

7-2018

Situation-aware authenticated video broadcasting over train-trackside WiFi networks

Yongdong WU
Jinan University - China

Dengpan YE
Wuhan University

Zhuo WEI
Huawei International Pte Ltd


Qian WANG
Wuhan University

William TAN
Mirai Electronics Pte Ltd

See next page for additional authors

DOI: <https://doi.org/10.1109/JIOT.2018.2859185>

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the [Information Security Commons](#), [OS and Networks Commons](#), and the [Transportation Commons](#)

Citation

WU, Yongdong; YE, Dengpan; WEI, Zhuo; WANG, Qian; TAN, William; and DENG, Robert H.. Situation-aware authenticated video broadcasting over train-trackside WiFi networks. (2018). *IEEE Internet of Things*. 1-11. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/4098

Author

Yongdong WU, Dengpan YE, Zhuo WEI, Qian WANG, William TAN, and Robert H. DENG

Situation-aware Authenticated Video Broadcasting over Train-trackside WiFi Networks

Yongdong Wu, Dengpan Ye, Zhuo Wei, Qian Wang, William Tan, and Robert H. Deng, *Fellow IEEE*

Abstract—Live video programmes can bring in better travel experience for subway passengers and earn abundant advertisement revenue for subway operators. However, because the train-trackside channels for video dissemination are easily accessible to anyone, the video traffic are vulnerable to attacks which may cause deadly tragedies.

This paper presents a situation-aware authenticated video broadcasting scheme in the railway network which consists of train, on-board sensor, trackside GSM-R (Global System for Mobile Communications-Railway) device, WiFi AP (Access Point), and train control center. Specifically, the scheme has four modules: (1) a train uses its on-board sensors to obtain its speed, location, and RSSI (Received Signal Strength Indicator) of train-trackside WiFi channel; (2) the train reports these real-time measurements to the railway control center with the legacy GSM-R networks; (3) according to the measurements, the control center or its WiFi AP adaptively customizes the protected codestream bitrate and AP-train handover time; (4) the train renders the received codestream which passes the authenticity verification process. As shown in the performance analysis, the present scheme ensures the codestream authenticity and provides high QoS (Quality of Service) in the lossy subway WiFi environment.

Index Terms—Situation-aware; Streaming authentication; Scalable Video Coding; Subway WiFi.

I. INTRODUCTION

As a daily transportation means for a large amount of passengers in many cities [1], by nature subway is an important area for broadcasting multimedia programmes, government notices, commercial advertisements, etc. However, since a video codestream delivered over wireless channel is usually erroneous in subway environments [2]–[4], most of subway

Manuscript received on x; revised on x; accepted on 03 July 2018. The associate editor coordinating the review of this paper and approving it for publication was x. This work was in part supported by Guangdong Innovative and Entrepreneurial Research Team Program (No. 2014ZT05D238), and the National Natural Science Foundation of China under Grant No. U1636209, U1636101, and U1736211. It was also in part supported by the Project of Scientific and Technological Breakthrough in Strategic Emerging Industries in Hunan Province (2017GK4006) and The National Key Research and Development Program of China (2018YFD070141). The work is in part supported by Institute for Infocomm Research, Singapore. Corresponding author: Dengpan Ye.

Y. Wu is with Jinan University, China and Wuhan University, China (e-mail: wuyd007@qq.com).

D. Ye and Q. Wang are with School of Cyber Science and Engineering, Wuhan University, China (e-mail: {yedp,qianwang}@whu.edu.cn).

Z. Wei is with Huawei International Pte Ltd, Singapore (e-mail: phdzwei@gmail.com).

W. Tan is with Mirai Electronics Pte Ltd, Singapore (email: mirai@singnet.com.sg)

R. H. Deng is with Singapore Management University, Singapore (e-mail: robertdeng@smu.edu.sg).

Digital Object Identifier XXX.

providers only serve pre-recorded video which are replayed on the trains. Apparently, this kind of offline services is not satisfactory as it can not render real-time programmes such as live sports games. Although 3G/4G/5G mobile networks enable to provide real-time multimedia broadcast services [5], the subway operators have to pay the subscription fee and rely on the telco all the time. Therefore, they would prefer to broadcasting video programmes with their own WiFi (or other spectrum-free) networks.

The subway video dissemination over WiFi networks must guarantee video authenticity as safety is always the first priority in subway services. Unfortunately, subway is an “ideal” target for attackers such as terrorists in Moscow subway tragedy [6]. As an example of practical threats, when an unprotected multimedia is disseminated over a public network, an adversary is able to tamper with the broadcast system to cause riots or bad effects [7]. When a video is distributed over a WiFi network, this kind of cyber-attack becomes possible theoretically [8] and practically [9].

The subway video dissemination over WiFi shall guarantee high QoS (Quality of Service) too. Clearly, if the quality of advertisement video is too low to satisfy the passengers, the subway operators will suffer from revenue loss. The degradation of the video QoS may be due to some factors: (1) interference sources (e.g., train movement, random noise, and signal fading) which incur packet errors [10]–[13]; (2) Handover delay which leads to the poor performance or instability of communicating quality in mobile applications. When a train moves from the coverage of one AP (Access point) to the coverage of another, it usually has to carry on a handover process which may take up to 500ms [14] such that many video frames may lose or include artifacts.

This paper presents a novel legacy-compatible method which ensures high quality and authenticity of live video broadcasting in a lossy subway environment. In the proposed scheme, an operation center creates a trusted SVC (Scalable Video Code) codestream, broadcasts it to all the APs on the subway lines. According to the measured train location, speed and WiFi signal quality, each AP adaptively tunes WiFi bitrate and optimally truncates codestream such that the passing-by trains can receive the video of high quality in real-time. Based on the performance analysis, the present scheme is able to protect any innocent train even if all APs and other trains are compromised, and provide a satisfactory video broadcast service in the harsh subway WiFi environments. The strengths of the present scheme are as follows.

- High compatibility with legacy rail transportation infrastructure. The present scheme employs the existing

video broadcast system, on-board sensors and track-side GSM-R communication systems to provide codestream authenticity and high QoS.

- Optimal authenticity rate according to real-time RSSI (Received Signal Strength Indicator) of the train-AP channel. As train-AP RSSI is readily measured by the train and sent to AP via the operation center, the AP is able to optimize the video delivery in terms of WiFi bitrate and FEC (Forward Error Correcting) code.
- Situation-aware handover for improving authentication rate and quality of service according to RSSI and train-AP distance. As train's state information (such as location, speed and moving direction) and AP location information are easily available in the railway system, the new AP can be determined in advance. Therefore, similar to GSM-R (Global System for Mobile Communications-Railway) handover [15], the WiFi handover time is shortened significantly such that the AP-train connectivity remains stable at handover time.

The remainder of this paper is organized as follows. Section II introduces the related work on WiFi networks, SVC streaming authentication, and train video broadcast. Section III elaborates the novel authenticated video streaming over train-trackside communication channels. Section IV introduces situation-aware optimization of streaming authentication process. Section V analyzes the present scheme. Finally, Section VI addresses the conclusion and future works.

II. RELATED WORK

In order to deliver a trusted video in a harsh subway environment, it is necessary to ensure error-resilience of WiFi communication, and authenticity of scalable video codestream in the train video broadcast system.

A. WiFi Communication

IEEE 802.11 or WiFi standard specifies different data rates over wireless channels [16]. Although a higher data rate means more emitted signals per second, the actual throughput may be lower because higher data rate may incur more transmission errors and demand more retransmissions [17]. As one part of IEEE 802.11 standard to reduce retransmissions, DRS (Dynamic Rate Switching) enables both mobile devices and APs to negotiate data rate based on some information, e.g., RSSI which represents the relationship between sending signal power and receiving power [18] [19]. Although DRS is critical to WiFi performance, its implementation mechanism is unspecified in IEEE 802.11 standards.

An enterprise WiFi network [20] enables users to roam among different regions of the enterprise building. Due to the restriction of WiFi AP coverage, multiple APs are needed to cover a larger building, multiple floors, outdoor areas etc. As an enterprise WiFi network is designed for high signal-noise-ratio and low speed applications, its technology may be applicable to vehicular opportunistic access [21], rather than video dissemination in the harsh subway WiFi network.

Unlike the low-speed mobile device, a moving train has to realize quick handover which enables the train to switch the

connectivity from an old AP to a new AP within a tolerable period, in order to provide the illusion of continuous WiFi connectivity. Whenever there is a handover, there is a QoS degradation risk due to packet delay and dropping. Hence fast handover [22]–[24] or even handover-free [25] technologies have been intensively investigated for high mobility performance. In particular, location-aware handover schemes are attractive as they are able to reduce handover time by exchanging communication context among neighboring APs [26]–[28]. Nonetheless, handover is still one of major challenging factors for real-time video delivery in dynamic and hostile environments.

B. SVC Codestream and its Authenticity

In a harsh subway environment, the WiFi connectivity between train and AP varies with train location, speed, and surround conditions. If the bitrate of a codestream is constant and the WiFi signal is weak, some video data can not be delivered properly. Hence, it is valuable to directly reduce the video codestream bitrate as the process of codestream decoding and re-encoding is time-consuming at the AP side.

1) *SVC codestream structure*: SVC enables “encode once, decode many ways”, i.e., its codestream can be directly truncated into many sub-codestreams without re-encoding. As shown in Fig. 1, an SVC codestream consists of NALUs (Network Abstract Layer Unit) which includes a 3-bit field NRI signalling importance of the NALU. The NALUs can be classified into VCL (Video Coding Layer) NALU and Non-VCL NALU. A VCL NALU has a payload field for the compressed visual data, while a Non-VCL NALU has an *Auxiliary payload* field for decoding (e.g., SVC header in prefix NALU). A VCL NALU has two kinds of structures. One has an SVC header itself, while another has to form a pair with a prefix Non-VCL NALU whose auxiliary payload is an SVC header. An SVC header includes PRID (Priority Identifier), DID (Dependency Identifier), QID (Quality Identifier) and TID (Temporal Identifier) which are used for different codestream reduction methods [29].

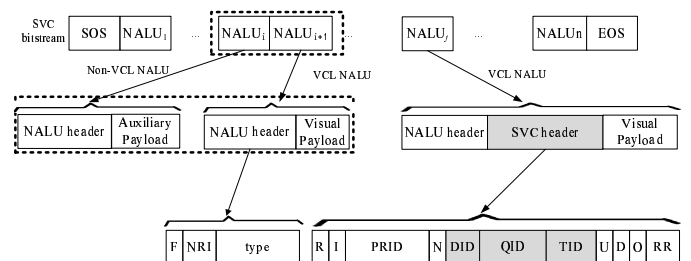


Fig. 1. The structure of SVC bitstream. The dash box means that some VCL NALU shall follow a prefix Non-VCL NALU [29].

2) *SVC authenticity*: As introduced in Section I, video broadcast on the train may be tampered with by a malicious attacker. A naïve way to thwart illegal manipulation is to treat multimedia bitstream as non-structural data, authentically encrypt them as a whole, and distribute the ciphertext bitstream. However, this approach is not suitable for multimedia

broadcast in the subway as the bitrate of delivered codestream shall be adaptive to the lossy network environment.

Up to now, there are many authenticated video streaming schemes which can be classified into three categories: cryptographic authentication, watermarking-based authentication and content-based authentication [30]. Cryptographic authentication techniques employ cryptography primitives such as digital signature or MAC (Message Authentication Code) to ensure data authenticity [31]–[33]; Watermarking-based authentication schemes embed a reference object (e.g., image or message) into an SVC codestream. As the reference object and the SVC codestream are mixed together, the embedded reference object will be manipulated if the SVC codestream is maliciously tampered with [34]; In a content-based authentication scheme, a content provider extracts multimedia features, generates a reference object with the extracted features, and delivers the reference object to end users via a secure channel such that the receiver is able to verify the received multimedia against the secured reference object [35]. However, they are designed for authenticated video streaming to stationary nodes, rather than mobile nodes.

C. Video Broadcasting on Train

In many railway broadcast systems, the video programmes are pre-loaded into the train and then replayed when the train is on-duty. This pre-recorded mode provides the best quality of services. However, its impact is not significant as passengers are often uninterested in “old” messages.

Presently, some railway systems offer non-reliable live programmes over train-trackside WiFi networks, as shown in Fig.2. Although unequal error protection [36], layer-aware FEC [37], and layer-mixed FEC [38] technologies are able to increase the robustness of network communications, the video QoS is yet not guaranteed as they are not customized for the error-prone railway network environments.

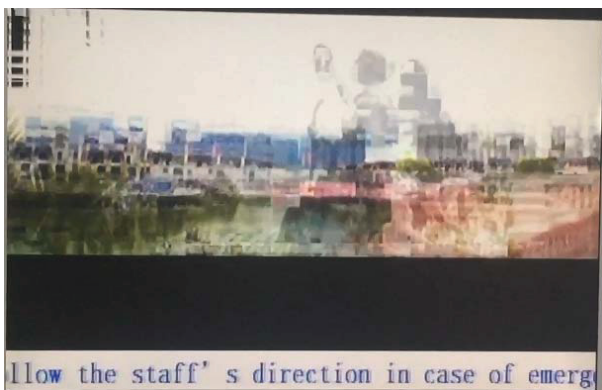


Fig. 2. An non-authenticated image captured from a screen of a real subway video system.

More seriously, the subway video delivery system is lack of security protection such that it is vulnerable to deadly attacks due to: (1) a video broadcast system is localized in an open area and easy to be physically manipulated by attackers; (2) Subway wireless signals are publicly accessible

and easy to be manipulated by anyone with a WiFi transceiver; (3) Multimedia are broadcast in plaintext in some real subways in order to avoid the complicated cryptography key management and compatibility problem existing between the video decoders from different suppliers; (4) broadcast system designers focus on reducing handover time and packet loss rate [39], worry about protection methods which may add overhead and propagate the packet errors; and believe that the subway is physically secure as the operator controls the subway infrastructure.

III. ON-BOARD AUTHENTICATED VIDEO BROADCASTING

On-board video programme services are beneficial to both passengers and subway operators, and hence become more and more popular in subway trains. This Section presents an on-board authenticated video broadcast system in a railway network.

A. System Diagram

As shown in Fig.3, a railway network consists of trains equipped with sensors, WiFi communication sub-systems, GSM-R communication sub-systems and an operation center. Each train communicates with the center via WiFi AP and GSM-R base station which are installed on the subway trackside. As GSM-R is the important train-trackside communication sub-system of a modern subway transport system such as ETCS (European Train Control System) [40], both WiFi APs and GSM-R stations can be installed simultaneously such that the total installation cost is small. Here, the GSM-R communication is bi-directional for train states while WiFi communication is unidirectional for video broadcasting.

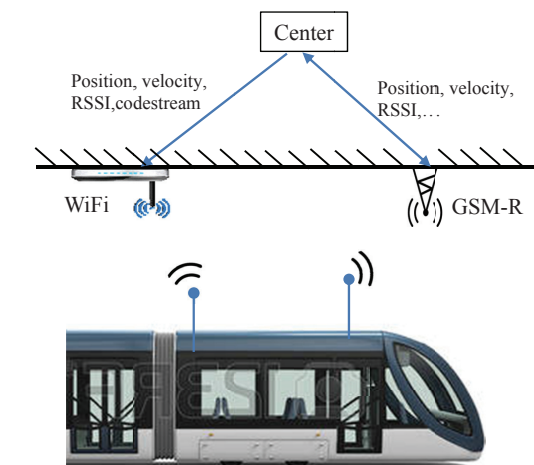


Fig. 3. System diagram, where the WiFi network and GSM-R network exist in the current subway infrastructure. Here, GSM-R is used to represent all the communication systems including LTE-R (Long-Term Evolution - Railway), TETRA (TERrestrial TRunked Radio) etc.

B. Security Model

In a subway system, WiFi APs may be manipulated by an attacker because they are installed in unprotected open areas.

Additionally, the attacker is also able to insert faked multimedia by hijacking the WiFi channels. Hence, to guarantee the authenticity of the broadcast multimedia, only the producer at the operation center is assumed to be trustworthy, but APs and trains may be vulnerable to attacks such as man-in-the-middle attack. In this paper, we ignore denial of service attack and/or channel jamming.

In addition, the sensors for train location, speed, and RSSI are assumed to be trusted, and hence their readings can be used as trusted sources (within tolerable error ranges) for optimizing the video dissemination.

C. Authenticated Video Broadcasting Scheme

In order to ensure the authenticity of the codestream sent from an operation center to a train, the center will create an authenticated codestream which will be broadcast to the WiFi APs. Each AP will adaptively truncate the codestream and prepare the authentication tokens. After receiving the truncated bitstream, the passing-by train will verify and decode it. The generic authentication process is similar to the cryptographic stream authentication scheme [30] [31], except that the low-cost symmetric key management and codestream truncation are customized for the subway system.

1) *Overview of on-board video broadcasting:* As shown in Fig.4, when a train is on duty, it periodically measures its location and speed using the on-board sensors, and then uploads the measurements to the train center via GSM-R base stations. Afterwards, the center continuously broadcasts the states of all the trains to the APs, as well as video codestreams. If a train is within the coverage of an AP, the AP will customize the video codestream according to RSSI, train speed and train location, and broadcast the customized codestream. After receiving the customized codestream, the passing-by train will verify and render them on the on-board screen.

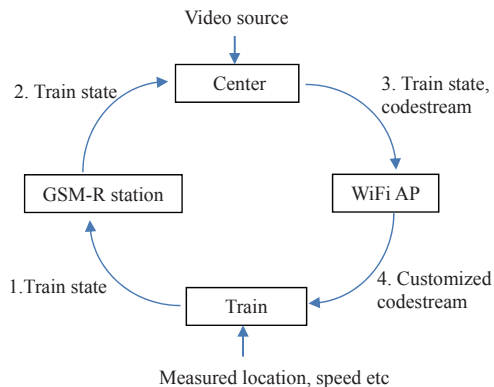


Fig. 4. Workflow for video streaming over train-trackside WiFi Network.

2) *Train-wise key generation:* In order to ensure over-the-air security of GSM-R communication, a train and the control center share a secret k_{GSM} in the legacy communication system. By re-using the shared key, a key for the codestream authentication can be generated as

$$k_{Tid} = \mathcal{H}(k_{GSM}|Tid) \quad (1)$$

is generated at both the center and the train for video authentication, where $\mathcal{H}(\cdot)$ is a one-way function. As the train keys are independent among the trains, an attacker is unable to attack the decoder of one train by compromising the decoder of another.

3) *Creating codestream at center:* A video can be encoded into different SVC codestreams but identical visual content by ordering the NALUs based on PRID, DID, QID and TID in different ways. The unique requirement for the ordering is: $\forall i, j$, if NALU U_i is directly or indirectly used to create NALU U_j (i.e., if NALU U_i is missing, the decoding of NALU U_j fails), $i < j$. Thus, as shown in Fig.5, the NALUs can be classified into different priority levels according to their dependency relationship. Those NALUs within the same level form a quality level. By experiment or experience, the center is able to select the number of priorities in advance.

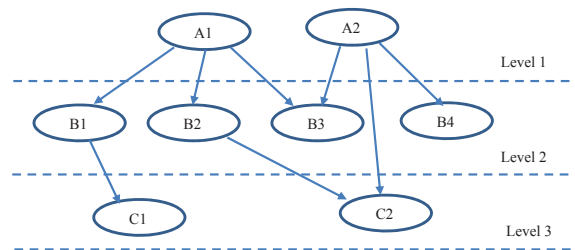


Fig. 5. NALU priority levels. Each eclipse represents an NALU.

In order to reduce the communication overhead for authenticity, the center will divide a video codestream into groups including the constant number of frames each. Assume a group G is encoded into l NALUs U_i , $i = 1, 2, \dots, l$. Then, its progressive hash h_G [41] is calculated as follows.

$$h_l = \mathcal{H}(U_l) \quad (2)$$

$$h_i = \mathcal{H}(U_i \parallel h_{i+1}), \quad i = l-1, \dots, 2, 1 \quad (3)$$

$$h_G = \mathcal{H}(h_1 \parallel G_{id} \parallel V_{id}) \quad (4)$$

where G_{id} is the identification of group G , V_{id} is the identification of the codestream (e.g., video number), and its MAC is

$$\sigma_G = \mathcal{H}(h_G, k_{Tid}) \quad (5)$$

where k_{Tid} is the shared key between the center and train T_{id} . Finally, σ_G is inserted into the **Auxiliary payload** field of the first Non-VCL NALU Γ of group G , and the entire codestream of group G is ready for broadcasting to all the APs via any high-speed network (e.g., fiber network). Thus, similar to the format-compliant encryption scheme [29], the present scheme produces protected codestream which is complaint with original codestream format. As the number of trains is small, the communication overhead for all the σ_G is small too. Especially, as only the authenticated token σ_G for the passing-by train is transmitted over WiFi networks, the WiFi communication overhead is merely one MAC for each group.

4) *Truncating codestream at AP:* In video broadcast applications, codestream data are usually transmitted with the non-reliable and non-retransmission UDP mode. To deal with

the transmission non-reliability, a common practice is that the sender adopts video codestream optimization techniques such as truncating given that the video is encoded at a flexible bitrate [42].

In the subway system, the WiFi quality varies with train location, speed and surround situation. To have an optimal quality of service, AP will properly select the FEC and WiFi bitrate (See Subsection IV-B for details). If there are several passing-by trains around an AP, the AP will broadcast the smallest codestream bitrate such that all the trains can verify their received codestreams.

Clearly, if the truncated codestream is directly delivered over a WiFi network, it will definitely be rejected by the receiver. In order to prove that the truncated codestream is really a portion of the original one, the AP will calculate an authentication token e

$$h_l = \mathcal{H}(U_l) \quad (6)$$

$$h_i = \mathcal{H}(U_i \parallel h_{i+1}) \quad i = l-1, \dots, u+1 \quad (7)$$

$$e = h_{u+1} \quad (8)$$

and insert e into NALU Γ .

5) *Verifying codestream at train:* The verification process basically reverses the generation process for a protected video group. Concretely, after receiving NALUs \hat{U}_j ($j = 1, \dots, u$) and NALU Γ including \hat{e} and $\hat{\sigma}_G$, the train calculates

$$\tilde{h}_u = \mathcal{H}(\hat{U}_u \parallel \hat{e}) \quad (9)$$

$$\tilde{h}_i = \mathcal{H}(\hat{U}_i \parallel \tilde{h}_{i+1}) \quad i = u-1, \dots, 2, 1 \quad (10)$$

$$\tilde{h}_G = \mathcal{H}(\tilde{h}_1 \parallel G_{id} \parallel V_{id}) \quad (11)$$

If and only if $\hat{\sigma}_G = \mathcal{H}(\tilde{h}_G, k_{Tid})$, the train confirms that the received (truncated if any) group G is authenticated.

In order to offer authenticity of the received codestream if there is no attack, the WiFi communication channel shall be sufficiently reliable. In general, the larger the distance between WiFi AP and train, the worse their signal strength and reliability [43]. Meanwhile, in the subway environment, WiFi signal strength is also affected by the path between transmitter and receiver [44], and dynamic train movement [45]. All these factors make the quality of on-board rendered video instable. To fill in the gap, the following sections will improve the QoS with the on-board sensors.

IV. SITUATION-AWARE OPTIMIZATION OF AUTHENTICATED VIDEO BROADCASTING

In video broadcasting applications, QoS of received codestream is related to WiFi data rate. As a suitable data rate should be selected according to many physical variables such as WiFi RSSI, train location, train speed etc, real-time measuring and sharing of the variables play an important role.

A. Real-time situational measurement

In a subway system, distance sensors are used to measure train's speed and/or position for continuously calculating the safe separation distance between neighboring trains. The sensors, typically include wheel angular speed sensors, Doppler radars, accelerometers, and gyroscopes. For instance, SCMT

(Sistema di Controllo Marcia Treno) for Italian railways measures the wheel angular speed to estimate train speed by counting the impulses generated from a sensor per second and calculates the travel distance [46]–[48].

Whenever a train obtains its real-time position, speed measurement, etc, it sends them to the train center, and receives the confirmation commands from the center via train-trackside communication devices. In a railway transportation system, it is critical for safety to share the real-time measurements among the neighboring trains. If the measurements are inaccurate or delayed, collision tragedy may happen [49].

In addition, the WiFi signal strength RSSI can be measured with the communication module in real time by AP and train independently [50].

B. Situation-aware WiFi Data-rate and FEC

As an AP knows RSSI of the AP-train WiFi connectivity, train location and speed, it roughly knows the bit error probability p of the WiFi communication with the passing-by train. Given that the error distribution is uniform, the AP calculates a set

$$S_i = \left\{ (r_i, n, k, t) \mid \exists \mathcal{E}(n, k, t), n \leq \frac{r_i}{\alpha f_G}, k \geq \beta, t \geq np \right\} \quad (12)$$

by testing FEC $\mathcal{E}(n, k, t)$ one by one for each WiFi data rate r_i specified in IEEE 802.11 standard, where n is the transmitted codestream size, k is the actual codestream size, t is the number of tolerable errors in bits, f_G is the number of groups per second, $\alpha \in [0.7, 1)$ is a conservation factor due to network header, IP header etc, and β is the predefined minimal codestream size to ensure the basic video quality.

As there are only thousands of FEC of suitable sizes, it is easy to store their parameters into a data array in advance. As a result, the solution to Eq.(12) can be quickly found by searching the small data array for each data rate r_i . Moreover, as the number R of specified WiFi data rate is also small, AP is able to quickly choose the highest actual codestream rate. i.e., AP chooses the tuple for WiFi data rate r_m and error correction code (n_m, k_m, t_m) as

$$(r_m, n_m, k_m, t_m) = \arg \max_{1 \leq i \leq R} \left\{ \frac{rk}{n} \mid (r, n, k, t) \in \bigcup S_i \right\} \quad (13)$$

Afterwards, the AP will choose the important NATUs U_i ($1 \leq i \leq u$) from the target SVC group, such that the size of all the selected NALUs as k_m . Then, the AP will encode all the important NALUs into a codeword n_m , and discard the unimportant NATUs U_i ($u+1 \leq i \leq l$).

C. Situation-aware Handover

When a train moves along a rail, its AP has to change from time to time. Although IEEE 802.11f IAPP (Inter-Access Point Protocol)¹ and the new standard MIH (Media Independent Information Handover) [51]–[53] might achieve fast handover

¹ IEEE 802 Executive Committee approved IAPP withdrawal on February 3, 2006 (http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm).

and hence increase the QoS, they are not adopted in this paper because they require to change the infrastructure and hence are not applicable to the legacy subway systems.

In the period of AP handover, the train may miss some code-stream packets such that the QoS is reduced. The handover process consists of three phases: scanning AP, authentication of moving station and association between new AP and the moving object, where the scanning AP may cost 80% handover time, or up to 400ms [54]. In order to select the proper handover time, we shall take into consideration of the following factors.

1) *Train location*: IEEE 802.11b specifies three independent WiFi channels, hence it is valuable to configure two neighbor APs with different channels. On the one hand, the interference between two neighboring AP is significantly reduced. On the other hand, as the train knows the locations of the APs, it knows the channel frequency of the next AP based on its measured location. Therefore, the scanning time for handover is reduced to 0. However, as the train localization sensor is inaccurate [40], and the connectivity quality varies from time to time, the train location measurement can be used to grossly determine the handover time only.

2) *WiFi connectivity RSSI*: RSSI is an important indicator for connectivity quality. Although the train-AP distance is a major factor on RSSI, some other factors such as iron bridge, tunnel, interference from passing-by train, and moving speed may have impact on RSSI too. For instance, Fig.6 shows that RSSI decreases with train-AP distance in general, and fluctuates considerably during mobility. Hence, when a train approaches to a predefined location region, it checks whether RSSI of the WiFi channel between the train and the old AP is sufficiently low. If positive, the train can start the handover process.

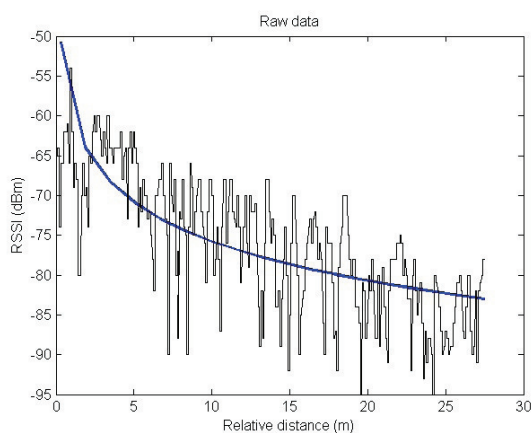


Fig. 6. RSSI vs distance between communication peers [55]. The experiments in [56] also demonstrate the variance of RSSI. RSSI representation varies with the communication chip.

3) *Codestream group*: The handover strategies in subsection V-B consider the connectivity smoothness, rather than content smoothness. In video broadcast applications, although all the APs receive the same packets broadcast from the center, they do not forward the packets to the passing-by trains simultaneously due to their difference in processor

performance, configuration etc. Thus, some broadcast packets may be unavoidably lost in the handover process. Even worse, some other packets which depends on the missed packets are unable to be decoded and have to be discarded, such that the video quality decreases a lot.

Fig.7 shows an example sequence of packets being sent from AP1 and AP2, where AP1 broadcasts video packets earlier than AP2. If the train passes AP1 first and AP2 later, it is able to handover as mentioned in Subsection V-B without missing packets/NALUs. Instead, it may receive redundant packets/NALUs which can be discarded or used to correct errors. On the contrary, if the train passes over AP2 first and AP1 later, some NALUs/packets are not received from either old AP2, or new AP1.

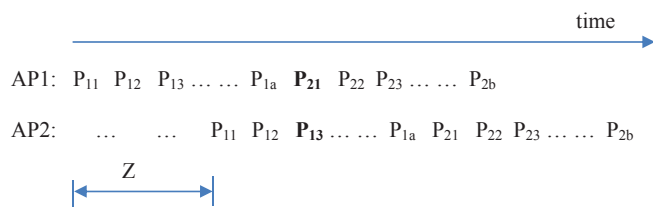


Fig. 7. Refined handover time by considering AP desynchronization.

In order to ensure the effect of the visual experience, the handover time should be refined based on NALU priority or IP packet priority as shown in Fig.5. When the train decides to handover, it will not receive the packet with lower priority from the old AP any more, but the packet with higher priority from the new AP. For example, with reference to Fig.7, when the connectivity is about to transfer from AP2 to AP1, the train shall handover before the time of receiving packet P_{13} sent from AP2 so as to receive packet P_{21} sent from AP1, as packet P_{21} has higher priority than packet P_{13} . In this example, the train has two handover time options: at the time of completely receiving P_{11} or P_{12} . Clearly, the second option is preferable as one more packet (i.e., P_{11}) is received for better QoS.

D. Situation-aware Antenna Switching

The smart handover schemes addressed in Subsection V-B enable to guarantee the QoS at a proper handover time. However, they are not helpful in performance improvement at the rest of communication time. Specifically, when the distance d between AP and train antenna is far, the quality is low according to the model $RSSI = -16.838 \log_{10} d - 59.0668$ in dBm [55]. As shown in Fig.8, if the distance $d > 30$ meters, the signal $RSSI < -80$ dBm, the error probability is high. Hence many off-the-shelf products requires $RSSI < -80$ dBm for good performance.

To reduce the packet error probability and improve the video quality, a straightforward solution is to add more trackside APs. As installing more APs means higher cost and more WiFi interference, it is not widely adopted. Instead, it is preferable to install multiple-antenna on a train [57]. In this case, if the train antenna interval is

$$D_a \leq 2 \times D_{AP} \quad (14)$$

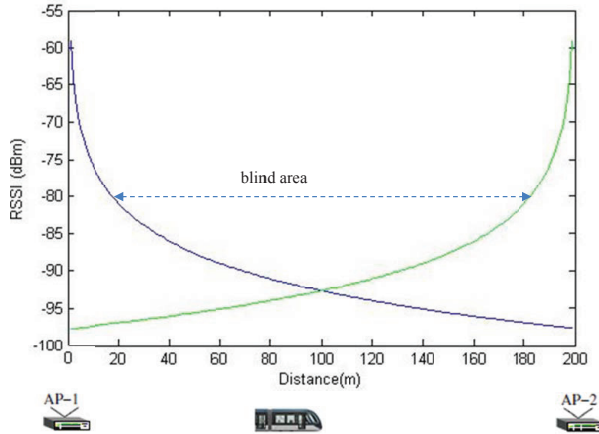


Fig. 8. RSSI changes between two access points and hand-over parameters. There may be a “blind” area between two APs.

where D_{AP} is the coverage of an AP, at least one train antenna is within the coverage of an AP, and the interference between neighboring APs may be very small. For example, in Singapore’s Mass Rapid Transit (MRT) North East Line, a train length is above 80 meters. Suppose that the AP coverage D_{AP} is 20m, $D_a = 40m$ is a good option for the train antenna interval. In other words, it is sufficient that each train is installed with 3 antennas at train head, middle and tail respectively.

Although a multiple-antenna scheme is able to offer high signal level, its importance may decrease significantly without proper multiple-antenna switch process. In the present scheme, based on its location and routine path, a train knows that it enters into the coverage of a new AP, it tunes to the channel of the new AP. When the train travels $2D_{AP}$, it checks the RSSI. If it is below some threshold (e.g., -80dBm), it will switch to the second antenna which are connected with train communication networks [58], and so on.

V. DISCUSSIONS

In this section, we assume that the distance between any two neighboring APs is constant (e.g., 200 meters in some real subway video systems). The communication speed of the backbone network comprising AP and center is sufficiently fast and hence backbone network delay is ignored. Let video frame rate be 25 frames per second, $\alpha = 70\%$, $\beta = 384\text{kbps}^2$ (Common Intermediate Format or CIF³ for short) and each group includes 25 frames, i.e., $f_G = 1$ group per second, and FEC BCH [59] $\mathcal{E}(n, k, t)$ is chosen.

A. Security Analysis

The authentication scheme employs a one-way hash function to protect each NALU, hence any adversary is unable

²Train Communication Network (TCN) connects the on-board train devices. It includes Multifunction Vehicle Bus (MVB) (1.5 Mbps) for the device of a car or car group, and wire train bus (WTB) (1 Mbps) for interconnected cars [58]. Hence, we assume that the video codestream rate is 384kbps.

³The present scheme is also applicable to high-bitrate video stream as the overhead is merely a very small percentage of the total traffic (Please refer to Subsection V-B).

to tamper with the NALUs at the transmission path from the center to the train. Even if the adversary is able to tamper with the APs, the video codestream can not be changed without being identified by the train. Specifically, assume that an attacker is able to fake a (truncated if any) group codestream \check{G} including NALUs $\{\check{U}_i\}$, patch \check{e} and MAC $\sigma_{\check{G}}$, and an innocent train can not identify whether \check{G} is bogus or not. It means that the attacker is able to ensure

$$\sigma_{\check{G}} = \mathcal{H}(h_{\check{G}}, k_{Tid}) \quad (15)$$

That is to say, the adversary is able to create a new MAC $\sigma_{\check{G}}$ without knowing the secret k_{Tid} . Thus, the above assumption does not hold.

A second possible attack strategy is that the attacker is able to fake a group such that $h_G = h_{\check{G}}$. If the strategy is possible, the adversary must be able to prepare the new group \check{G} and \check{e} such that

$$\check{h}_u = \mathcal{H}(\check{U}_u \parallel \check{e}) \quad (16)$$

$$\check{h}_i = \mathcal{H}(\check{U}_i \parallel \check{h}_{i+1}) \quad i = u - 1, \dots, 2, 1 \quad (17)$$

$$h_G = h_{\check{G}} = \mathcal{H}(\check{h}_1 \parallel G_{id} \parallel V_{id}) \quad (18)$$

According to the one-wayness property of $\mathcal{H}(\cdot)$, it is impossible to find the pair (\check{G}, \check{e}) unless it is generated according to Subsection III-C4.

A third one is counterfeiting attack which combines groups of different codestreams [60]. Nonetheless, as group identification G_{id} and codestream ID V_{id} are inserted into Eq.(4), this counterfeiting attack can not be launched either.

B. FEC and Bitrate selection

When there are errors in the codestream, some regions of the decoded frames may include mosaic blocks. Furthermore, the errors will be propagated to their dependencies such that the video quality is decreased to cause bad perception feeling. Therefore, FEC shall be employed to improve the QoS.

When the codestream is distributed over an Ethernet network, each IP packet may be over 1000 bytes. As it is time-consuming to decode/encode a long codeword, the codestream in a group is divided into chunks and encode/decode chunk by chunk in practice. With regard to Eq.(12), for some integer l , we have

$$\begin{cases} n & = 2^l - 1 \\ n - k & \leq lt \\ n & \leq \frac{\alpha r}{f_G} = 0.7r \\ k & \geq \beta = 384 \times 10^3 \\ t & \geq np \end{cases} \quad (19)$$

according to BCH.

To solve Eq.(19), the AP tries $r = 2\text{Mbps}$, assume that network bit error⁴ $p = 7 \times 10^{-4}$ for some train location and

⁴As it is hard to find an existing wireless error probability formula in a subway environment and perform the test experiments, we adopt a conservative method which assumes the bit error here is about as 10 times as bit errors (7.4428×10^{-5}) in [61] for the purpose of explanation here.

speed. Therefore, Eq.(19) can be rewritten as

$$\begin{cases} n_m = 2^{l_m} - 1 \\ n_m - k_m \leq l_m t_m \\ n_m \leq 0.7r = 0.7 \times 2 \times 10^6 \\ k_m \geq \beta = 384 \times 10^3 \times \frac{n_m}{r} = 0.192n_m \\ t_m \geq 0.0007n_m \end{cases} \quad (20)$$

By searching the BCH codebook, the AP can choose $l_m = 10$, $n_m = 2^{l_m} - 1 = 1023$, $t_m \geq 0.0007n \approx 1$, $k_m = 1013$, i.e., BCH $\mathcal{E}(1023, 1013, 1)$ is used to encode each 1013-bit codestream chunk. As a result, the received codestream rate is about $\frac{\alpha r}{f_G} \times \frac{k_m}{n_m} = 0.7 \times 2 \times 10^6 \times \frac{1013}{1023} \approx 1.386 \times 10^6$, or about 1.386Mbps, which is sufficient for most rendering devices in trains. That is to say, data rate $r = 2$ Mbps is suboptimal and viable. Optionally, the AP can solve Eq.(19) by trying other WiFi data rate if it demands better QoS. When the FECs is BCH $\mathcal{E}(1023, 1013, 1)$, the communication overhead is approximately 1% ($\approx \frac{1023-1013}{1013}$).

C. Group Authentication Rate

Given that the WiFi transmission rate is 1.386 Mbps, and each group has 1.386 Mbits as the period is 1 second. Suppose the WiFi Ethernet packet size is 1023 bytes, the number of packets in a group is about 170 ($\approx 1386000/(1023 \times 8)$).

According to the experiments in [61], if there is no error correcting code, the rate of received packets is 93.6%, or 6.4% packet loss rate on average. When each packet is embedded with error correcting code BCH $\mathcal{E}(1023, 1013, 1)$, and each codeblock has the independent error, each codeblock is received at the rate of $b_0 = (0.936^{1/8} + 1023 \times 7.4438 \times 10^{-6})^8 = 99.5\%$. Then the loss rate of FEC packets is 0.5% only.

If the authenticator (MAC σ_G and e) is piggybacked on c packets uniformly distributed over the group, the loss probability of the authentication packet is $A_c = (0.005)^c$. For instance, $A_1 = 0.5\%$, $A_2 = 2.5 \times 10^{-5}$. In spite of the improvement of the video quality, some groups of the codestream will not be fully received correctly and hence fail the codestream verification.

Remark 1: According to Subsection IV-C3, a train may ignore the unimportant NALUs of the old AP, but accept the important packets from the new AP at the handover time. Hence, the authenticity may fail at the handover time. This case is known to the train and hence has minor impact on the authenticity of video content.

D. Codestream buffering

As the train-AP connectivity strength varies over time, the highest data rate fluctuates accordingly. Thus if the actual AP throughput rate r_a is higher than codestream rate r_c , codestream buffering is a viable solution to ensure the stability of codestream bitrate. Specifically, when the WiFi connectivity between train and AP is excellent, the AP broadcasts the codestream at a high data rate such that the train is able to store some codestream for rendering later. Its disadvantage is that the video rendering may be delayed for some time. In other words, codestream buffering aims for the trade-off between real-time and QoS.

As an illustrative example, the distance between two IEEE 802.11b APs in subway is 200m, then travel time between two APs is 20s. Assume that the subway train moves at a constant speed 10m/s or 36km/h, and the WiFi data rate (in million bits per second) is simply selected with the distance d (in meter) between WiFi AP and train antenna.

Table I is the data sheet for codestream transmission, where the first column is the distance between train and AP, the second column is the WiFi data rate selected based on the first column, the third column (the fourth column) is the transmission time (amount resp.) when the WiFi AP transmits the codestream at the data rate in the second column, while the last column is the amount of bitstream sent by the AP in total.

As the AP sends 39 Mbits codestream to the passing-by train within 20 seconds, the average rate is 1.95Mbps which meets the specification of the 4CIF (4 × Common Intermediate Format) @25frames per second. Hence, the datarate switching strategy works. However, when the data-rate of AP is selected to be higher than the codestream bitrate, some codestream shall be prepared in advance. For instance, if the datarate is 11Mbps and the codestream bitrate is 1.5Mbps, the data transmitted in 2 seconds will be rendered within $11 \times 2/1.9 = 11.5$ seconds. In other words, some codestream data will be stored in the buffer and delayed about 10 seconds for rendering.

TABLE I
DATA SHEET FOR IEEE 802.11B RATE SWITCHING, SINGLE ANTENNA

Distance $ d $	Data-rate (Mbps)	Transmission time(s)	Amount (Mbit)	Total (Mbit)
[0,10]	11	2	22	22
(10, 20]	5.5	2	11	33
(20, 30]	2	2	4	37
(30, 40]	1	2	2	39
(40, 100]	0	12	0	39

Suppose the length of the train is 80 meters, and two antennas are installed on the train head and tail. Then Table I will be updated to Table II. As the train is able to receive 78Mbits codestream from each AP, the admissible codestream bitrate is 3.8Mbps. If the bitrate is still 1.5Mbps, the rendering delay can be reduced to 5 seconds.

TABLE II
DATA SHEET FOR IEEE 802.11B RATE SWITCHING, DOUBLE ANTENNAS

Distance $ d $	Data-rate (Mbps)	Transmission time(s)	Amount (Mbit)	Total (Mbit)
[0,10]	11	4	44	44
(10, 20]	5.5	4	22	66
(20, 30]	2	4	8	74
(30, 40]	1	4	4	78
(40, 100]	0	4	0	78

TABLE III
PERFORMANCE COMPARISON

Scheme	Authenticity rate	Quality of service	Mobility	Adaptation	Computation	Traffic overhead
[32]	Middle	Nil	No	No	High	Middle
[38]	Nil	Middle	Yes	No	Low	Nil
Present	High	High	Yes	Yes	Low	Low

E. Comparison

As the subway video broadcast systems are usually proprietary of the vendors, few technical details are publicly accessible. In this Section, we compare the representative of mobile TV technology [38] and video streaming authentication technology [32] with the presented situation-aware trusted video scheme.

As shown in Table III, the second column lists the authenticity rate which is the ratio between authenticated data and received data if there is no attack. Scheme [38] does not address the video authenticity, but video quality only. As scheme [32] is a streaming authentication without considering the network performance, hence its authenticity rate is subject to the packet loss rate.

In the third column, scheme [38] employs FEC to provide packet loss resilience, but the FEC is static rather than adaptive. It can not remain high QoS in all the situations. Scheme [32] assumes that packet loss rate is known for the participants, and ignore the QoS. In the present scheme, the FEC and network bitrate are adaptively tuned, therefore, the QoS is always high.

Column 4 shows that scheme [32] ignores the mobility application where AP handover is necessary, while column 5 indicates that only the present scheme is adaptive in terms of the wireless signal strength, location etc.

In column 6, the computation cost states the computation resource used for the purpose of authenticity and FEC. As the present scheme adopts the symmetric key system, hence its computational cost is low at the center, AP and train, in comparison with scheme [32] which adopts asymmetric key cryptographic primitives.

In the last column, the traffic overhead means the number of bytes is added to the WiFi traffic so as to offer authenticity. Although the overhead of the present scheme is linear with the number of passing-by trains, it is small because the number of trains linking to the same AP is no more than 3 in practice. As MAC is usually much smaller than a digital signature, the present scheme incurs low communication overhead.

VI. CONCLUSION AND FUTURE WORK

Live video programmes can bring in not only better travel experience for the subway passengers, but also extra income for the subway operators. Nonetheless, as unprotected video programmes might be changed by the adversary, deadly riot may happen on the subway trains. By exploiting the legacy sensors of subway, this paper presents a video streaming method which ensures high quality of service and authenticity.

Due to the restriction on the railway infrastructure, it is not easy to evaluate the present scheme in a real railway

environment. Instead, it will be possible to perform simulation with some vehicles in a residential area, where the APs can be installed together with the street lights. When the vehicle moves along the road and reports to the center its locations and speed, the AP will broadcast the video according to the proposed scheme. With the received codestream, the vehicle is able to verify the authenticity and evaluate the QoS.

REFERENCES

- [1] "MRT & LRT trains," Land Transport Authority of Singapore. Last access on 03 May 2018. <http://www.lta.gov.sg/content/ltaweb/en/public-transport/mrt-and-lrt-trains.html>
- [2] S. Dudoyer, V. Deniau, S. Ambellouis, M. Heddebaut, and A. Mariscotti, "Classification of transient EM noises depending on their effect on the quality of GSM-R reception," *IEEE Transactions on Electromagnetic Compatibility*, vol.55, no.5, pp.867-874, Oct. 2013.
- [3] M. Pous, M.A. Azpurua, and F. Silva, "Radiated transient interferences measurement procedure to evaluate digital communication systems," in *Proc IEEE Symp. on Electromagnetic Comp.*, pp.456-461, 2015.
- [4] M. S. Wang, A. Wang, B. G. Bathula, C. P. Lai, I. Baldine, C. Chen, D. Majumder, D. Gurkan, G. N. Rouskas, R. Dutta, and K. Bergman, "Demonstration of QoS-Aware video streaming over a metro-scale optical network using a cross-layer architectural design," in *Proc Optical Fiber Comm. Conf./National Fiber Optic Engineers Conf.*, 2011.
- [5] P. Fraga-Lamas, T. M. Fernandez-Carames, and L. Castedo, "Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways," *Sensors*, 17(6), Article 1457, Jun. 2017.
- [6] L. Harding, and M. Tran, "Moscow metro bombs kill dozens," 29 Mar. 2010. Last access on 03 May 2018. <https://www.theguardian.com/world/2010/mar/29/moscow-metro-bombs-explosions-terror>
- [7] L. Rosencrance, "Hacker hits Toronto transit message system, jabs prime minister," *Computerworld*, 05 May 2006. Last access on 03 May 2018. <https://www.computerworld.com/article/2555194/cybercrime-hacking/hacker-hits-toronto-transit-message-system--jabs-prime-minister.html>
- [8] C. Song, B. Han, H. Yu, and X. Zhang, "Study On Coexistence and Anti-interference Solution For Subway CBTC System And Mifi Devices," in *Proc IEEE Conf. on Broadband Network and Multimedia Technology*, pp.174-180, 2013.
- [9] Y. Huang and Y. Shi, "Shenzhen Metro disruption leads to call to ban Wi-Fi devices on subways," *China Daily*, 06 Nov. 2012. Last access on 03 May 2018. http://usa.chinadaily.com.cn/epaper/2012-11/06/content_15880678.htm
- [10] C. Tang and P. K. McKinley, "Modeling multicast packet losses in wireless LANs," in *Proc ACM workshop on Modeling analysis and simulation of wireless and mobile systems*, pp.130-133, 2003.
- [11] J. Andersen, T. Rappaport, and S. Yeshiva, "Propagation measurements and models for wireless communications channels," *IEEE Communications Magazine*, vol.33, no.1, pp.42-49, 1995.
- [12] D. Eckhardt, and P. Steenkiste, "Measurement and analysis of the error characteristics of an in-building wireless network," *ACM SIGCOMM Computer Communication Review*, pp.243-254, 1996.
- [13] H. Wang and N. Moayeri, "Finite state markov channel - a useful model for radio communication channels," *IEEE Transactions on Vehicle Technology*, pp.163-171, 1995.
- [14] D. Murray, M. Dixon, and T. Koziniec, "Scanning delays in 802.11 networks," in *Proc International Conference on Next Generation Mobile Applications, Services and Technologies*, pp.255-260, 2007.
- [15] K. Kastell, S. Bug, A. Nazarov, and R. Jakoby, "Improvements in railway communication via GSM-R," in *Proc IEEE Vehicular Technology Conference*, pp.3026-3030, 2006.

- [16] An Introduction to Wi-Fi, Digi International Inc, 019-0170 090409-B, 2007. Last access on 03 May 2018. cwi.unik.no/fimages/7/75/An_Introduction_to_wifi.pdf.
- [17] Q. Pang, V.C.M. Leung, and S. C. Liew, "A rate adaptation algorithm for IEEE 802.11 WLANs based on MAC-layer loss differentiation," in *Proc Int. Conf. on Broadband Networks*, vol.1, pp.659-667, 2005.
- [18] M. Hinson, "Data rate selection for legacy Wi-Fi networks," 22 Feb. 2016. Last access on 03 May 2018. <https://wirelessmore.net/blog/2016/02/22/data-rate-selection-for-legacy-networks/>
- [19] Q. Xia and M. Hamdi, "Smart Sender: A practical rate adaptation algorithm for multirate IEEE 802.11 WLANs," *IEEE Transactions on Wireless Communications*, vol. 7, no. 5, pp.1764-1775, May 2008.
- [20] K. Sui, Y. Zhao, D. Pei, and Z. Li, "How bad are the rogues' impact on enterprise 802.11 network performance?" in *Proc IEEE Conference on Computer Communications*, pp.361-369, 2015.
- [21] N. Cheng, N. Lu, N. Zhang, X. Zhang, X. S. Shen, J. W. Mark, "Opportunistic WiFi offloading in vehicular Environment: A Game-Theory Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol.17, no.7, pp.1944-1955, 2016.
- [22] I. Ramani and S. Savage, "SyncScan: practical fast handoff for 802.11 infrastructure networks," in *Proc Annual Joint Conference of the IEEE Computer and Communications Societies*. vol. 1, pp. 675-684, 2005..
- [23] H. Lee, Y.-u. Chung, and Y.-H. Choi, "A seamless handover scheme for IEEE WAVE networks based on multi-way proactive caching," in *Proc International Conference on Ubiquitous and Future Networks*, pp.356-361, 2013.
- [24] L. Zhang, N. Seta, H. Miyajima, and H. Hayashi, "Fast authentication based on heuristic movement prediction for seamless handover in wireless access environment," in *Proc IEEE Conference on Wireless Communications and Networking*, pp.2889-2893, 2007.
- [25] A. Croitoru, D. Niculescu, and C. Raiciu, "Towards Wifi mobility without fast handover," in *Proc USENIX Symposium on Networked Systems Design and Implementation*, pp.219-234, 2015.
- [26] Y.-S. Chen, M.-C. Chuang, and C.-K. Chen, "Deuce-based fast handoff scheme in IEEE 802.11 wireless networks," *IEEE Transactions on Vehicular Technology*, vol.57, no.2, pp.1126-1141, Mar. 2008.
- [27] M. Shin, A. Mishra, and W. A. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," in *Proc ACM International Conference on Mobile Systems, Applications, and Services*, pp. 70-83, 2004.
- [28] M. Almulla, Y. Wang, A. Boukerche, and Z. Zhang, "Design of a fast location-based handoff scheme for IEEE 802.11 vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 8, pp.3853-3866, 2014.
- [29] Z. Wei, Y. Wu, X. Ding, and R. H. Deng, "A scalable and format-compliant encryption scheme for H.264/SVC bitstreams," *Signal Processing: Image Communication*, vol. 27, no. 9, pp.1011-1024, 2012.
- [30] Z. Wei, Z. Yan, Y. Wu, and R. H. Deng, "Trustworthy Authentication on Scalable Surveillance Video with Background Model Support," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 12, no. 4, Article 64, page 1-20, Sept., 2016.
- [31] Y. Wu and R. H. Deng, "Scalable authentication of MPEG-4 streams," *IEEE Trans. on Multimedia*, vol. 8, no. 1, pp.152-161, 2006.
- [32] Z. Wei, Y. Wu, R. H. Deng, and X. Ding, "A Hybrid Scheme for Authenticating Scalable Video Codestreams," *IEEE Transactions on Information Forensics and Security*, 9(4):543-553, Apr., 2014.
- [33] K. Mokhtarian, and M. Hefeeda, "Authentication of scalable video streams with low communication overhead," *IEEE Transactions on multimedia*, vol. 12, no. 7, pp. 730-742, 2010.
- [34] S. W. Park and S. U. Shin, "Authentication and copyright protection scheme for H.264/AVC and SVC," *Journal of information science and engineering*, vol. 27, no. 1, pp. 129-142, 2011.
- [35] B.B. Zhu and M. D. Swanson, "Multimedia authentication and watermarking," *Multimedia Information Retrieval and Management*, pp. 148-177, 2003.
- [36] L. Yuan, H. Li, and Y. Wan, "A novel UEP fountain coding scheme for scalable multimedia transmission," *IEEE Trans. on Multimedia*, vol. 18, no. 7, pp. 1389-1400, Jul. 2016.
- [37] C. Hellge, D. Gomez-Barquero, T. Schierl, and T. Wiegand, "Layer-aware forward error correction for mobile broadcast of layered media," *IEEE Trans. on Multimedia*, vol. 13, no. 3, pp. 551C562, Jun. 2011.
- [38] L. Zhang, Y. Li, P. Cheng, and M. Li, "A layer-mixed FEC scheme for scalable media transmission over mobile TV services," *IEEE Transactions on Broadcasting*, vol. 63, no. 2, pp. 309-320, 2017.
- [39] Y. Xu, Y. Zhou, and D.-M. Chiu, "Analytical QoE models for bit-rate switching in dynamic adaptive streaming systems," *IEEE Transactions on Mobile Computing*, vol.13, no.2, pp.2734-2748, 2014.
- [40] ERTMS/ETCS, SUBSET-041, 3.1.0, "Performance requirements for interoperability," 01 Mar. 2012.
- [41] Y. Wu, D. Ma, and R. H. Deng, "Progressive protection of JPEG2000 codestreams," in *Proc IEEE International Conf. on Image Processing*, pp.3439-3442, 2004.
- [42] S. H. Ahmed, S. H. Bouk, A. Mehmood, N. Javaid, and S. Iwao, "Effect of fast moving object on RSSI in WSN: An experimental approach," *Communications in Computer and Information Science:Emerging Trends and Applications in Information Communication Technologies*, vol. 281, pp. 43-51, 2012.
- [43] M. Brown, and J. Galbraith, "Fact or fiction: what affects Wi-Fi speed?," *MacWorld*, 04 Nov. 2013. Last access on 03 May 2018. <http://www.macworld.com/article/2058324/fact-or-fiction-what-affects-wi-fi-speed-.html>
- [44] C.-C. Pu and H.-J. Lee, "State and path analysis of RSSI in indoor environment," in *Proc International Conference on Machine Learning and Computing*, pp.289-293, 2009.
- [45] T. Zhou, H. Sharif, M. Hempel, P. Mahasukhon, and S. Ci, "Performance of IEEE 802.11b in mobile railroad environments," in *Proc IEEE Conference on Vehicular Technology Conference*, vol. 4, pp.2527-2531, 2005.
- [46] M. Malvezzi, G. Vettori, B. Allotta, L. Pugi, A. Ridolfi, F. Cuppini, and F. Salotti, "Train position and speed estimation by integration of odometers and IMUs," *World Congress Railway Research*, 2011.
- [47] B. Allotta, V. Colla, and M. Malvezzi, "Train position and speed estimation using wheel velocity measurements," *the Institution of Mechanical Engineers Part F Journal of Rail and Rapid Transit*, vol. 216, no. 3, pp.207-225, 2002.
- [48] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, "Vulnerabilities, attacks, and countermeasures in balise-based train control systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no.4, pp.814-823, Apr. 2017.
- [49] "Completion of detailed investigation into the train collision at joo koon mrt station," Land Transport Authority of Singapore, 18 Dec. 2017. Last access on 03 May 2018. <https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=68a49bb6-7d93-47f3-b435-590481caadd5>
- [50] S. Sun, Y. Wu, B. S. Lim, and H. D. Nguyen, "A High Bit-Rate Shared Key Generator with Time-Frequency Features of Wireless Channels," in *Proc IEEE Global Communications Conference*, pp.1-6, 2017.
- [51] IEEE Std 802.21c-2014, "IEEE Standard for local and metropolitan area networks- Part 21: Media Independent Handover Services Amendment 3: Optimized Single Radio Handovers," 12 Jun. 2014.
- [52] M. Q. Khan, and S. H. Andresen, "Zero scanning time for 802.11 networks by using media independent information server (MIIS)," in *Proc International Conference on Advanced Information Networking and Applications*, pp.467-473, 2012.
- [53] A.D.L. Oliva, A. Banchs, I. Soto, T. Melia, and A. Vidal, "An overview of IEEE 802.21: media-independent handover services," *IEEE Wireless Communications*, vol. 15, no. 4, pp.96-103, 2008.
- [54] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp.93-102, Apr. 2003.
- [55] Q. Dong, and W. Dargie, "Evaluation of the reliability of RSSI for indoor localization," in *Proc International Conference on Wireless Communications in Unusual and Confined Areas*, pp.1-6, 2012.
- [56] J.-G. Lee, B.-K. Kim, S.-B. Jang, S.-H. Yeon and Y. W. Ko, "Accuracy enhancement of RSSI-based distance estimation by applying gaussian filter," *Indian Journal of Science and Technology*, vol.9, no.20, pp.1-5, May 2016.
- [57] P. Du, L. Luo, Y. Ma, and C. Long, "A dual-antenna based handover scheme for GSM-R network," in *Proc International Conference on Wireless Communications & Signal Processing*, pp.1-6, 2012.
- [58] J. C. Moreno, E. Laloya, and J. Navarro, "A link-layer slave device design of the MVB-TCN bus (IEC 61375 and IEEE 1473-T)," *IEEE Transactions On Vehicular Technology*, vol. 56, no. 6, pp. 3457-3468, Nov. 2007.
- [59] S. Lin, D. J. Costello, "Error control coding: fundamentals and applications," 2nd Edition, pp.195, Pearson Education International, 2004.
- [60] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Transactions on Image Processing*, vol.9, no.3, pp.432-441, 2000.
- [61] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a wireless link in an industrial environment using an IEEE 802.11-compliant physical layer," *IEEE Transactions on Industrial Electronics*, vol. 49, no. 6, pp.1265-1282, Dec. 2002.



Yongdong WU Received the B.Eng and M.S. from Beijing University of Aeronautics and Astronautics, the Ph.D degree from Institute of Automation, Chinese Academy of Science, and the Master for Management of Technology from National University of Singapore. He is a Professor of Jinan University, China, Adjunct Professor of Wuhan University, China and CTO of Mirai Electronics Pte Ltd Singapore. He was Head of System Security Lab, Institute for Infocomm Research, Singapore. His research interests include cyber-physical system security, IoT security, multimedia security, and Network security. He is Associate Editor of International Journal of Security and Communication Networks, and was Program co-Chair of the 11th International Conference on Information Security Practice and Experience (2015). He has published 80 papers as the first author, and 7 patents, won Tan Kah Kee Young Inventors' award in 2004 and 2005. His flexible JPEG2000 image protection schemes were incorporated in the ISO/IEC JPEG 2000 security standard 15444-8 in 2007. He received the Best Paper Award of IFIP Conference on Communications and Multimedia Security (CMS) 2012. He was awarded by China-Singapore Joint Research Programme, NRF (National Research Fund, Singapore), and EMA (Energy Management Agency, Singapore).



Dengpan Ye Received the B.Sc. degree in automatic control from South China University of Technology in 1996 and the Ph.D. degree from Nanjing University of Science and Technology in 2005. He was a Post-Doctoral Fellow in information system with the School of Singapore Management University. Since 2012, he has been a Professor with the School of Cyber Science and Engineering, Wuhan University. His research interests include machine learning and multimedia security. He has authored and/or co-authored over 30 refereed journal and conference

papers.



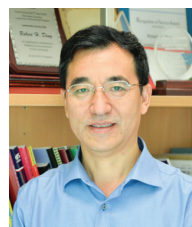
Zhuo Wei received the B.A. degree from Jilin University, China, and the M.S. and Ph.D. degrees from the Huazhong University of Science and Technology, China. He is currently a Research scientist with Huawei International Co. Singapore. His interests include vehicle security and privacy, multimedia security, image processing and video processing. He received the Best Paper Award of CMS 2012.



Qian Wang Received the B.S. degree from Wuhan University, China, in 2003, the M.S. degree from Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences, China, in 2006, and the Ph.D. degree from Illinois Institute of Technology, USA, in 2012, all in Electrical Engineering. He is a Professor with the School of Cyber Science and Engineering, Wuhan University. His research interests include AI security, data storage, search and computation outsourcing security and privacy, wireless systems security, big data security and privacy, and applied cryptography etc. He is an expert under National *1000 Young Talents Program* of China. He is a recipient of IEEE Asia-Pacific Outstanding Young Researcher Award 2016. He is also a co-recipient of several Best Paper and Best Student Paper Awards from IEEE ICDCS17, IEEE TrustCom16, WAIM14, and IEEE ICNP11 etc. He serves as Associate Editors for IEEE Transactions on Dependable and Secure Computing (TDSC) and IEEE Transactions on Information Forensics and Security (TIFS).



William Tan is Managing Director, Mirai Electronics Pte Ltd, Quadstar Pte Ltd, and Mega Power Automation International Ltd. His research interest is R&D in SCADA (Supervisory control and data acquisition), especially RTU (Remote Terminal Unit), FTU (Feeder Terminal Unit), smart meters in utilities and smart Grid development and deployment using Communication Module.



Robert H. Deng (F'16) is AXA Chair Professor of Cybersecurity and Director of the Secure Mobile Centre, School of Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, network security and Internet of Things security. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from SMU, and Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium. His professional services include the editorial boards of IEEE Security & Privacy Magazine, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, Steering Committee Chair of the ACM Asia Conference on Computer and Communications Security, and member of Scientific Advisory Committee of Huawei Research Singapore.