# Security Enhancement for IoT Video Streaming via Joint Network Coding and Retransmission Design

Pengxiang Qin[1,2], Pinyi Ren[1,2](✉), Qinghe Du[1,2], and Li Sun[1,2]

[1] School of Electronic and Information Engineering, Xi'an Jiaotong University,
28 West Xianning Road, Xian 710049, Shaanxi, China
qinpengxiang@stu.xjtu.edu.cn, pyren@mail.xjtu.edu.cn

[2] Shaanxi Smart Networks and Ubiquitous Access Research Center,
28 West Xianning Road, Xian 710049, Shaanxi, China

**Abstract.** Relying on the development of technology, the communication Internet has included not only the traditional Internet but also the Internet of Things (IoT). However, a large number of IoT applications especially video streaming confront kinds of security challenges. In this paper, we consider the requirements of video streaming such as sufficient reliability, security, real-time and investigate the trade-off among them. Based on the above consideration, a security scheme for IoT video streaming via joint network coding and retransmission is proposed. The scheme relates the independent packets and ensures a part of them to be reliably transmitted by ARQ protocol simultaneously. Moreover, the secrecy performance is evaluated by probability analysis. And simulation results which make comparison with the noise aggregation scheme further corroborate the performance in our scheme.

**Keywords:** IoT video streaming · Physical layer security · Network coding · ARQ protocol

## 1 Introduction

With development and popularization of Internet of Things technology, various applications of IoT have been implemented gradually, which impels people's life more convenient and efficient [1]. In the meantime, wireless communication has been the main key technology of IoT. However, openness, an inherent nature of wireless transmission environment, makes information in IoT applications exposed to security threats [2]. For few years, traditional encryption schemes [3] based on computational complexity are confronting a huge challenge due to

The research reported in this paper was supported in part by: Key Research and Development Program of Shannxi Province under Grant 2017ZDXM-GY-012, National Natural Science Foundation of China under Grant No. 61431011, Fundamental Research Funds for the Central Universities.

B. Li et al. (Eds.): IoTaaS 2018, LNICST 271, pp. 40–47, 2019.
https://doi.org/10.1007/978-3-030-14657-3_4

higher performance chips. Depend on Shannon information theory, physical layer security utilizes the physical nature of wireless channel to degrade the wiretap channel quality to enhance security with no relying on computational complexity. On contrast of traditional encryption schemes, physical layer technologies are more applicable to enhance security for IoT.

Automatic repeat request scheme has been widely implemented in secure communications to provide high reliability. That's suitable and feasible for secure transmission of IoT streaming data because the round-trip time (RTT) is relatively small compared to the allowed delay most of time. The issue of quality of service (QoS) for real-time traffic over a wireless channel deploying ARQ error control was studied in [4]. A novel and simple loss impact estimation based ARQ algorithm was proposed in [5]. Furthermore, a number of schemes based on ARQ protocol has been studied. For instance, an information-theoretic perspective of retransmission protocols for reliable packet communication under a secrecy constraint was considered in [6]. A packet coding scheme in [7] relates all the packets and used ARQ to achieve secure file delivery. Noise aggregation scheme [8] used ARQ to degrade the wiretap channel quality in immersive system. In addition, the average secrecy rate in noise aggregation scheme has been analyzed in [9]. Though the noise aggregation scheme meets real-time transmission but can't well ensure the security due to its encoding method. Our basic idea is to relate the original independent packets and use ARQ protocol to achieve sufficiently reliable, secrecy and real-time transmission. Considering other problems ARQ protocol brings, the balance between reliability and security would be made up in IoT video streaming. On the basis of the above thoughts, a security scheme via joint network coding and retransmission is proposed in this paper.

The rest of this paper is organized as follows: Sect. 2 presents the system model in wireless physical layer security transmission. Section 3 describes the proposed scheme and analyzes the performance. Section 4 evaluates the average performance by probabilistic analysis. Finally, the paper concludes with Sect. 5.

## 2 System Model

The system model is illustrated in Fig. 1. A legitimate transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve) constitute this model. On contrast of wire-tap model [10], there is an extra noiseless feedback link between Alice and Bob to ensure Bob's reliable transmission. In this case, Bob expects to receive the confidential information without being overheard by Eve. Nevertheless, Eve always exists in the network and is hard to be eliminated. When Alice is transmitting a packet to Bob over the legitimate channel, Eve also is passively receiving the data over the wiretap channel. Different from Eve, Bob can request the retransmission of lost or wrong packets via feedback link. In other words, if Bob has correctly received a packet, Alice starts to transmit the next one whether Eve successfully received the previous packet or not.

In this paper, we assume that both the legitimate channel and the wiretap channel undergo independent quasi-static fading, where the channel gains remain

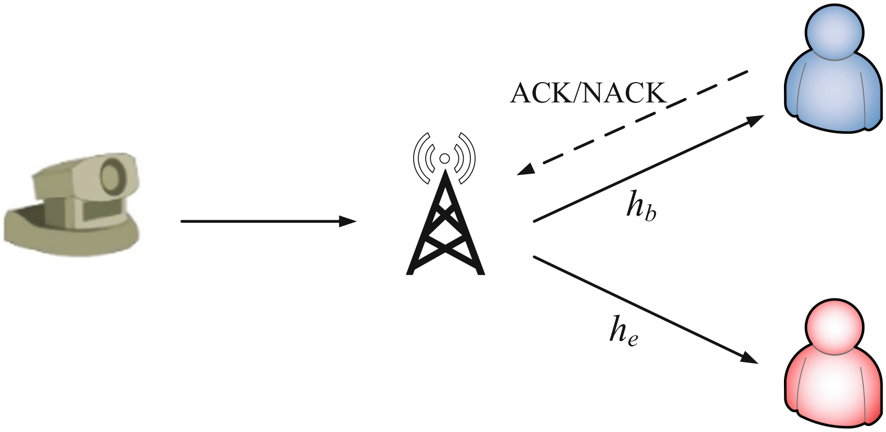

**Fig. 1.** System model for secrecy transmission.

constant in a packet slot and change independently at random from one slot to another. A transmitting and receiving antenna is equipped at Alice and Bob. However, Eve just has one receiving antenna as a passive node. When Alice transmits a symbol $x$, the received signals at Bob and Eve are

$$y_{b,i} = h_{b,i}x + n_{b,i} \tag{1}$$

and

$$y_{e,i} = h_{e,i}x + n_{e,i} \tag{2}$$

respectively. The legitimate channel gain is denoted as $h_{b,i}$ in slot $i$ and the wiretap channel gain is $h_{e,i}$. The symbols $n_{b,i}$ and $n_{e,i}$ represent additive white noises with variances $\sigma_b^2$ and $\sigma_e^2$, respectively.

When receiving the signals, both Bob and Eve try to recover the confidential information. Assuming Eve has known the principle of the encoding method deployed at Alice, Eve and Bob recover information by the corresponding decoding method. Besides, both Eve and Bob use the optimal decision rules. The proposed scheme is discussed in detail in Sect. 3.

## 3 Joint Network Coding and Retransmission Design

### 3.1 Principles of the Scheme

Although ARQ protocol ensures the reliability of data, it also brings some problems. In common or bad transmission environment, Bob would request retransmission in several times, which means the same packet would be transmitted by Alice until Bob correctly receives this packet. As a passive node, Eve would also receive these packets which contain the same confidential information. It would bring Eve more available information to correctly receive this packet. In other words, Eve would have more probability to recover information in this case in contrast to not deploying ARQ protocol. In this way, it obviously violates the principle of secrecy transmission if no other measures are implemented. Additionally, the delay which retransmission in overmany times brings may not meet the real-time requirement. Based on the above consideration, we propose a security scheme for IoT video streaming, where Eve can't decode the current packet which is related to other previous packets ensured by ARQ protocol.

We assume that Alice needs to transmit plenty of packets $S_1, S_2, ..., S_N$ and each packet contains the same length binary data. The original packets are encoded to $X_1, X_2, ..., X_N$ one by one. In our scheme, Alice performs bitwise exclusive-or (XOR) operation on packets. If Alice starts to transmit $S_i$ where $i$ is odd and greater than 1, the corresponding packet $X_i$ is given by

$$X_i = S_{i-2} \oplus S_i. \tag{3}$$

Specifically, $X_1$ is equal to $S_1$ when $i = 1$. Furthermore, $X_{i+1}$ is given by

$$X_{i+1} = S_i \oplus S_{i+1}. \tag{4}$$

Assuming $Y_1, Y_2, ..., Y_N$ denote the received packets at receiver after demodulation, Bob or Eve try to recover the packets by the decoding method inverse to the encoding method. It's easy to describe the corresponding decoding method. We assume $\tilde{S}_1, \tilde{S}_2, ..., \tilde{S}_N$ denotes decoded packets and $i$ is odd. Then, $\tilde{S}_i$ is given by

$$\tilde{S}_i = Y_1 \oplus Y_3 \oplus \cdots \oplus Y_{i-2} \oplus Y_i. \tag{5}$$

Furthermore, the even packet $\tilde{S}_{i+1}$ is given by

$$\tilde{S}_{i+1} = Y_1 \oplus Y_3 \oplus \cdots \oplus Y_{i-2} \oplus Y_i \oplus Y_{i+1}. \tag{6}$$

It's noted that the odd packets are transmitted by ARQ protocol to ensure the reliability but the even not. In fact, each received packet is influenced by inherent noise and random fading for Bob or Eve. Nevertheless, Bob can request retransmission for the odd packets via feedback link in contrast to Eve. According to the decoding method and ARQ protocol deployed on the odd packets for Bob, every odd original packet can be correctly recovered. And whether Bob can recover an even original packet only depends on the quality of transmission environment including noise and fading. On the contrary, Eve can correctly recover an odd original packet relying on all the previous odd packets. Moreover, an even packet can be correctly recovered also depends on the previous odd packets. Considering the different and random position in each packet in error and the huge bits a packet contains in reality, any odd packet in error greatly influences information recovering for Eve. The probabilistic model for the security capacity of the scheme is presented in Sect. 3.2.

### 3.2 Performance Analysis

According to the principle of the scheme in Sect. 3.1, Eve can correctly recover the information under many difficult conditions so that there exists the probability that the original packet or the original bit error occurs. Assuming $\alpha$ and

$\beta$ are the packet error probabilities of the legitimate channel and the wiretap channel, respectively. Then, the probability that Eve can get the correct packet before Bob gets the correct packet is given in [8] by

$$P_{\text{p,odd}}(\mathrm{C}_{\text{eve}}) = \frac{1-\beta}{1-\alpha\beta}. \tag{7}$$

Because just one bit error results in a packet error and the feature of XOR, it's more essential to analyze the bit error probability (BER) in our scheme. For Bob, the BER in the odd original packets is zero due to ARQ protocol. Assuming both the legitimate channel and the wiretap channel are independent identically distributed (idd) Rayleigh fading, the receiving BER with binary phase shift keying (BPSK), which is equal to the BER in the even original packets at Bob, is given in [11] by

$$P_{\text{b,odd}}(\mathrm{E}_{\text{bob}}) = \frac{1}{2}\left(1-\sqrt{\frac{\bar{\gamma_b}}{1+\bar{\gamma_b}}}\right), \tag{8}$$

where $\bar{\gamma_b}$ is the average signal-to-noise ratio (SNR) at Bob. Then, we consider maximal ratio combining (MRC) reception diversity method is equipped at Eve when Eve can't get the correct packet before Bob gets the correct packet. In this case, the BER in the odd packets is given in [11] by

$$P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}}) = \left(\frac{1-\mathit{\Gamma}_e}{2}\right)^M \sum_{m=0}^{M-1} \binom{M-1+m}{m} \left(\frac{1+\mathit{\Gamma}_e}{2}\right)^m. \tag{9}$$

In Eq. (9), $M$ is the number of the odd packet's transmission and $\mathit{\Gamma}_e = \sqrt{\bar{\gamma_e}/(1+\bar{\gamma_e})}$, where $\bar{\gamma_e}$ is the average SNR at Eve. In the even slots, the BER at Eve can also be expressed in Eq. (8) except the difference of $\bar{\gamma}$. Assuming receiving the odd packet in slot $2n-1$ and one packet just contains one bit, Eve can correctly recover the $(2n-1)$th original packet if an even number of error occurs in the previous $n$ packets due to the feature of XOR. On the contrary, Eve can't correctly recover it if an odd number of error occurs. According to the specific feature of XOR, it's easy to prove

(a) When $0 < P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}}) < 0.5$, the BER at Eve is always less than 0.5. when $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ is constant, the BER approaches 0.5 from 0 gradually as $n$ increases. When $n$ is constant, the BER also approaches 0.5 gradually as $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ increases.

(b) When $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}}) = 0.5$, the BER at Eve is always 0.5.

(c) When $0.5 < P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}}) < 1$, it should be divided to two parts to discuss. When $n$ is odd, the BER at Eve is always greater than 0.5. When $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ is constant, the BER approaches 0.5 from 1 gradually as $n$ increases. When $n$ is constant, the BER approaches 1 from 0 as $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ increases. On the contrary, When $n$ is even, the BER at Eve is always less than 0.5. When $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ is constant, the BER approaches 0.5 from 0 as $n$ increases. When $n$ is constant, the BER approaches 0 from 1 as $P_{\text{b,odd,MRC}}(\mathrm{E}_{\text{eve}})$ increases.

According to the above conclusion, the BER would approach 0.5 if the sufficient packets are related. Although the BER is less than 0.5 in some cases, we can't promise these harsh conditions in reality. Hence, an efficient and effective way is increasing the related packets resulting in the probability of correctly decoding one bit for Eve is almost only 0.5. In the meantime, one packet contains so many bits in reality, which leads that error occurs in different positions in one packet. Considering the above analysis, our scheme can ensure secrecy transmission obviously.

Besides error probability analysis, the delay as another considerable part should be considered. Firstly according to the encoding method, each encoded packets to be transmitted relates to the previous original or current packet, which means Alice can transmit signals in real time. Secondly, Eve or Bob can decode the current packet with the previous and current received packets, which meets the real-time condition at receivers. The feasibility of real-time proves our scheme is suitable for IoT video streaming. The only odd packets are ensured by ARQ protocol but the even ones not, which reduces us nearly half of delay in whole transmit. There are many other measures can be implemented to achieve various objectives during the extra time which the scheme brings.

## 4 Simulation Results

To evaluate the performance of the proposed scheme, simulation results are present in this section. Note that the secrecy performance is related to the size of bits which one packet contains. In this paper, we consider one packet contains 512 bits. In addition, maximum likelihood hard decision decoding is implemented at Bob and Eve. Furthermore, maximal rate combination is deployed at Eve when not correctly received the packet before Bob gets the correct packet in one packet slot. Then, Rayleigh fading and additive white Gaussian noise (AWGN) also been considered.

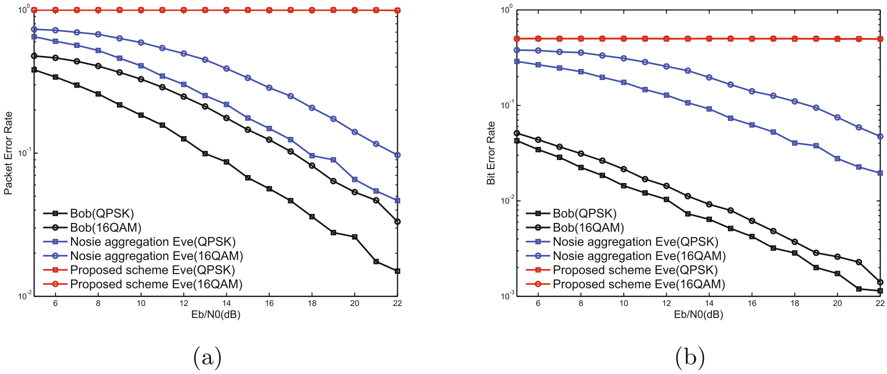

**Fig. 2.** (a) PER of Bob and Eve for same channel conditions in two schemes. (b) BER of Bob and Eve for same channel conditions in two schemes.

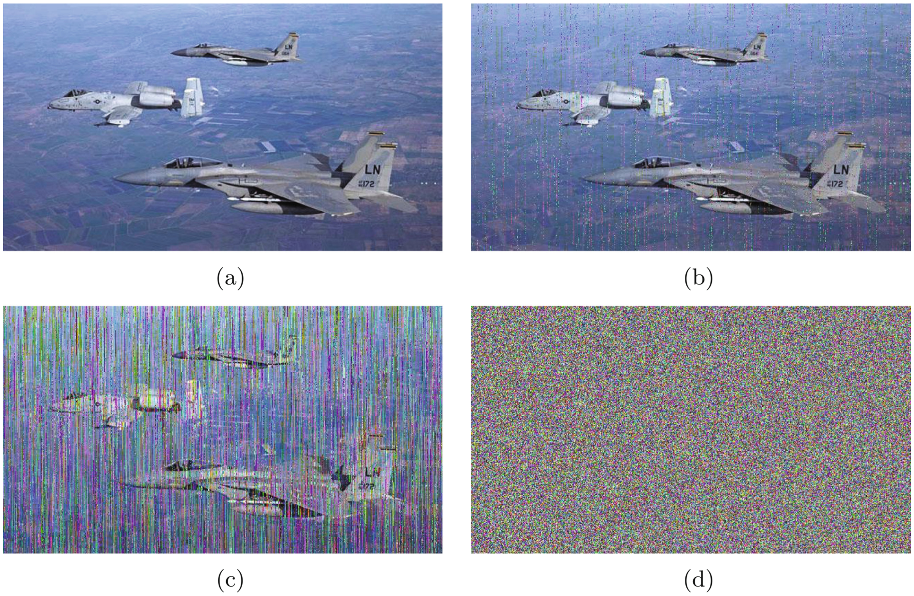
(a)
(b)
(c)
(d)

**Fig. 3.** (a) Screenshots of original video. (b) Video screenshot decoded by Bob. (c) Video screenshot decoded by Eve in the noise aggregation scheme. (d) Video screenshot decoded by Eve in the proposed scheme.

Figure 2(a) shows the packet error rate (PER) of two schemes for Bob and Eve in QPSK and 16QAM modulation. It should be noted that the PER in the noise aggregation scheme in [8]is equal to the proposed scheme because of the same proportion of reliable transmission packets due to ARQ protocol. For Eve in the proposed scheme, we can see PER is still zero that means Eve can't correctly decode any confidential packet. Comparing to Noise Aggregation, it greatly improves the security of confidential information. In order to prove the effectiveness more convincingly, the BER is also analyzed. Figure 2(b) shows the BER of two schemes for Bob and Eve. There is an error floor where the BER is 0.5 for Eve in the proposed scheme but the other not. Besides, the BER is always higher in the proposed scheme. That also proves the scheme has higher secrecy performance.

To further verify the effectiveness of the proposed scheme, we compare the received video screenshot in different ways. From Fig. 3(b) at Bob, we can clearly recognize the content although there is some noise on the screenshot. Comparing to the screenshot via noise aggregation in Fig. 3(c) at Eve, the screenshot in Fig. 3(d) at Eve is illegible and inundated with noise in the proposed scheme. Intuitively, our scheme also can preferably ensure the security.

## 5 Conclusions

The paper proposes a security scheme for IoT video streaming, which employs joint network coding and retransmission. Based on wire-tap model with a feedback link, the scheme degrades the wiretap channel quality. Furthermore, it also provides sufficient reliability, security, real-time and low delay simultaneously. Then, we theoretically study the performance. Besides, the comparison between the noise aggregation scheme and the proposed scheme has been given. And simulation results show that the proposed scheme has more high secrecy performance than the other and still supports real-time secure transmission and prove the effectiveness of our proposed scheme.

## References

1. Khan, R., et al.: Future internet: the internet of things architecture, possible applications and key challenges. In: International Conference on Frontiers of Information Technology, pp. 257–260. IEEE (2013)
2. Xu, Q., et al.: Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access **4**, 2840–2853 (2016)
3. Keoh, S.L., Kumar, S.S., Tschofenig, H.: Securing the internet of things: a standardization perspective. IEEE IoT J. **1**(3), 265–275 (2014)
4. Quan, Z., Chung, J.M.: Analysis of packet loss for real-time traffic in wireless mobile networks with ARQ feedback. In: 2004 IEEE Wireless Communications and Networking Conference, WCNC 2004, vol. 1. IEEE (2004)
5. Ge, X., Liu, H., Wang, G.: A novel loss-impact-estimating based ARQ for wireless real-time H.264/SVC video stream. In: International Conference on Electronics Information and Emergency Communication, pp. 131–135. IEEE (2015)
6. Tang, X., et al.: On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. IEEE Trans. Inf. Theory **55**(4), 1575–1591 (2009)
7. He, H., Ren, P.: Secure ARQ protocol for wireless communications: performance analysis and packet coding design. IEEE Trans. Veh. Technol. **PP**(99), 1 (2018)
8. Hussain, M., et al.: Security enhancement for video transmission via noise aggregation in immersive systems. Multimed. Tools Appl. **75**(9), 5345–5357 (2016)
9. Xu, Q., et al.: On achievable secrecy rate by noise aggregation over wireless fading channels. In: IEEE International Conference on Communications, pp. 1–6. IEEE (2016)
10. Wyner, A.D.: The wire-tap channel. Bell Labs Tech. J. **54**(8), 1355–1387 (2014)
11. Stuber, G.L.: Principles of Mobile Communication. Kluwer Academic Publishers, Dordrecht (2001). 98C106