Multimedia Tools and Applications (2024) 83:7583–7607
https://doi.org/10.1007/s11042-023-15957-y

Resource allocation functionality with cluster aggregation (RAFCA) for secure HST video transmission

Elias Yaacoub[1]

Received: 24 January 2022 / Revised: 24 April 2023 / Accepted: 29 May 2023 /
Published online: 9 June 2023

Abstract
This paper presents an approach for resource allocation functionality with cluster aggregation (RAFCA) for securely transmitting surveillance videos in high-speed trains (HSTs). Each train wagon is assumed to be equipped with a surveillance camera, along with a mobile relay (MR) that communicates with the cellular base station (BS) on one hand and with the indoor devices inside the train on the other. The RAFCA approach is based on a permutation process of the video frames across multiple MRs, such that parts of the video captured by the camera of a given wagon are transmitted by the MRs of all other wagons. The probability of detection by an eavesdropper is calculated in this paper and shown to be negligible, which leads to the preservation of the privacy of the passengers. Moreover, the proposed approach is shown to have no or little impact on the quality of experience (QoE) of the transmitted videos, thus preventing quality degradation.

Keywords Video transmission · Quality of service · Quality of experience · Physical layer security · Railroad networks

1 Introduction

Nowadays, high speed trains (HSTs) are expected to provide ubiquitous connectivity to their passengers. They should be equipped with the state-of-the-art 5G and beyond communication capability, for both addressing the passengers' needs and carrying network management and control information in real-time [16, 7].

In fact, passengers would expect to enjoy voice, video, and data services; hence, streaming high quality videos on-board HSTs should be performed with high quality of service (QoE). Moreover, the network should support internet of things (IoT) traffic, which sometimes is mission-critical (especially for safety purposes), from the various sensors and actuators on-board the train and along the rail track [32].

Although historically it was suggested in the literature that two networks, one for passenger traffic and another for mission-critical data, should coexist for HST networks, it is

✉ Elias Yaacoub
elias.yaacoub@gmail.com

[1] Computer Science and Engineering (CSE) Department, Qatar University, Doha, Qatar

now accepted that a single 5G (and beyond) network can handle both types of traffic [11, 9].

The trend for increased mobility of passengers and goods is expected to continue in the future. Therefore, the security and safety of passengers should be of utmost importance. The use of surveillance cameras on-board HSTs can help in this direction. Such cameras would record the situation in each wagon, and the surveillance video can be transmitted to a central command center for analysis and processing. In case any suspicious activity is detected, the train can be stopped at the nearest station for the intervention of security personnel.

The transmission of these surveillance videos in real-time not only poses communications challenges on the network, but also leads to security challenges concerning the privacy of the passengers [32]. Any malicious eavesdropper capturing the transmissions can try to identify the passengers and their locations within the train, which goes counter to the purpose of installing a surveillance system for passenger protection. Encrypting the video streams might solve the problem; however, it might lead to significant delays due to encrypting several video streams, transmitting them, and then decrypting them before displaying them in the control center.

The work in this paper aims to address this problem by proposing a lightweight physical layer security approach for scrambling the video frames before transmitting them. The proposed approach assumes the existence of multiple mobile relays (MRs), at least one on top of each train wagon, which is a scenario studied extensively in the recent literature, e.g., [8, 29, 3]. Each MR can be considered as a cluster head relaying the traffic from its wagon to the base stations (BSs) along the rail track in the uplink, and from the BS to the devices in the downlink. Since these MRs can be connected to the internal network of the train, a specific MR does not have to exclusively transmit the surveillance video of its own wagon. Instead, the traffic can be aggregated and scrambled in a way to increase security and maintain the privacy of passengers. Thus, an approach based on Resource Allocation Functionality with Cluster Aggregation (RAFCA) is proposed in this paper and shown to achieve high security levels without impacting the QoE of the video traffic, compared to the traditional scenario. According to the author's knowledge, physical layer security techniques for securing real-time transmission of surveillance videos in HSTs are not well investigated in the literature.

The rest of this paper is organized as follows. A review of the related literature is presented in Sect. 2. Section 3 presents the system model. The proposed approach is described in Sect. 4. The simulation results are presented and discussed in Sect. 5. Finally, in Sect. 6, conclusions are drawn and directions for future research are outlined.

2 Literature review

With the increase in the number of train passengers, real-time surveillance becomes more important to maintain safety and security. In fact, incidents can happen inside trains, e.g., see [15] for a recent example from Japan, which has led the authorities to consider deploying CCTV surveillance cameras in all trains, as their absence made it more difficult to law enforcement authorities to capture the assailant [15]. Several CCTV surveillance solutions for HSTs are available in the market, e.g., [18, 26]. They support communication with operators inside the train, and with a control center outside the train. Transmission of video surveillance data to outside the train can occur either continuously [18], or only when an artificial intelligence (AI) system inside the train detects an incident, i.e., the video is stored locally and shared on-board the train with train operators, but transmitted to the control center in case an incident is suspected that might require external intervention [26].

Securing these transmissions is important to maintain the safety and privacy of passengers, although the security process should not affect the real-time nature of these transmissions. Although remote video monitoring over IP networks was investigated long ago [13], few papers in the literature have addressed this problem for railroad networks. In a recent survey [17] on security in railway transportation, the papers mentioned as working on HST video transmission were more concerned with transmission of entertainment video [28], but not surveillance videos. Naturally, securing entertainment videos is less critical, and could afford a certain (reasonable) delay, compared to real-time surveillance videos.

Therefore, despite the unique challenges related to the HST scenario, we consider further the papers in the literature investigating the security of surveillance videos over wireless channels in general, without necessarily being related to HST transmissions. Most of the existing works in the literature investigate video encryption techniques [2, 4, 10, 19, 22]. Due to the computational overhead and time consumption required, they attempt to find encryption methods that can be implemented faster.

In [4], the authors propose a joint approach for video encryption and transmission, with the aim of achieving good cryptographic security while reducing the impact of bit error propagation due to losses of encrypted bits, when transmitted over wireless channels. In [2], surveillance videos stored on the cloud are considered, and a complete security framework based on encryption, authentication, and key management, is proposed and investigated. In [10], the authors propose an improvement to the advanced encryption standard (AES), and name it Improved AES (IAES). They prove that IAES reduces encryption time while still providing a strong key space. In [19], fountain codes are proposed for enhancing enterprise multimedia security. The purpose is to secure video frames transmitted wirelessly to edge servers. The authors use rotation constellation to increase errors at the eavesdropper, whereas the main idea is to perform detection at the legitimate receiver by having that receiver accumulate enough packets before the eavesdropper. This relies on having redundant coding packets and thus increasing the overall amount of data to be transmitted. The authors of [22] investigate the security of a video transmission system for training surgeons remotely. They consider the joint use of AES and RSA encryption with video steganography techniques.

Other works also use steganography [24, 25] to secure transmissions, where the video to be protected is “hidden” inside another video. This can be done with or without encryption. In fact, steganography itself provides security through hiding, whereas encryption in this case adds an extra level of security. In a practical HST surveillance scenario, this would require the generation of “cover” videos to hide the surveillance “secret” videos, which adds more delay and increases the data required for transmission, notwithstanding the time needed to extract the secret video from the cover video at the receiver.

The use of various encryption techniques does not preclude the fact that the encryption process is still computationally intensive. In addition, several solutions are not directly compatible with existing video compression standards, such as MPEG4 and H.264/H.265. Moreover, the vulnerability of encryption to bit errors can further affect the correct decoding of the video at the receiver [4].

The proposed approach in this paper can be used separately to provide a good level of security in the absence of encryption. However, it should be noted that it could also be easily implemented in conjunction with encryption methods, as an added layer of security, when the encryption can be done fast enough to meet the requirements of real-time surveillance and be robust enough to avoid excessive error propagation during the transmission over the wireless channel, which is challenging in HSTs.

The closest work that uses physical layer security for video transmission is presented in [14]. It assumes the odd frames are transmitted unencrypted, whereas the even frames are XORed with the odd frames (each even frame is XORed with the previous odd frame) before transmission. When an odd frame and the subsequent encrypted even frame are received correctly, the receiver (whether legitimate or a malicious eavesdropper) can detect both frames. However, when a frame is lost by the legitimate receiver (due to transmission over a wireless channel), a request for retransmission is made by the receiver over a noise free feedback channel. This channel cannot be used by the eavesdropper if he loses a frame. Thus, the legitimate receiver can recover losses, unlike the eavesdropper. In scenarios where no separate feedback channel exists, as is the case in the scenario investigated in this paper, this method cannot be implemented.

Although in [4] the contribution is about proposing a new encryption method, the authors briefly mention that permutation or scrambling can be used as a fast solution in case the complexity of encryption and the ensuing delays cannot be tolerated due to the nature of the application, as is the case in the HST video surveillance scenario. The authors of [4] mention that this comes at the cost of reduced security. However, the assumption in the references that mention permutation is that the packets of frames of the same video sequence are permuted between each other. In the proposed approach of this paper, we are permuting the frames of various video sequences across multiple MRs, i.e., the video frames transmitted by a given MR come each from a different MR. This adds an additional degree of freedom and significantly improves security. In Sect. 4, the security level of this approach will be assessed and compared to the case of having permutation over a single sequence only.

The proposed approach in this paper does not require any separate feedback channel, does not need any changes to the existing video coding standards, and does need the overhead of encryption or steganography. Thus, it is not affected by error propagation due to the loss of encrypted bits. In addition, it can benefit from traditional existing error concealment techniques to partially address the loss of video data during transmission over wireless channels. As noted previously, this does not prevent it from being used as a supplementary approach adding an extra level of security, in addition to encryption and/or steganography methods, whenever these methods are made suitable for the real-time video surveillance in HSTs.

Thus, the main contributions of this paper are:

- Proposing an approach named Resource Allocation Functionality with Cluster Aggregation (RAFCA), for achieving security of real-time video surveillance data in HSTs, using frame permutations across the surveillance videos of multiple MRs in the train,
- Proving that RAFCA achieves high levels of security in face of eavesdropping, such that the reconstruction of the transmitted videos is virtually impossible,

- Showing that on the long run, RAFCA does not lead to degradation of QoE of the transmitted videos, and
- Performing extensive simulations to analyze the impact of RAFCA on QoE in various scenarios and various types of transmitted videos.

3 System model

The system model is shown in Fig. 1. MRs placed on top of train wagons communicate with the BS through their outdoor antennas, and communicate with the passengers as indoor access points (APs) through their indoor antennas. Thus, they mitigate the attenuation caused by penetration loss when the signal has to reach the passenger devices without MRs. Moreover, their low mobility with respect to the passengers allows avoiding Doppler issues inside the train. As for the outdoor links, they can mitigate the Doppler effect through signal processing techniques as they are more powerful devices than passenger devices and are connected to the internal train network where powerful servers can be used for this purpose.

Figure 1 also shows surveillance cameras inside each train wagon, which in turn are also connected to the on-board network of the train. Their recorded videos are scrambled at the server before redistributing their frames over multiple MRs using the proposed secure

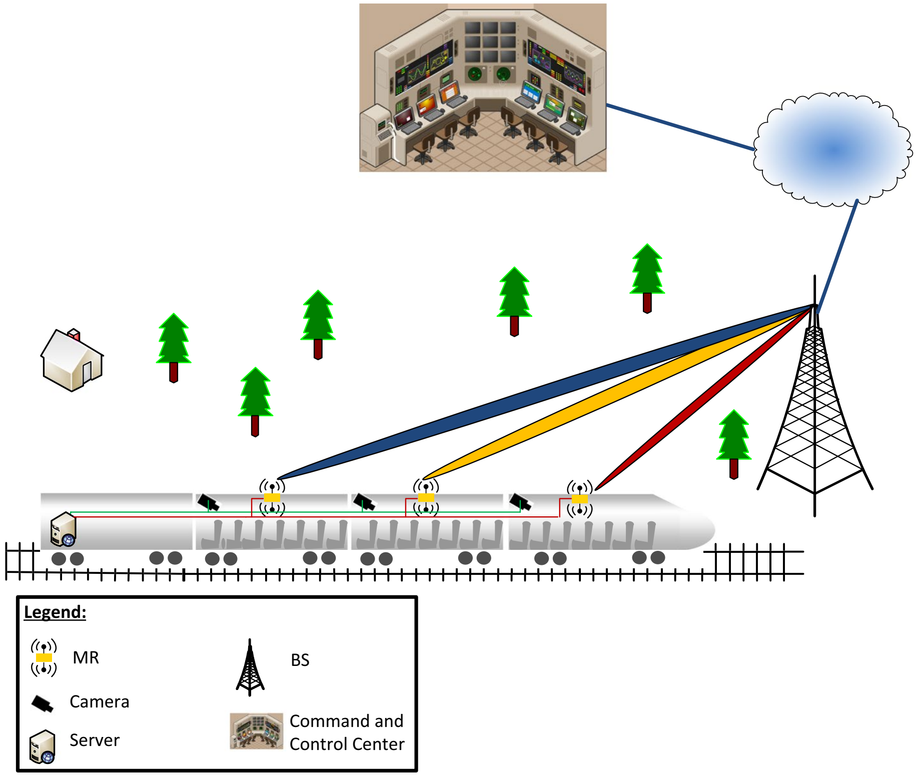


Fig. 1 System Model

approach described in Sect. 4. From there, they are transmitted to the BS and routed to the central command center where they can be analyzed and processed. In addition, appropriate action can be taken in case of an emergency.

The encoding/compression at the server (discussed in Sect. 3.2) reduces the size of the video frames transmitted, which allows for easier transmission of the surveillance data over the wireless links due to the reduced data rate. The proposed approach, since it is based on scrambling the frames before transmission, does not add overhead to the transmitted data. This allows securing the transmitted information without increasing the required data rate. Resource allocation over the wireless channel is performed as described in Sect. 3.3. In order to concentrate the scope of this paper on assessing the proposed permutation-based physical layer security method, we resort to relatively "traditional" resource allocation methods without using very advanced techniques. Hence, the color-coded links in Fig. 1 between the BS and MRs in our scenario simply correspond to different frequency subcarriers (more details in Sect. 3.3). More advanced features could include the use of massive multiple input multiple output (MIMO) or adaptive beamforming antenna techniques, in order to further increase the data rate and reduce losses over the wireless channel. These enhancements can be performed as future work in a subsequent study, as the scope of this paper is to evaluate the proposed security technique and its potential impact on QoE, without boosting its performance with other non-security related enhancements.

3.1 Channel model

We use the channel model implemented in [31], which is adapted from the D1 channel model in the WINNER II specifications [6]. It consists of (i) pathloss, calculated based on the distance between the BS and the MRs, (ii) lognormal shadowing or slow fading, caused by large scale obstacles, and (iii) fast small-scale fading.

Correlation between consecutive shadowing samples is considered based on the approach of [27, 33], whereas fast fading samples are considered independent [31].

3.2 Video encoding and QoE

In this paper, we consider that the videos are encoded using MPEG4 or H.264/H.265 format. We consider that a video sequence is subdivided into groups of pictures (GOPs), where each GOP consists of an I-frame and several subsequent P-frames. B-frames can also be considered without affecting the proposed approach. However, in this paper, we investigate GOPs with I-frames and

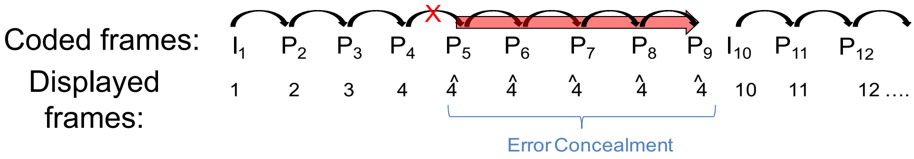

Coded frames:
I_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 I_{10} P_{11} P_{12}
Displayed frames:
1 2 3 4 $\hat{4}$ $\hat{4}$ $\hat{4}$ $\hat{4}$ $\hat{4}$ 10 11 12 ....
Error Concealment

Fig. 2 Video Encoding and Error Concealment

P-frames only. Due to the interdependency between video frames, when a frame is lost, all the subsequent frames in the GOP cannot be displayed and are considered lost, until the correct reception of the next I-frame. The previous frame concealment method (freeze frame) is adopted: in case a frame is lost, the latest correctly received frame is displayed until the next I-frame is received. An illustrative example is shown in Fig. 2 with a GOP of 10 frames, where the fifth frame (fourth P-frame) is lost.

3.2.1 Video QoE

The QoE metric used in this paper is:

$$Q_{m,k} = Q_{max}\left(1 - \frac{1}{1 + e^{b_1\left(PSNR_{m,k} - b_2\right)}}\right) \tag{1}$$

In (1), $PSNR_{m,k}$ is the peak signal to noise ratio of frame k recorded in MR m, whereas b_1 and b_2 are parameters dependent on the video characteristics. The QoE metric (1) is based on the metric used in [30] as a special case of the metric derived in [21]. Although b_1 and b_2 are hard to determine in real-time, it should be noted that the proposed approach described in Sect. 4, and the resource allocation approach described in Sect. 3.3, are independent from these parameters (In the simulations of Sect. 5, we use video sequences for which these parameters are known in the literature). Thus, in this paper, we use the metric (1) for the purpose of analyzing the QoE performance of the proposed approach, although the proposed approach can run independently of these parameters, and can be analyzed using other QoE metrics or using the PSNR itself. The maximum QoE is set to $Q_{max} = 100$ in order to conveniently measure the QoE on a scale between 0–100.

3.2.2 Network QoE

Equation (1) corresponds to the QoE metric at a given device, e.g., an MR in the scenario of Fig. 1. More specifically, we consider the average performance over all frames in a GOP at a given MR as:

$Q_m = \sum_{k=1}^{K} Q_{m,k}/K$. However, to assess the performance of the proposed approach, we need to evaluate QoE across all MRs. Therefore, we use the "network" QoE metrics derived in [33] and listed in Table 1.

The first metric is the sum QoE and corresponds to adding the QoE values of all MRs. Although this gives an indication of the overall performance in the

Table 1 Network QoE Metrics Summarizing Performance across all MRs

Metric Definition	Metric Description
$Q_{oE}^{(\mathrm{sum})} = \sum_{m=1}^{M} Q_m$	Sum QoE
$Q_{oE}^{(\mathrm{GM})} = \left(\prod_{m=1}^{M} Q_m\right)^{1/M}$	Geometric Mean QoE
$Q_{oE}^{(\mathrm{min})} = \mathrm{min}_m Q_m$	Minimum (Min) QoE

network, the worst-case MRs could be masked by the high QoE achieved by the MRs having better performance. This can be addressed by using the geometric mean QoE, which is based on the product, rather than the sum, of individual QoEs. This way, a very low QoE at one MR can affect the whole network performance. For example, if all MRs have very high QoE but only one achieves a QoE of zero, then the geometric mean QoE will be equal to zero in this case (although the sum QoE might still be good). The third QoE network metric is the minimum QoE. Although the geometric mean QoE metric is fair, the minimum QoE metric is more biased towards the performance of the worst-case MR. Thus, in case one optimizes the worst-case performance (minimum QoE), it is guaranteed that the overall performance will be enhanced, since all other MRs will perform better than the worst-case MR.

3.3 Resource allocation approach

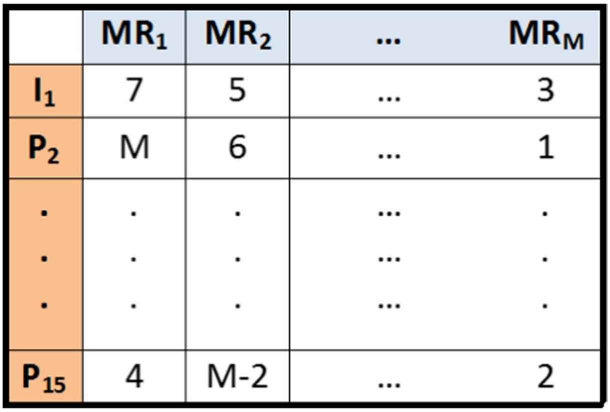
We consider an LTE advanced (LTE-A) network deployed along the rail track. Since it will be used for serving the passengers and the control/management network, unless otherwise specified, we assume that a chunk of bandwidth of 5 MHz is allocated for the sole purpose of transmitting the surveillance videos in the uplink, from the MRs to the BS. In LTE-A, the time–frequency resources are subdivided into resource blocks (RBs), such that each RB consists of 12 consecutive subcarriers using orthogonal frequency division multiple access (OFDMA). Each subcarrier has a bandwidth of 15 kHz. An RB is allocated for a minimum duration of 1 ms, which is the duration of one transmission time interval (TTI). The 5 MHz bandwidth consists of 25 RBs. Wireless channel conditions will vary over the RBs for each MR. Thus, the channel state information (CSI) of each MR is estimated at the BS based on sounding reference signals transmitted in the uplink direction by each MR [1]. The BS can then perform intelligent resource allocation in order to allocate RBs to MRs such that high data rates can be achieved.

We perform resource allocation using the algorithm proposed in [31] (Algorithm 1 in [31]). It works by finding the (RB, MR) pair that leads to the highest data rate, and allocates that RB to the MR. Then it continues with other RBs and MRs until serving all MRs, or until consuming all RBs.

4 Proposed approach

This section describes the proposed RAFCA approach for scrambling the videos and transmitting them across multiple MRs. Thus, parts of the video captured in a given train wagon are transmitted by every other wagon, in a way to make the video almost undetectable by an eavesdropper. The proposed approach is summarized in Algorithm 1, with the detailed description of the algorithm provided as follows:

- **Step 1:** Perform a permutation of the video frames between the MRs. For example, the first frame (I_1) of MR 7 can be transmitted by MR 1; the first frame (I_1)



	MR_1	MR_2	...	MR_M
I_1	7	5	...	3
P_2	M	6	...	1
. . .	. . .	. . .	... ...	. . .
P_{15}	4	M-2	...	2

Fig. 3 Illustration of the Permutation Method for Transmitting Video Frames from Multiple MRs

of MR 5 can be transmitted by MR 2, etc. The permutation varies from frame to frame within the same GOP. For example, continuing with the previous example, the second frame (P_2) of MR M can be transmitted by MR 1; the second frame (P_2) of MR 6 can be transmitted by MR 2, and so on. An example is illustrated in Fig. 3.

- **Step 2:** Each MR transmits the frames assigned to it for the duration of one GOP. These frames will actually constitute a hybrid GOP where each frame comes from a different MR; i.e., each MR i transmits K frames during the duration of one GOP, the first being an I-frame and the rest being P-frames, but each will be coming from a different MR. Thus, an eavesdropper capturing the transmissions of a given MR will not be able to reconstruct the MR's video sequence, since the transmitted frames are not dependent on each other, because each one comes from a different MR.
- **Step 3:** At the receiver, the various frames are detected. We consider a conservative approach where a frame is considered in error if at least one bit of the frame is received in error. Thus, the frames are marked as either correctly received or erroneously received.
- **Step 4:** The reverse permutation is performed at the receiver, by reversing the process done in Step 1. Hence, the frames corresponding to the GOP of each MR are sorted in order.
- **Step 5:** Perform error concealment. After placing the frames in order, the consecutive frames that are correctly received can be displayed properly. In case a frame is lost, the subsequent frames in the GOP are considered lost and the concealment approach of Fig. 2 is implemented.
- **Step 6:** Calculate the PSNR and QoE metrics.

In Algorithm 1, we denote by $\prod_k(1 : M)$ the permutation vector of frames at position k from all MRs, with its inverse being denoted by $\prod_k^{-1}(1 : M)$. Comments in the pseudocode of the Algorithm are preceded by the symbol "//".

Algorithm 1: RAFCA Approach

```
1:  for k=1:K do
2:     Generate $\prod_k (1: M)$ //permutation vector of frames at position k from all MRs m=1,..., M
3:     for  m=1:M do
          // Transmission of permuted frames: MR m transmits frame no. k generated in MR m’:
4:        MR m transmits frame  $k_{m\prime} = \prod_k (m)$
5:     end for
6:     for  m=1:M do
          // At the receiver, permuted frames are received and placed back in the initial order:
7:        Receive frame $k_m = \prod_k^{-1}(m')$  // Take the inverse permutation to put the frames in order
8:        if (frame $k_m$ is received in error) and (frame $(k_m - 1)$ is received correctly) then
             //If a frame is lost for MR m, assume all subsequent frames in the GOP are lost:
9:           set $Frame\_{}_m(j) = Frame\_{}_m(k_m - 1)$  for all j=k, ..., K // previous frame concealment
10:       end if
11:       Calculate $Q_{m,k}$ (from Equation (1))
12:    end for
13: end for
14: for m=1:M do
15:    Calculate $Q_m = \sum_{k=1}^{K} Q_{m,k}/K$
16: end for
17: Calculate Network QoE Metrics from Table 1.
```

4.1 Complexity analysis

In this section, we discuss the complexity order of Algorithm 1. The steps at Lines 3–5 and Lines 6–12 have each a complexity of order *M*. However, they are nested in the “for loop” of Lines 1–13, which is looping over the variable *k*. Thus, the complexity order of Lines 1–13 is *O*(*2MK*). Finally, the loop at Lines 14–16 is of order *M*. Hence, the total complexity is of order $2KM+M \sim O(KM)$. Thus, the algorithm has linear complexity with respect to the number of frames and the number of MRs in the train.

4.2 Probability of detection

Since the frames are randomly permuted over all MRs, for each frame there are (*M*!) possible permutations. Since all these permutations are equally probable, the probability of guessing the correct permutation for a given frame is:

$$P_{e,frame} = 1/(M!) \tag{2}$$

With the permutation of the frames at any position i in the GOP ($1 \leq i \leq K$) being independent from the permutation of the frames at any other position j, then the probability of correct detection of the whole video sequences is given by:

$$P_{e,GOP} = (1/(M!))^{\mathrm{K}} = 1/(M!)^{\mathrm{K}} \tag{3}$$

For example, having $M = 10$ MRs on the train and having $K = 15$ frames per GOP will lead to $P_{e,frame} = 2.76 \times 10^{-7}$ and $P_{e,GOP} = 4.1 \times 10^{-99}$. Thus, it is almost impossible for an eavesdropper to capture the videos in a time that is short enough to affect or disrupt the communications with the command center or to violate the privacy of the passengers. Comparing these numbers to encryption techniques, we can note that the number of possible keys in AES is 2^{128}, and in IAES [10] the authors consider 2^{256}. The probabilities of correct detections in these cases are $1/2^{128} = 2.94 \times 10^{-39}$and $1/2^{256} = 8.64 \times 10^{-78}$, respectively, which are still significantly lower than $P_{e,GOP} = 4.1 \times 10^{-99}$. Moreover, considering permutation of frames within a single GOP, i.e., within the video of a single MR (which is what is often assumed by permutation in the literature, e.g., [4]), without considering the added degree of freedom by permuting across MRs as in RAFCA, we obtain a probability of detection of $1/(K!)$. With $K = 15$ this leads to a value of 7.65×10^{-13}. This explains why

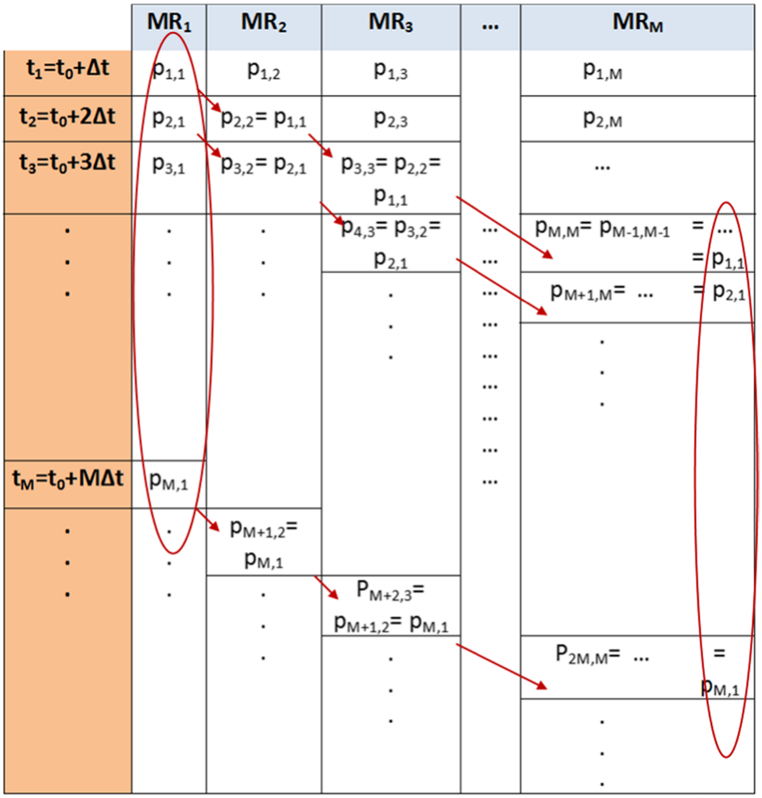


Fig. 4 Assessment of the Packet Loss Probability with the Proposed Permutation Approach

permutation is considered in the literature to have less security than encryption. However, RAFCA clearly overcomes this limitation by achieving a value of $P_{e,GOP}=4.1\times 10^{-99}$ using the realistic values in the above example ($M=10$ and $K=15$).

4.3 Evaluation of QoE degradation

In this section, we show that the implementation of the proposed approach does not asymptotically lead to an increase in packet losses, and thus does not affect the QoE of the videos, compared to the benchmark case where each MR transmits its own video frames in order.

We consider that the train starts moving at $t=t_0$. Given the speed of the train, we assume that if MR 1 transmits at time t_1 from a certain position, then MR 2 will reach that position at time $t_2=t_1+\Delta t$, MR 3 will reach it at time $t_3=t_1+2\Delta t$, and so on. Let $p_{i,j}$ denote the packet error probability at time t_i for MR j. Since the BS positions on the rail track are fixed, and since the MRs are fixed on the train, then the pathloss of MR2 at time t_2 will be the same as that of MR1 at time t_1. In addition, this will apply to a large extent to large scale fading (it is unlikely that large scale structures would have moved significantly within Δt). With the fast fading being independent identically distributed (iid), then the overall distribution of the channel gain for MR 2 at time t_2 will be similar to that of MR 1 at time t_1. Following the same reasoning for all MRs, then $p_{i+1,j+1}=p_{i,j}$. The situation is illustrated in Fig. 4.

Hence, after the last MR, MR M, has reached the position of MR 1, then $M\Delta t$ seconds would have elapsed. Considering transmissions for $N\Delta t$ seconds after that and computing the average packet loss probability will lead to:

$$\begin{aligned}
&\text{At MR 1}: P_{avg,1}=\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M}P_{t=i,1}.\\
&\text{At MR 2}: P_{avg,2}=\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M}P_{t=i,2}=\tfrac{1}{N+M}P_{1,2}+\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M-1}P_{t=i,1}.\\
&\text{At MR 3}: P_{avg,3}=\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M}P_{t=i,3}=\tfrac{1}{N+M}\left(P_{1,3}+P_{2,3}\right)+\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M-2}P_{t=i,1}.\\
&\text{At MR } M: P_{avg,M}=\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+M}P_{t=i,M}=\tfrac{1}{N+M}\left(P_{1,M}+P_{2,M}+\cdots+P_{M-1,M}\right)+\tfrac{1}{N+M}\textstyle\sum_{i=1}^{N+1}P_{t=i,1}.
\end{aligned}$$

Since

$$\frac{1}{N+M}\sum_{i=1}^{N+M}P_{t=i,1}\le P_{avg,j}\le\left(\frac{1}{N+M}\sum_{i=1}^{N}P_{t=i,1}+\frac{M}{N+M}\right) \tag{4}$$

Then,

$$\lim_{N\to\infty}\frac{1}{N+M}\sum_{i=1}^{N+M}P_{t=i,1}\le \lim_{N\to\infty}P_{avg,j}\le\lim_{N\to\infty}\left(\frac{1}{N+M}\sum_{i=1}^{N}P_{t=i,1}+\frac{M}{N+M}\right) \tag{5}$$

Hence, with the left-hand side and the right-hand side of (5) converging to the same value when N is large, we can write:

$$\lim_{N\to\infty}P_{avg,j}=\lim_{N\to\infty}P_{avg,1}=P_{avg},\forall j \tag{6}$$

The conclusion from (6) is that the average packet loss probability is almost the same from all MRs in the long run. Thus, the probability of losing a packet from the GOP of MR i without the proposed permutation approach will be the same probability, on average, when that packet is transmitted by any other MR $j\neq i$ with the proposed approach.

Table 2 Simulation parameters

Style Tag	Definition
Train Speed	250 km/h
Separation between MRs	10 m
Pathloss constant	-128.1 dB
Pathloss exponent	3.76
Shadowing standard deviation	8 dB
Uplink bandwidth	5 MHz
Number of RBs	25
TTI duration	1 ms
GOP duration	1 s
Frames per GOP	15

Consequently, the proposed approach should not lead to any QoE degradation in the long run. The simulation results of Sect. 5 will validate these conclusions.

5 Simulation results and discussion

This section presents the simulation results of implementing the RAFCA method described in Sect. 4, along with resource allocation on the BS-MR links using the approach described in Sect. 3.3. The performance is evaluated using the video QoE techniques presented in Sect. 3.2.

5.1 Simulation parameters

The simulation parameters are listed in Table 2.

In the simulations, we use the Foreman and Football video sequences, encoded in CIF format. The parameters (b1, b2) are selected as (0.34; 29.09) for the Foreman sequence, and as (0.34; 25.9) for the Football sequence (values obtained from [21]).

Fig. 5 Video Sequences used in the Simulations

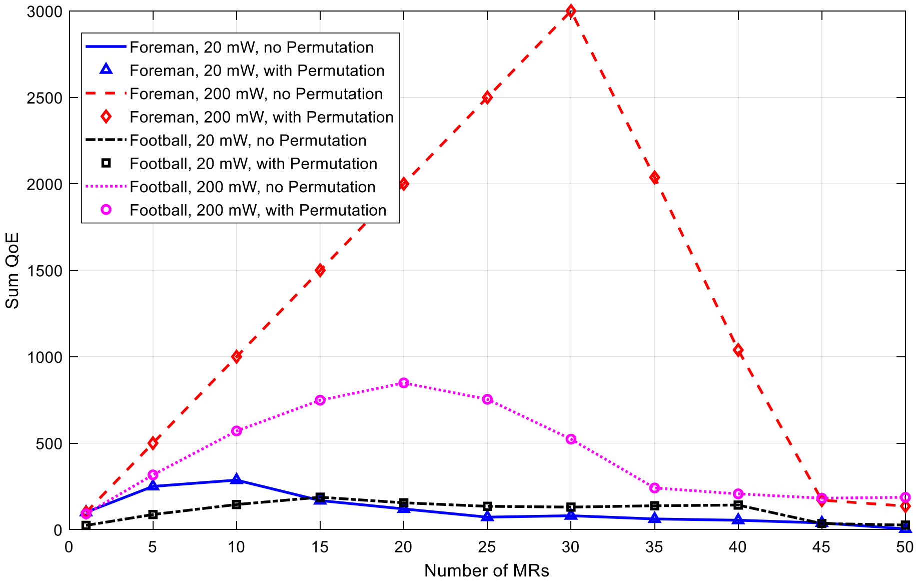


Fig. 6 Performance Evaluation of the Sum QoE Metric

Figure 5 shows a snapshot of these video sequences. The foreman sequence corresponds to a low motion scenario with limited activity, whereas the football sequence corresponds to a highly dynamic scenario with a lot of motion and activity. Thus, a video corresponding to a calm situation in a train wagon would be expected to behave similarly to the Foreman

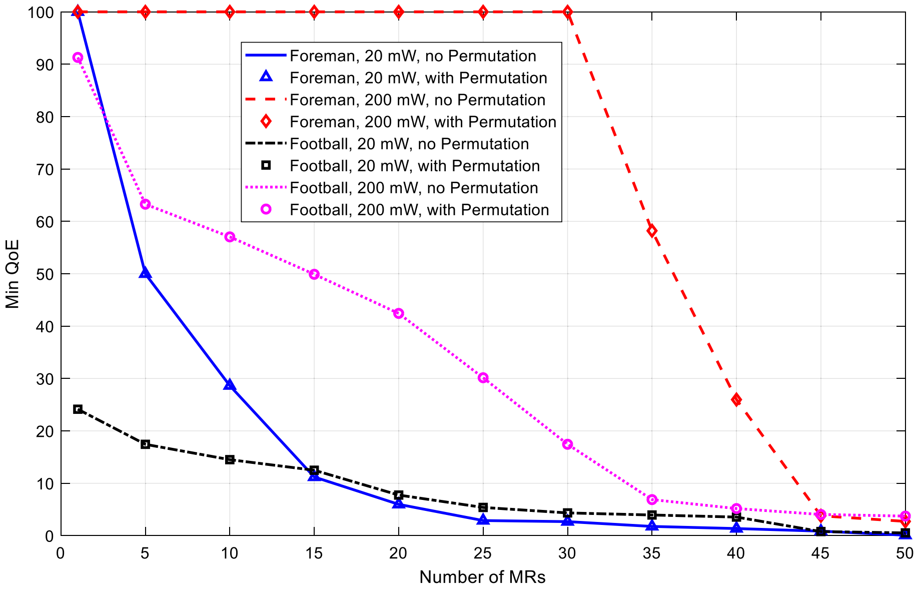


Fig. 7 Performance Evaluation of the Min QoE Metric

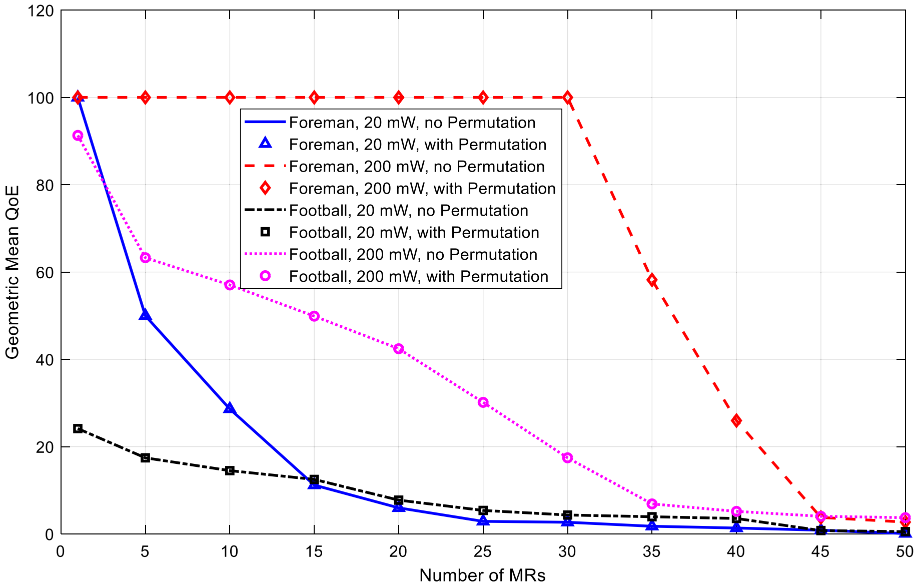


Fig. 8 Performance Evaluation of the Geometric Mean QoE Metric

sequence, whereas a video corresponding to an agitated situation would be expected to have a performance closer to the behavior of the football sequence.

5.2 Simulation results

Figures 6, 7, and 8 show the network QoE metrics listed in Table 1, sum QoE, min QoE, and Geometric mean QoE, respectively, of the received videos. The Foreman and Football video sequences are considered, and the scenario with the proposed RAFCA approach (with frame permutation) is compared to the scenario without permutation, where each MR systematically transmits the video of the camera installed in its corresponding wagon. Different values of the transmit power used at the MRs are also considered and plotted in the results. Resource allocation, for both the RAFCA approach and the traditional approach, is performed using the method described in Sect. 3.3.

Interestingly, the main and most important conclusion is that, in all scenarios of Figures 6, 7, and 8, the proposed approach leads to the same performance of the traditional approach without permutation, i.e., no noticeable performance degradation is noted. Thus, the approximations (4)-(6) illustrated in Fig. 4 are accurate.

Other (more expected) conclusions can also be drawn from the figures. First, the QoE increases with the MR transmit power, for both sequences. Second, for a given MR transmission power, the QoE of the Foreman sequence is higher than that of the Football sequence. As mentioned previously, this is because the Foreman sequence corresponds to a less dynamic scenario than Football, and thus the variations between consecutive frames are less pronounced. Consequently, the size of the compressed frames is smaller, and the effects of frame loss are less dramatic when the previous frame concealment method is used. Third, higher transmission power leads to higher QoE. Indeed, this leads to a higher signal to noise ratio (SNR) over the wireless MR-BS link, thus leading to a higher data rate

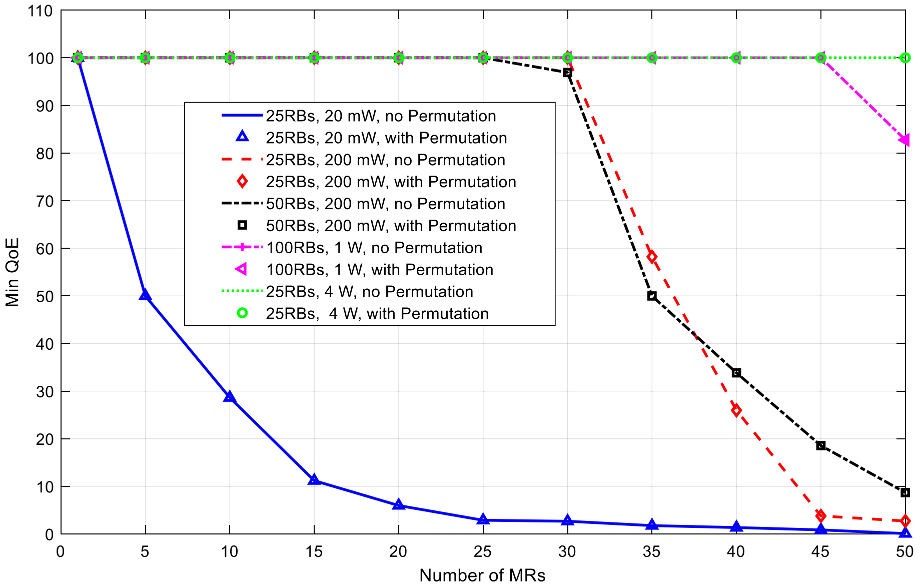


Fig. 9 Performance Evaluation of Foreman with Different Transmit Power and Number of RBs

which allows the correct transmission of more bits from the encoded videos. Fourth, the QoE performance of the Foreman is ideal for 200 mW transmit power, as long as the number of MRs is below 30. In fact, in the simulation parameters presented in Table 2, we have reserved 25 RBs, corresponding to a 5 MHz bandwidth, to be allocated for the transmission of the surveillance videos. The resource allocation approach described in Sect. 3.3 allocates one RB per MR at each TTI. Hence, with up to 25 MRs, each MR is guaranteed to have an RB allocated to it at each TTI. In addition, the resource allocation approach seems to be able to serve perfectly a slightly higher number of MRs (up to 30), before the performance starts to degrade. By "ideal" performance, we mean that all MRs achieved a 100% QoE, as evidenced by Fig. 6 (sum QoE = 3000 = 30 × 100 for 30 MRs), Fig. 7 (min QoE = 100, i.e., the worst-case MR already achieves 100% QoE), and Fig. 8 (geometric mean QoE = 100, which cannot be achieved unless the QoE of each MR is equal to 100). Due to the highly dynamic nature of the Football sequence, more RBs and/or more power is needed to achieve ideal performance. However, with the current simulation parameters, performance seems to be acceptable with 10 MRs per train and a transmit power of 200 mW per MR.

To assess the impact of increasing the power or the bandwidth on performance, we investigated different scenarios with different combinations of transmission power and available number of RBs for the Foreman sequence. The results are plotted in Fig. 9. Clearly, the increase of bandwidth or power enhances performance. For example, the use of 100 RBs allows all MRs to achieve 100% QoE. Even with 25 RBs, a 4W transmission power allows up to 50 MRs to achieve 100% QoE. The high transmit power leads to more bits to be transmitted per TTI, thus allowing the resource allocation algorithm to alternate the allocation of RBs to MRs without affecting performance, although at a given TTI not all MRs are allocated an RB.

It should be noted that the results presented in Figures 6, 7, 8 and 9 are based on using omnidirectional antennas at the MRs, as the main purpose of these simulations is to investigate whether the RAFCA approach leads to any QoE degradation compared to the traditional approach without permutation. However, the use of beamforming with adaptive antenna arrays at the outdoor part of the MRs is expected to lead to significantly better results by increasing the antenna gains, which constitutes an interesting topic for future research.

The previous figures (Figures 6, 7, 8 and 9) assumed the videos of the various MRs had a comparable level of activity. This was represented in the simulations by having all MRs transmit the Foreman sequence, or all of them transmit the Football video sequence. Thus, the results showed a perfect match between the approximation of Eqs. (4)-(6) (illustrated in Fig. 4) and the simulations. In fact, considering an example where, at a given time t, MR i is closer to the BS than MR j, then MR j will have a higher probability of losing a packet. One can analyze the following two scenarios:

- Scenario A: Assuming that at that time, in the case with permutation, frame k of MR i is transmitted by MR j, and is lost over the channel, whereas the permuted frames transmitted by MR i (including those of MR j) incur no losses. If this is the only loss in the transmissions, then, after reversing the effect of the permutation at the receiver, the video recorded at MR i will have a loss of frame k, whereas the video recorded at MR j will have no losses.
- Scenario B: In the case without permutation, assuming the same wireless channel conditions and the same positions with respect the BS, frame k of MR j will be lost by MR j itself (as there is no permutation), whereas the frames of MR i will incur no losses.

In terms of QoE metrics, when both video sequences are more or less similar (e.g., all passengers are seated in the two wagons i and j which have the same architecture and design, and where the cameras are placed in identical positions in each wagon), then the overall performance will be the same (the impact of losing a frame at position k from a GOP at MR j is not very different than losing a frame at position k from a GOP at MR i).

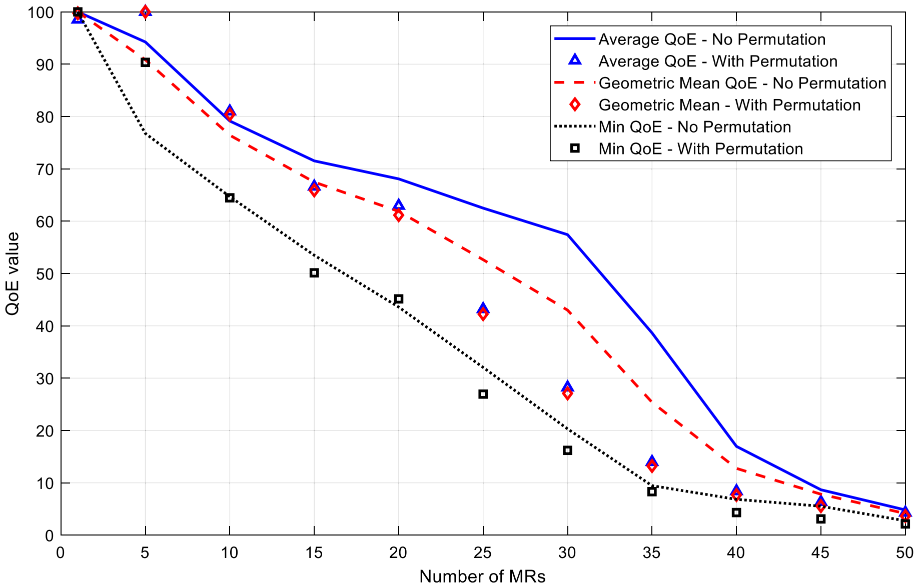


Fig. 10 Performance Evaluation with different types of video sequences transmitted by MRs: 50% Foreman and 50% Football. The results are shown for the various QoE metrics

This is confirmed by the results of Figures 6, 7, 8 and 9. In fact, if in Fig. 6 we consider the average QoE, expressed as $Q_{oE}^{(\text{avg})} = \sum_{m=1}^{M} Q_m/M = Q_{oE}^{(\text{sum})}/M$, instead of the sum QoE, the results and QoE values will be similar to those of Figs. 7 and 8 (we will the use the Average QoE in the remaining results to make the comparison easier and of the same scale to the other QoE metrics, since it is has similar behavior to the sum QoE). Indeed, when the video characteristics are similar, the results of Scenarios A and B above (with and without permutation) will be similar.

However, when the video sequences are significantly different, e.g., in the case where everything is quiet in MR j whereas an incident is occurring in MR i with a lot of activity going on, then the effect of frame loss will be different. In fact, in this case, Scenario A will lead to a more serious degradation in QoE than Scenario B. Indeed, in Scenario A, frame k lost by MR j corresponds to the dynamic video of wagon i. In Scenario B, lost frame k would correspond to the calm and stable video of wagon j. Thus, the loss in Scenario A will have a more dramatic effect on the QoE. Had the conditions in the wagons been reversed (more activity in wagon j whereas we have a calm situation in wagon i), then the reverse would happen: Scenario B (without permutation) would lead to more QoE loss.

This analysis is confirmed by the results shown in Fig. 10. In fact, in order to validate this analysis, we simulate a scenario where 50% of the MRs are randomly chosen to transmit the Foreman sequence (used to represent a scenario with little variations), and the other 50% of the MRs are transmitting the Football sequence (used to represent a dynamic scenario with many variations in the video). Then we implement the proposed approach and display the results with and without permutation.

Figure 10 shows that the min QoE metric is well-approximated by the proposed RAFCA approach presented in this paper, even in the extreme scenario considered. The permutation and non-permutation scenarios perform comparably with this metric. For

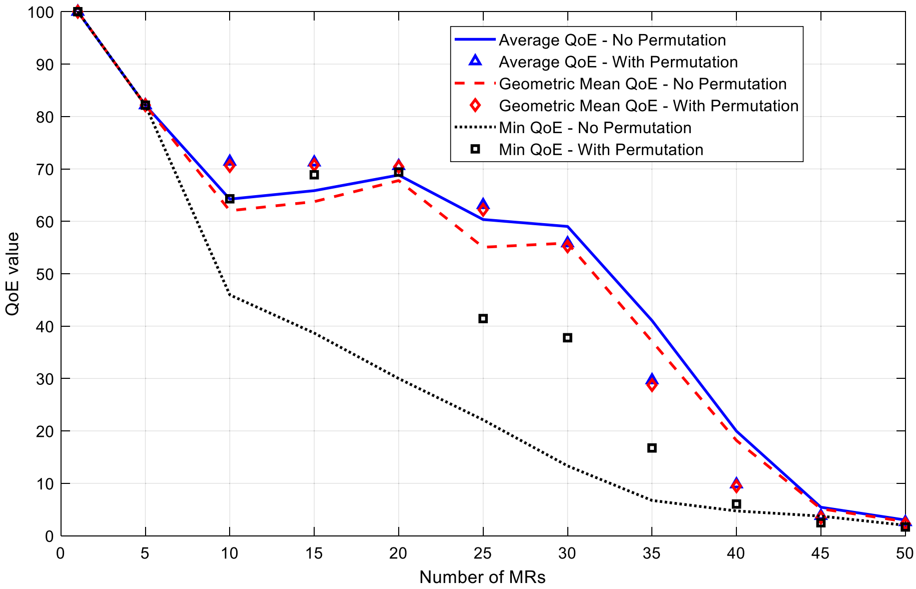


Fig. 11 Performance Evaluation with different types of video sequences transmitted by MRs: 80% Foreman and 20% Football. The results are shown for the various QoE metrics

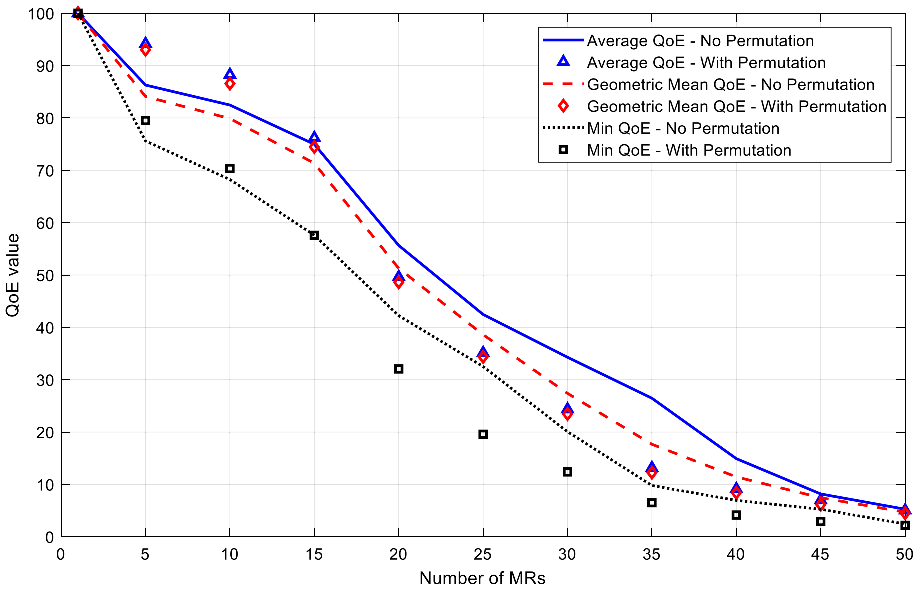


Fig. 12 Performance Evaluation with different types of video sequences transmitted by MRs: 20% Foreman and 80% Football. The results are shown for the various QoE metrics

the average and geometric mean QoE, the performance is acceptable when the number of MRs is low, thus leading to a high QoE. When the QoE degrades due to the increase in the number of transmitters (MRs), thus causing a strain on the available resources, the performance of the permutation scenario degrades by around 15% compared to the performance without permutation in the geometric mean QoE, and to significantly worse performance in terms of average QoE. This is interpreted by the fact that permutation spreads the video frames of one MR to be transmitted by all the other MRs. Thus, all MRs with good channel conditions have at least one chance to have one of their frames transmitted by an MR with worse channel conditions. Hence, when losses start occurring, they are equally likely to occur to the GOP of any MR, due to the random permutation. This leads to more losses of the dynamic frames that more severely affect QoE. In the case without permutation, the MRs having good channel conditions are less likely to incur any losses. Hence, since videos of different characteristics are transmitted per each wagon and thus the frames do not affect QoE equally, those MRs with more variations in their video and with good wireless channel conditions will lead to increasing the QoE for the non-permutation case.

This analysis is confirmed by the plots of Fig. 11, showing the results of the scenario where 80% of the MRs transmit the Foreman sequence and 20% transmit the Football sequence, and Fig. 12, showing the results of the scenario where 20% of the MRs transmit the Foreman sequence and 80% transmit the Football sequence.

In fact, Figs. 11 and 12 show that as more and more MRs are transmitting videos with similar characteristics, the average QoE approximations of Eqs. (4)-(6) become more accurate. The same applies for the case of the geometric mean QoE. Indeed, Figs. 11 and 12 show that the average QoE results of the permutation case are significantly closer to those of the non-permutation case, compared to the scenario of Fig. 10.

An interesting outcome of Figs. 10, 11 and 12 is the behavior of the Min QoE metric, which corresponds to the worst-case scenario among all MRs, and deserves a detailed analysis of its own. In Fig. 11, the case with permutation (RAFCA) achieves better Min QoE performance than the case without permutation. In fact, this figure corresponds to a scenario with few dynamic videos (20% Football) that more severely affect QoE in case of loss. The Min QoE case, unlike the average and geometric mean QoE, corresponds solely to the worst-case performance. Thus, if one MR (say MR X) transmitting the Football sequence has bad channel conditions, its losses will determine the Min QoE performance in the case without permutation. When permutation happens using RAFCA, the video frames transmitted are spread across all MRs. Thus, the frames of the worst-case MR X will be spread across all other MRs, which have better channel conditions, and thus it will suffer from fewer losses, which will increase its QoE. The losses caused by the transmissions of MR X to other MRs (because of permutation) will most of the time correspond to MRs transmitting the Foreman sequence (since they constitute 80% of all MRs) and thus will have less dramatic effect on their QoE. This diversity benefit for the worst-case MR will get reduced more and more as the number of MRs transmitting the Football sequence increases, as can be seen in Fig. 10 (50% Football) and Fig. 12 (80% Football). In fact, with more MRs transmitting the Football sequence, even if the frames of the worst-case MR X are transmitted by other MRs, MR X itself will be transmitting more and more frames of Football MRs (MRs having videos with characteristics similar to the Football sequence). Thus, the losses caused by MR X will affect these MRs, causing one of them to have the worst-case performance and achieve a lower Min QoE. The performance of Min QoE can be seen to degrade from Fig. 11 (20% Football) to Fig. 10 (50% Football), and on to Fig. 12 (80% Football), as the number of MRs having highly dynamic videos increases.

Nevertheless, it should be noted that this Min QoE behavior is a nice side effect of the permutations of RAFCA. In fact, in a typical HST scenario, incidents would be rare to happen, with most scenarios being similar to our case of 100% Foreman (in Figs. 6, 7, 8 and 9). Whenever an incident happens, it will mostly be in one or few MRs, thus causing more activity in these MRs only. This is more similar to the case of Fig. 11 (80% Foreman corresponding to MRs with little activity or trouble, and 20% Football corresponding to MRs with higher activity and agitation), where the permutation leads to enhancing the worst-case performance! Thus, in case an incident occurs even in a wagon with an MR having bad wireless channel conditions, the proposed RAFCA approach has the desirable and unexpected side effect of boosting the quality of that MR's video, while protecting the privacy of passengers.

5.3 Discussion, limitations, and potential solutions

In this section, we discuss some practical limitations of the above approach and propose solutions for each of them. The first issue is the permutation vector used, as both the server inside the train and at the command center need to know the permutation vector, so that the permutation can be correctly reversed. This can be done by having a similar pseudorandom number generator at both the train and command center, with the condition of initializing it with the same seed. Hence, it will produce the same sequence of numbers. The challenge becomes how to share the seed and change it periodically. Different solutions exist for this scenario: (i) The seed could be set offline (e.g., each day before the trains start their trips), (ii) it could be exchanged over a separate secure channel (e.g., through free space optics when the train is stationary at the station), or it could be sent in encrypted form over the same wireless channel used for transmitting the videos. The encryption key could be obtained using physical layer techniques: For example, the channel state information (CSI) of each RB on the BS-MR links could be used to generate a key. Since the CSI can be known at the BS and train, the key can be generated and used without having to be wirelessly transmitted.

The second issue is that the proposed approach is a physical layer security technique based on permuting the transmitted frames, without resorting to traditional encryption methods. It should be noted that a P or B frame cannot be decoded without the previous I and P frames. By shuffling the order of frames, the process is made very hard on the eavesdropper to correctly decode a GOP. However, the I-frames, if unencrypted, can still be decoded, although the eavesdropper cannot immediately guess to which wagon a detected I-frame corresponds. This issue can be addressed by using the proposed approach in conjunction with other more traditional encryption techniques, thus providing an additional layer of security. However, this does not serve the purpose of fast transmission and reception/display of the surveillance videos without incurring encryption/decryption delays. This limitation can be addressed by noting that a P or B frame cannot be decoded without the previous I and P frames. Thus, an eavesdropper cannot detect the frames in a GOP if it cannot correctly decode the I-frame. Consequently, only the I-frames need to be encrypted. This can be done using lightweight encryption techniques. For example, a stream cipher can be used where each bit of the I-frame is simply XOR-ed with a bit from the cipher stream. For decryption, the same stream has to be generated at the receiver. This requires that the key used for the stream cipher generator be the same at the train and at the command center. Again, this can be solved by determining the key using physical layer techniques based on CSI over the OFDMA subcarriers, as described in the previous paragraph.

Another possible solution is to use cipher block-chaining (CBC) to encrypt the I-frames. Although not a Blockchain, CBC could be a feasible Blockchain-like solution

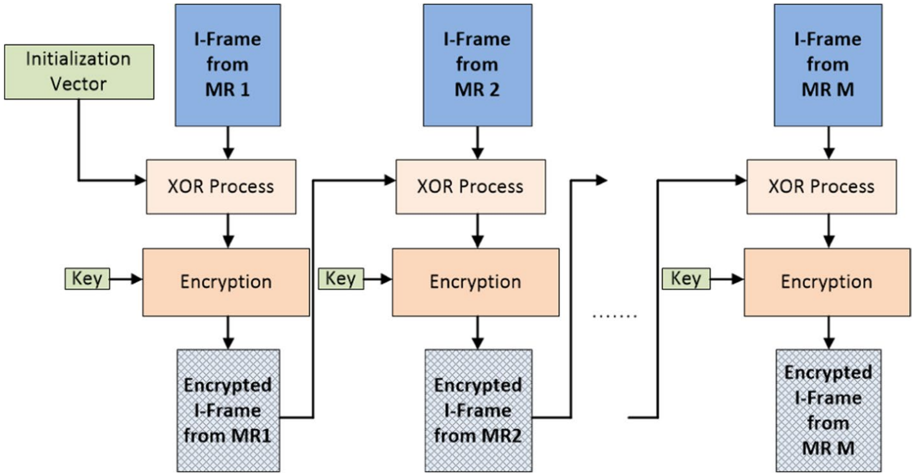


Fig. 13 CBC process for encrypting the I-frames

that could be easily implemented in conjunction with physical layer security. Blockchain has been suggested in recent years as a solution to several security problems [12-5], including IoT [12, 23], 5G [5], and video storage for forensics purposes [20]. Despite the benefits of Blockchain, several challenges seem to be underestimated by most of the literature. For example, the scalability of blockchain might be challenging when the number of transactions increases. Since the blocks are hashed and interconnected, it might take significant time for a specific transaction to be retrieved and decrypted. Having shorter chains might solve this problem but will reduce the security of the blockchain approach. Moreover, the energy required for transaction validation, similarly to bitcoin mining, is significant. The consumption and cost will increase with the number of nodes added to the blockchain. Thus, since the main objective of this paper is to use lightweight physical layer security methods, a full-fledged Blockchain is not recommended with the proposed approach. It could be used for securing stored videos from multiple trains after reception at the command center (or after storage at multiple distributed locations), where they can be retrieved when needed for forensic purposes for example, as suggested in [20]. However, for real-time wireless transmission from the train to the command center, CBC would nicely complement the proposed approach at the price of a reasonable increase in computational requirements. An example is shown in Fig. 13.

CBC is suitable for the proposed scenario because this scenario involves one train and one command center (thus the distributed condition needed for Blockchain does not apply); in addition, the chains are short, since the process of Fig. 13 is repeated with every GOP. Thus, the number of blocks in the chain is equal to the number of MRs, which is manageable. With the approach of Fig. 13, it would be virtually impossible to decode an I-frame without knowledge of the key, initialization vector, and all the previous I-frames. The key and/or initialization vector could be generated and shared using the techniques suggested in the first paragraph of this subsection. If speed of transmission is an issue, the encryption blocks in Fig. 13 could be reduced to simple XOR operations, assuming the key has the proper size in this case (otherwise, more advanced encryption algorithms, such as AES [23], can be used). It should be noted that, when the CBC approach of Fig. 13 is implemented, the encrypted I-frames at the output would then undergo the RAFCA process, where they are permuted and transmitted over the wireless channel. At the receiver, the effect of the permutation is reversed, and the frames are decrypted in sequence using the key and initialization vector. This extra decryption step would occur after Step 4 in the RAFCA process described in Sect. 4, or, equivalently, after Line 7 in Algorithm 1.

6 Conclusions and future research directions

In this paper, we presented resource allocation functionality with cluster aggregation (RAFCA) for securely transmitting surveillance videos in high-speed trains. The RAFCA approach is based on a permutation process of the video frames across multiple mobile relays (MRs), such that parts of the video captured by the camera of a given wagon are transmitted by the MRs of all other wagons. The probability of detection by an eavesdropper was calculated and shown to be negligible, which leads to the preservation of the privacy of the passengers. Moreover, the QoE of the transmitted videos was investigated, and it was shown that the RAFCA approach does not lead to any noticeable performance degradation, compared to the benchmark scenario where each MR transmits the video of its corresponding wagon, using the same resource allocation method, when the videos transmitted have comparable characteristics. In the case of videos with different characteristics, different scenarios were investigated and analyzed in detail. RAFCA was shown to have a desirable side effect of boosting the worst-case QoE performance in realistic scenarios, due to the diversity provided by permutations.

Future research directions consist of implementing the proposed approach with advanced techniques to enhance the performance, such as reconfigurable intelligent surfaces (RIS) that can be deployed along the track or on top of the train wagons, as a substitute of the outdoor part of the MRs. Another interesting direction for future investigation consists of implementing the proposed approach in scenarios where cluster aggregation can be performed, other than in high-speed trains. Such scenarios could include, for example, transmission of surveillance video by street cameras (in case they are transmitting wirelessly), and ambient assisted living scenarios where patients are monitored by surveillance cameras, and where there is a possibility to aggregate the streams of the cameras corresponding to neighboring patients.

Funding Open Access funding provided by the Qatar National Library. This publication was jointly supported by Qatar University and IS-Wireless—International Research Collaboration Co-Fund Grant no. IRCC-2021–003. The findings achieved herein are solely the responsibility of the author.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflicts of interests/competing interests The author declares that there are no Conflicts of Interests/Competing Interests.

References

1. 3rd Generation Partnership Project (3GPP), “3GPP TS 36.213 3GPP TSG RAN Evolved Universal Terrestrial Radio Access (EUTRA) Physical layer procedures, version 16.7.0, Release 16,” September 2021
2. Alsmirat MA, Obaidat I, Jararweh Y, Al-Saleh M (2017) A security framework for cloud-based video surveillance system. Multimedia Tools and Applications 76:22787–22802
3. Banerjee S, Rakshit SM, Hempel M, Sharif H (2018) "5G-UCDA in high speed rail with multi antenna-to-logical cell circular FIFO mapping strategy", International Conference on Computing, Networking and Communications (ICNC)
4. Chen J-R, Sun S-W, Lu C-S, Chang P-C (2009) Video JET: packet loss-resilient video joint encryption and transmission based on media-hash-embedded residual data. Multimedia Tools and Applications 44:249–278

5. Djenouri Y, Srivastava G, Belhadi A, and Lin J C-W (2021) "Intelligent blockchain management for distributed knowledge graphs in IoT 5G environments", Transactions on Emerging Telecommunications Technologies e4332 1–13, open access https://doi.org/10.1002/ett.4332
6. Döttling M, Mohr W, Osseiran A (2010) "WINNER II Channel Models," in Radio Technologies and Concepts for IMT-Advanced , Wiley,39–92 https://doi.org/10.1002/9780470748077.ch3
7. Friedner S, Womersley R, Treacher T (2018) "Connected train and customer communications: Rail and digital industry roadmap", Tech. Rep., Rail Safety and Standards Board (UK)
8. Ghazzai H, Bouchoucha T, Alsharoa A, Yaacoub E, Alouini MS, Al-Naffouri T (2017) Transmit power minimization and base station planning for high-speed trains with multiple moving relays in OFDMA systems. IEEE Trans Veh Technol 66(1):175–187
9. Gonzalez-Plaza A et al (2017) "5G communications in high speed and metropolitan railways", 11th European Conference on Antennas and Propagation (EUCAP)
10. Hafsa A, Fradi M, Sghaier A, Malek J, Machhout M (2022) Real-time video security system using chaos- improved advanced encryption standard (IAES). Multimedia Tools and Applications 81:2275–2298
11. Hasegawa F et al (2018) High-speed train communications standardization in 3GPP 5G NR. IEEE Communications Standards Magazine 2(1):44–52
12. Hayat RF, Aurangzeb S, Aleem M, Srivastava G, and Lin JC-W (2022) "ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments", IEEE Trans Eng Manag, early access, p.p. 1–14, publsihed online https://doi.org/10.1109/TEM.2022.3170519
13. Hu SC, Wang F (2003) Remote Video Monitoring Over the WWW. Multimedia Tools and Applications 21:173–195
14. Hussain M, Du Q, Sun L, Ren P (2016) Security enhancement for video transmission via noise aggregation in immersive systems. Multimedia Tools and Applications 75:5345–5357
15. Isobe M, "Surveillance cameras in train cars could soon be the norm", The Asahi Shimbun, news article, Dec. 3 2021; online; url: https://www.asahi.com/ajw/articles/14494491 [Accessed: January 13, 2023]
16. Kim J et al (2018) A comprehensive study on mmWave-based mobile hotspot network system for high-speed train communications. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2018.2865700(earlyaccess),August
17. López-Aguilar P, Batista E, Martínez-Ballesté A, Solanas A (2022) Information Security and Privacy in Railway Transportation: A Systematic Review. Sensors (MDPI) 22:7698. https://doi.org/10.3390/s22207698
18. MOXA, "Tailored Onboard CCTV Solutions", tech. rep., online; url: https://www.moxa.com/en/spotlight/integrated-solutions/rail/onboard-cctv/index [Accessed: January 13, 2023]
19. Nie H, Jiang X, Tang W, Zhang S, Dou W (2020) Data security over wireless transmission for enterprise multimedia security with fountain codes. Multimedia Tools and Applications 79:10781–10803
20. Ottakath N, Al-Maadeed SA (2022) "Reliable Video Forensics Evidence Cataloguing using Video Source device Identification on the Blockchain", International Conference on Emerging Trends in Smart Technologies (ICETST) 1–6, Karachi, Pakistan
21. Ou Y-F, Ma Z, Liu T, Wang Y (2011) Perceptual Quality Assessment of Video Considering Both Frame Rate and Quantization Artifacts. IEEE Trans Circuits Syst Video Technol 21(3):286–298
22. Patel B, Alsadoon A, Prasad PWC, Dawoud A, Rashid TA, Alsadoon OH, Jerew OD (2022) Secure data transmission in a real-time network for a tele-training education system. Multimedia Tools and Applications 81:27819–27836
23. Prokop K, Połap D, Srivastava G, Lin JC-W (2022) "Blockchain-based federated learning with checksums to increase security in Internet of Things solutions", J Ambient Intell Humaniz Comput 1–10 https://doi.org/10.1007/s12652-022-04372-0
24. Rajalakshmi K, Mahesh K (2018) ZLBM: zero level binary mapping technique for video security. Multimedia Tools and Applications 77:13225–13247
25. Ranjithkumar R, Ganeshkumar D, Senthamilarasu S (2021) Efficient and secure data hiding in video sequence with three layer security: an approach using chaos. Multimedia Tools and Applications 80:13865–13878
26. SIEMENS, "Intelligent CCTV", tech. rep., online; url: https://www.mobility.siemens.com/global/en/portfolio/rail/rolling-stock/digital-train-solutions/intelligent-cctv.html [Accessed: January 13, 2023]
27. Wang Z, Tameh E, Nix A (2008) Joint shadowing process in urban peer-to-peer radio channels. IEEE Trans Veh Technol 57(1):52–64
28. Wu Y, Ye D, Wei Z, Wang Q, Tan W, Deng RH (2019) Situation-Aware Authenticated Video Broadcasting Over Train-Trackside WiFi Networks. IEEE Internet Things J 6(2):1617–1627

29. Yaacoub E (2021) Travel Hopping Enabled Resource Allocation (THEResA) and delay tolerant networking through the use of UAVs in railroad networks. Ad-Hoc Networks (Elsevier) 122:1–10
30. Yaacoub E, and Dawy Z (2014) “Fair Optimization of Video Streaming Quality of Experience in LTE Networks using Distributed Antenna Systems and Radio Resource Management”, Journal of Applied Mathematics, Special Issue on “Fair Optimization and Networks: Models, Algorithms, and Applications”, Vol. 2014, Article ID 562079, Open Access, Published online: https://doi.org/10.1155/2014/562079
31. Yaacoub E, Atat R, Alsharoa A, Alouini M-S (2014) Mobile Relays for Enhanced Broadband Connectivity in High Speed Train Systems. Physical Communication (Elsevier) 12:105–115
32. Yaacoub E, Alsharoa A, Ghazzai H, Alouini M.-S (2021) “Seven Challenges for Communication in Modern Railway Systems”, Frontiers in Communications and Networks, 1, 8 https://doi.org/10.3389/frcmn.2020.619527
33. Yamamoto K, Kusuda A, Yoshida S, (2006) Impact of shadowing correlation on coverage of multihop cellular systems, In Proc. IEEE International Conference on Communications (ICC 2006), Istanbul, Turkey, 4538–4542

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.