correctly at destination, receiver requires to get all odd packets correctly. Hence loss of odd packet tends to loss of next even packet as well. The input and output of the security encoder at the transmitter is characterized as X and M given in Fig. 3, where

$$M_i = X_i \quad for\ i = 1,3,5,\ldots,2n{-}1 \tag{1}$$

$$M_i = X_i \oplus X_{i-1} \quad for\ i = 2,4,6,\ldots,2n \tag{2}$$

Let's assume message packets received by Bob and Eve corrupted by the channel affect are $Y=Y_1,Y_2,\ldots,Y_N$ and $Z=Z_1,Z_2,\ldots,Z_N$ respectively; as given in Fig. 2, where

$$Y_i = M_i \oplus W_i \tag{3}$$

$$Z_i = M_i \oplus U_i \tag{4}$$

When receiver start decoding the received packets noise of previous packet will be superimposed into the next packet, hence this technique is called noise aggregation method. The output of the security decoder at the receiver side Bob and Eve is given in Figs. 4 and 5 respectively. Following assumptions can be made based on the received packets.

- Bob receives packet $\tilde{X}_1$ correctly and able to decode next security-enhanced packet Y_2 to extract the required information $\tilde{X}_2$ however if Eve is unable to receive packet $\hat{X}_1$ he will

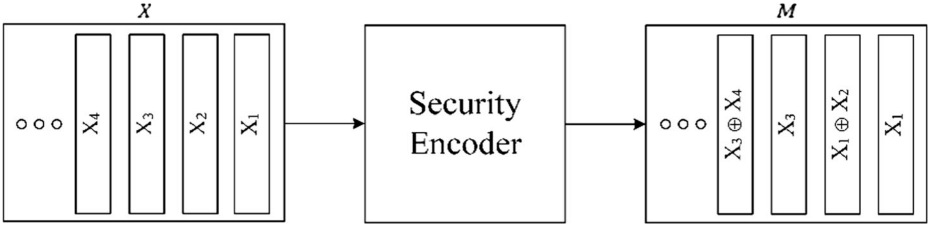

Fig. 3 Security Enhancement module at Source

be unable to decode Z_2. Hence the noise of previous packet will be superimposed on next packet and degrade the quality of services at Eve's end.

- Eve receive packet $\hat{X}_1$ correctly he will use it to decode Z_2 to extract $\hat{X}_2$. However if Bob is unable receives packet $\tilde{X}_1$ correctly so it will request ARQ and Alice will send the packet again until he gets correct packet. So he able to decode Y_2 to extract the required information $\tilde{X}_2$. The retransmission does not leak more information to Eve
- The retransmission are made only when requested by Bob hence does not leak more information to Eve.

The ith packet received by Bob and Eve after decoding using the security decoder are given by expression 5 and 6 respectively.

$$\tilde{X}_i = X_i \oplus W_i \oplus W_{i-1} \tag{5}$$

$$\hat{X}_i = X_i \oplus U_i \oplus U_{i-1} \tag{6}$$

It could be observed that W_{i-1} and U_{i-1} became the extra noise i.e. noise of previous packet is aggregated to next packet. The probabilistic model for the security capacity of this technique is presented in Section 4.2.

4.2 Analyses for noise aggregation

According to the principle of noise aggregation method presented in Section 4.1, Eve can decode the message correctly iff he receives all the packets by following retransmissions of a packet between Alice and Bob. Otherwise he cannot decode the message encoded by noise aggregation method. The loss of one packet tend towards the loss of next packet, as it serves as a key to decode next packet. To derive an exact expression for the error probability of Bob and Eve, let us consider Bob requests for successive retransmissions against a single packet transmitted from Alice. Let α and β are the error probabilities of Bob and Eve's channel

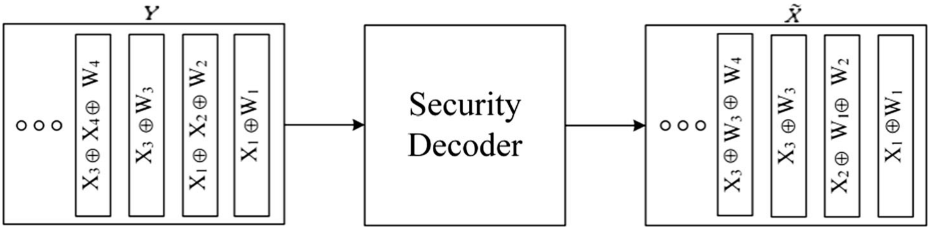

Fig. 4 Example of Decoding Module at Bob

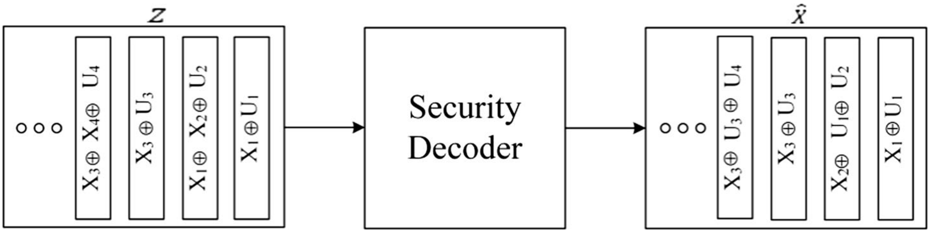

Fig. 5 Example of Decoding Module at Eve

respectively. Let n be the total number of transmissions of a packet i.e. the transmission of a packet from Alice and subsequent requests of retransmission by Bob. Where n is a random variable, depends on the channel quality of Bob. Assuming each transmission of packet is independent of previous one. The probability that Bob finally receives the packet without any error can be given by independent and identically distributed Bernoulli trials [7] as

$$\Pr(B_c) = (1-\alpha)\alpha^n \tag{7}$$

The probability that Eve can receive the correct packet in n independent retransmissions be $1-\beta^n$. However, the probability that Eve can get the correct packet following the number of total transmissions before Bob gets the correct packet is given by total probability theorem [4] as

$$\begin{aligned}\Pr(E_C) &= \sum_{n=1}^{\infty}\Pr\left(E_C\middle|B_c\right)\Pr B_c\\ \Pr(E_C) &= \sum_{n=1}^{\infty}(1-\beta^n)(1-\alpha)\alpha^{n-1}\\ \Pr(E_C) &= \frac{1-\beta}{1-\alpha\beta}\end{aligned} \tag{8}$$

Now let us find the probability of receiving packet correctly, encoded by physical layer security mechanism based on noise aggregation method. Assuming that the probability of receiving a correct packet is independent of each other. Let's assume the error probabilities of the ith and *(i-1)*th packets are $\in$ and $\overline{\in}$ respectively. The probability of receiving erroneous packets due to physical layer security mechanism as a function of error probability of packets is given as

$$\Pr\left(\tilde{U}_i = 1\right) = \Pr(U_i = 1, U_{i-1} = 0) + \Pr(U_i = 0, U_{i-1} = 1) \tag{9}$$

$$\Pr\left(\tilde{U}_i = 1\right) = \Pr(U_i = 1)\Pr(U_{i-1} = 0) + \Pr(U_i = 0)\Pr(U_{i-1} = 1) \tag{10}$$

$$\Pr\left(\tilde{U}_i = 1\right) = \epsilon\left(1-\overline{\epsilon}\right) + \overline{\epsilon}(1-\epsilon) = \epsilon + \overline{\epsilon} - 2\epsilon\overline{\epsilon} = \hat{\epsilon} \tag{11}$$

As in case of binary modulation schemes, error rate is less than 0.5 i.e. $0 < \epsilon, \overline{\epsilon} < \frac{1}{2}$, hence the probability of decoding even packet erroneously $\left(\Pr\left(\tilde{U}_i\right) = \hat{\epsilon} > \epsilon,\ \overline{\epsilon}\right)$ is enhanced. Now let us find the probability that Eve cannot decode both packets correctly encoded using noise aggregation scheme. Assuming that Eve cannot decode the ith packet $\hat{\beta}$, also each packet received by Eve is independent of all other. Finally the probability that Eve cannot extract information by decoding via noise aggregation method can be given as

$$\Pr(E_E) = 1 - \left(\frac{1-\beta}{1-\alpha\beta}\right)\left(\frac{1-\hat{\beta}}{1-\alpha\hat{\beta}}\right) \tag{12}$$

Hence the probability that Eve cannot be able to decode the packets correctly is greater than Bob, unless the error probability of wiretap channel is much smaller than main channel i.e. $\beta \ll \alpha$.

4.3 Application of noise aggregation approach to immersive systems

In immersive systems to transmit 3D video content, the high Quality of Experience (QoE) is required besides intensive bandwidth. To transmit multimedia contents over wireless networks, the data generated by multimedia sources have to be efficiently compressed. Compression standards like H.264/AVC, MPEG2 and MPEG4 normally aim to achieve high compression ratio. The compressed video content bit-streams are very sensitive to channel errors. Even a single bit error in the compressed bit-streams may lead to loss in synchronization at the receiver's side, which could significantly degrade the quality of the reconstructed multimedia content [15].

In this paper we have exploited error sensitive nature of compressed video content by using noise aggregation approach while keeping in mind the delay sensitive nature of video content. Eavesdropper experiences degradation in the Quality of Experience (QoE) for video content due to the fact that noise aggregation in encoded message packets increases the error probability. Also it is not required to share a secret key to decode the message packets at receiver's end; because previous packet serves as a key for the next encoded packet. Therefore the method proposed in this paper does not increase the overhead to wireless communication systems unlike other cipher techniques. Our proposed noise aggregation method effectively enhance the security for video communication by limiting the amount of information eavesdropped by the unauthorized user at bit level.

5 Performance evaluation

The QoE for video content is evaluated against the subjective and objective measurements. The subjective measurements are assumed to be the most precise measures as it based on human experience. While objective measurements are based on statistical methods. In this paper, we have presented both subjective and objective measurements to evaluate the video quality. Objective measurements are based on Peak-Signal-to-Noise-Ratio (PSNR), a most commonly used video quality metric to observe the quality of 3D video.

We assume a frequency-flat block-fading additive white Gaussian noise channel for the system model presented in Section 3. Performance of the system is evaluated against the bit error rate (BER) of legitimate user and passive eavesdropper. The decoding at legitimate user Bob's end is trivial, Bob can request for retransmission of lost packets until he gets the correct packet or the limit for maximum ARQ is reached. Figure 6 presents the BER of Eve on three dimensional axes as a function of SNR of main and wiretap channel. Error rate is presented on logarithmic scale along z-axis. It could be observed that when the SNR of main channel is lower than a certain limit, the probability of receiving missing packets for Eve is high; therefore he could enjoy a low BER. However if the SNR of main channel is above the

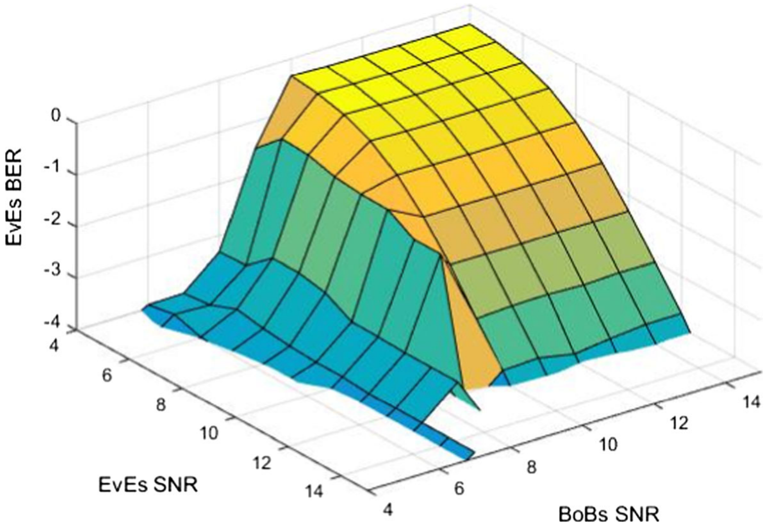

Fig. 6 Bit Error Rate of Eve as a function of Bob and Eve's channel SNR (dB)

certain limit error rate of Eve increases. If the average SNR of the main channel is better than wiretap channel there is significant degradation of services for eavesdropper.

Figure 7 shows the frame error rate (FER) gain of Bob and Eve against the same channel conditions i.e. both experience the same average SNR. FER is presented on the logarithmic scale along y-axis vs. the average SNR of wireless channel along x-axis. There is approximately 1dB SNR gain between Bob and Eve for the same error rate, represents that Bob experienced better quality as compared to Eve. However this difference tends to minimize after a certain average SNR limit when the packet lost is significantly lower for Eve.

In order to justify that our proposed scheme can provide security for video communication, system model presented in Fig. 2 is simulated for video content transmission. Both main and

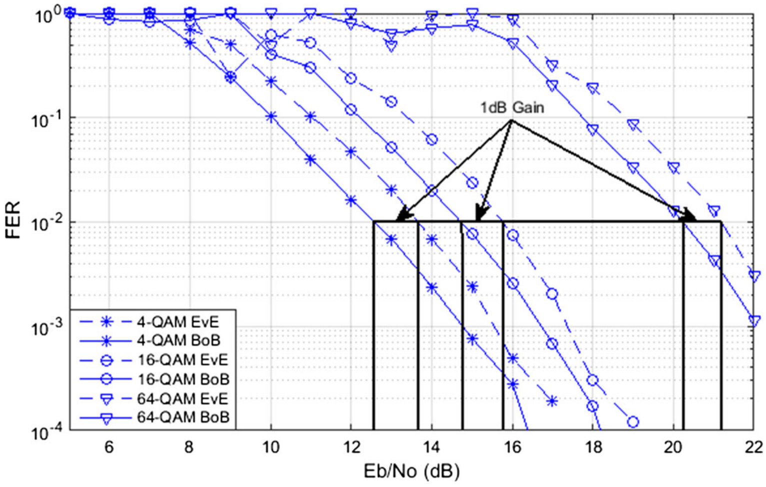

Fig. 7 FER of legitimate user Bob and passive eavesdropper Eve for same channel conditions

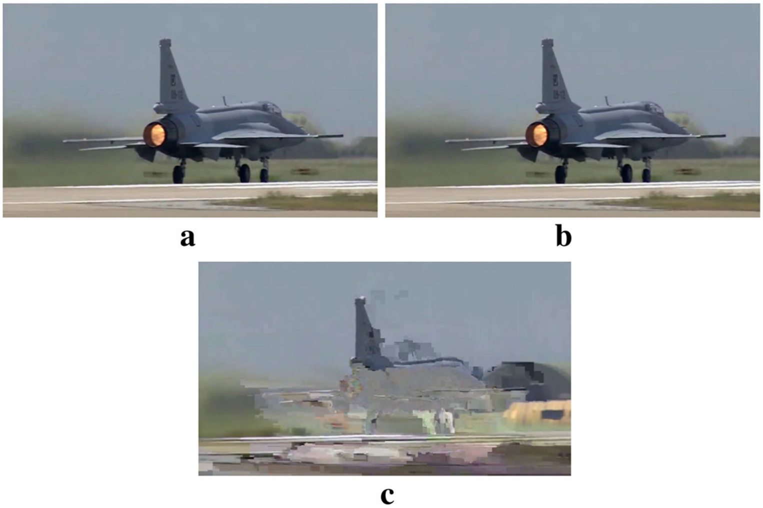

Fig. 8 Comparison of the video frames **a**) original transmitted frame, **b**) received by legitimate user Bob and **c**) passive eavesdropper Eve

wiretap channel are assumed to be identical and independent of each other. In Fig. 8, it could be observed that Bob experienced better quality as compared to Eve. A frame from the original video, frame received by legitimate user and passive eavesdropper is presented. While an objective comparison for the quality of video content received by legitimate user Bob and passive eavesdropper Eve as a function of Peak Signal to Noise Ratio (PSNR) is presented in Table 1. PSNR values of the video content received by Bob and Eve for different channel conditions, i) when the average SNR of both channels is same, ii) when average SNR of Bob's channel is better than Eve's channel and iii) when average SNR of Bob's channel is worse than Eve's channel.

6 Conclusion

In this paper, we have presented a noise aggregation method for secure video communication over wireless channel. Noise aggregation method is a physical-layer security approach based on the wiretap channel model with no assumptions on channel quality of eavesdropper. Our proposed physical-layer security scheme provides security against the passive eavesdropper above the SC of main channel. Comprehensive simulation results are provided which prove

Table 1 Peak Signal to Noise Ratio (PSNR) vs. channel SNR of legitimate user Bob and eavesdropper Eve

SNR (dB)	PSNR legitimate user Bob (dB)	PSNR eavesdropper eve (dB)
Bob = 14, Eve = 14	126.4	77
Bob = 14, Eve = 12	125.2	50.5
Bob = 14, Eve = 16	126.1	94

the effectiveness of our proposed schemes. This scheme can be implemented by adding security encoder in applications that utilize Transmission Control Protocol (TCP) for video transmission/streaming. We believe that this noise aggregation approach will reveal the potential of physical-layer security to secure wireless communications systems.

For future work, we plan to extend our scheme to achieve perfect secrecy against the passive eavesdropper. The scope of this scheme can be extended to provide absolute video security including security against the active eavesdropper and copyright violations.

Acknowledgments The research work reported in this paper is supported by the National Natural Science Foundation of China under the grant No. 61431011, the Specialized Research Fund for the Doctoral Program of Higher Education under the grant no. 20110201120014, Open Research Fund of National Mobile Communications Research Laboratory under the grant no. 2012D04 and the Fundamental Research Funds for the Central Universities

References

1. Amitav M, Fakoorian SAA, Jing H, Lee Swindlehurst A (2014) Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun Surv Tutorials 16:1550–1573
2. Baldi M, Bianchi M, Chiaraluce F (2011) Increasing physical layer security through scrambled codes and ARQ. IEEE Int Conf Commun Workshops (ICC) 1–5
3. Barros J, Rodrigues MRD (2006) Secrecy capacity of wireless channels. IEEE Int Symp Inf Theory 356–360
4. Bar-Shalom Y, Li R, Kirubarajan T (2001) Estimation with applications to tracking and navigation. Wiley, New York
5. Bloch M, Barros J, Rodrigues MRD (2008) Wireless information-theoretic security. IEEE Trans Inf Theory 2515–2534
6. Boho A, Van Wallendael G, Dooms A, De Cock J, Braeckman G, Schelkens P, Preneel B, Van de Walle R (2013) End-To-end security for video distribution: the combination of encryption, watermarking and video adaptation. IEEE Signal Process Mag 30:97–107
7. Harrison WK, Almeida J, Klinc D, McLaughlin SW, Barros J (2010) Stopping sets for physical-layer security. IEEE Inf Theory Workshop (ITW) 1–5
8. Harrison WK, Boyce P (2014) Parity modifications and stopping sets in high-rate codes for physical-layer security. IEEE Conf Commun Netw Secur (CNS) 115–120
9. Maurer U (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39:733–742
10. Naef M, Staadt O, Gross M (2005) Multimedia integration into the blue-c API. Elsevier, vol. Comuter and Graphics 29, pp. 3–15
11. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715
12. Shiu Y-S, Chang SY, Huang SC-H, Chen H-H (2011) Physical layer security in wireless networks: a tutorial. IEEE Wirel Commun 18:66–74
13. Vernam GS (1926) Cipher printing telegraph system for secret wire and radio telegraphic communication. Trans Am Inst Electr Eng 45:285–301
14. Voloshynovskiy S, Koval O, Deguillaume F, Pun T (2008) Multimedia security: open problems and solutions. Aspects of Network and Information Security, IOS Press, vol. 17, pp. 143–151
15. Wang Y, Wang H, Wang C (2013) Graph-based authentication design for color-depth-based 3D video transmission over wireless networks. IEEE Trans Netw Serv Manag 245–255
16. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54:1355–1387
17. Yang Z, Wu W, Nahrstedt K, Kurillo G, Bajcsy R (2009) Enabling multi-party 3D tele-immersive environments with ViewCast. ACM Trans Multimedia Comput Commun Appl
18. Zhou L, Wu D, Zheng B, Guizani M (2014) Joint physical-application layer security for wireless multimedia delivery. IEEE Commun Mag 66–72

Mukhtar Hussain received BS degree in Electrical (Telecommunication) Engineering from COMSATS Institute of Information Technology, Lahore, Pakistan in 2013. Mr. Hussain is now with COMSATS Institute of Information Technology, Lahore, Pakistan, working as a Research Associate. He is also now pursing the Master of Science Degree in Xi'an Jiaotong University, China. His research focuses include wireless communication and networking with emphasis on video security via physical-layer techniques and multimedia QoS assurance for 5G Networks.

Qinghe Du received his B.S. and M.S. degrees both from Xi'an Jiaotong University, China, and his Ph.D. degree from Texas A&M University, USA. He is currently an Associate Professor of Information and Communications Engineering Department, Xi'an Jiaotong University, China. His research interests include mobile wireless communications and networking with emphasis on cross-layer design, 5G networks, mobile multicast, statistical QoS provisioning, and cognitive radio networks, and physical-layer techniques. He has published over 90 technical papers. He received the Best Paper Award in IEEE GLOBECOM 2007. He is serving as an Associate Editor of IEEE COMMUNICATIONS LETTERS.

Li Sun received his B.S., M.S., and Ph.D. degrees all from Xi'an Jiaotong University, China. He is currently an Assitant Professor of Information and Communications Engineering Department, Xi'an Jiaotong University, China. His research interests include mobile wireless communications and networking with emphasis on relay, physical-layer security, and 5G networks. He has published over 50 technical papers. He received the Best Paper Award in IEEE GLOBECOM 2007. He is serving as an Editor of KSII Transactions on Internet and Information Systems.

Pinyi Ren received his B.S., M.S. and Ph.D. degrees all from Xi'an Jiaotong University, China. He is currently a Professor and the Department Head of Information and Communications Engineering Department, Xi'an Jiaotong University. His current research interests include cognitive radio networks, MIMO systems, game theory in wireless communications, wireless relay, routing, signal detection, etc. Prof. Ren has published more than 100 technical papers in peer-reviewed international Journals and conferences. He received the Best Letter Award of IEICE Communications Society in 2010. He has 18 authorized Chinese Patents and the Copyrights for 3 Software Programs. Prof. Ren serves as an Editor for the Journal of Xi'an Jiaotong University, the Lead Guest Editor for the Special Issue of Mobile Networks and Applications on "Distributed Wireless Networks and Services", and the Lead Guest Editor for the Special Issues of Journal of Electronics on "Cognitive Radio". He served as the General Chair of ICST WICON 2011 and Symposium Co-Chair of WCSP 2014. He has served ss the Technical Program Committee members for many conferences including IEEE GLOBECOM, IEEE ICC, IEEE VTC, IEEE ICCC, etc. Prof. Ren is a Senior Member of Chinese Institute of Communications, a Member of IEICE, and a Member of IEEE.