Design and Analysis of HARQ-Based Network Coding for Secure Optical Satellite Systems

Luan V. Doan*, Cuong T. Nguyen*, Hoang D. Le*, Duy-Tuan Dao†, and Anh T. Pham*
* Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan
† The University of Danang-University of Science and Technology, Da Nang 50000, Vietnam

***Abstract*—This paper investigates the reliability and security challenges in free space optics (FSO)-based low Earth orbit (LEO) satellite systems. We propose hybrid automatic repeat request (HARQ)-based network coding (NC) schemes to enhance the security and reliability of FSO-based LEO satellite-assisted Internet of Vehicles (IoV). The approach, HARQ-NC with burst transmission, is introduced. Performance metrics, including frame leakage and frame loss probabilities, and throughput, are analyzed. Numerical results demonstrate the superiority of our proposed schemes over existing solutions. Additionally, we validate our proposals through a case study involving Starlink LEO satellites and moving vehicles.**

***Index Terms*—Low Earth orbit satellite, Internet of Vehicles, free-space optics (FSO), HARQ, network coding, security.**

I. Introduction

Recent years have witnessed the speedy advancement in space communications, e.g., low Earth orbit (LEO) satellite constellation from SpaceX's Starlink project [1]. Moreover, some of the world's leading organizations, including the National Institute of Information and Communications Technology (NICT), Sony Computer Science Laboratories (CSL), German Aerospace Center (DLR), and NASA, have been actively working on free-space optics (FSO) satellite projects [2]. These advancements position FSO-based LEO satellites as a promising network architecture for expanding coverage and enabling high-speed Internet connectivity from space.

FSO-based LEO satellite links face significant challenges, including atmospheric attenuation, turbulence, and pointing misalignment, all of which degrade system performance [3]. Hybrid automatic repeat request (HARQ) is a widely used error-control technique that improves data transmission reliability in FSO-based satellite systems [4]. However, the broad FSO beam footprint of LEO satellites, combined with HARQ retransmissions, introduces a critical security risk. Specifically, passive eavesdroppers within the beam footprint can intercept additional information from HARQ retransmissions, making their presence difficult to detect.

A promising solution to address the aforementioned concern is the integration of network coding and HARQ. In this approach, multiple frames are first encoded using a network coding scheme before being transmitted or retransmitted via HARQ. Since eavesdroppers are passive and cannot request transmissions, they are likely to miss several frames, making it difficult to reconstruct the complete file composed of multiple frames. Consequently, HARQ-based network coding (NC) enhances both security and reliability. The combination of network coding and HARQ has been extensively studied in radio frequency (RF) systems to improve not only reliability and throughput [5] but also security [6], [7]. However, unlike RF systems, which typically handle single-frame transmissions, FSO-based LEO satellites feature long-fat transmission links, allowing multiple data frames to be accommodated within a burst transmission over a long channel coherence time [8]. Additionally, the distinct fading characteristics of FSO channels compared to RF necessitate a tailored HARQ-NC design to optimize system performance. Therefore, designing HARQ-NC with burst transmissions for FSO-based LEO satellite systems is crucial. To the best of our knowledge, such designs remain unexplored in the literature, motivating this study.

This paper aims to design a HARQ-based NC scheme for secure and reliable FSO-based LEO satellite-assisted Internet of Vehicles (IoV). Specifically, we introduce and detail the HARQ-NC framework, which integrates network coding techniques with HARQ protocols to jointly improve both security and reliability in vehicular satellite communication systems. The core idea of the proposed HARQ-NC scheme is to exploit network coding to maintain statistical independence between the channels of legitimate users and potential eavesdroppers, thereby enhancing physical layer security. At the same time, the use of HARQ ensures that only authorized users can successfully recover all private data through selective retransmissions. To assess the effectiveness of the proposed schemes, we evaluate key performance metrics, including frame leakage probability, frame loss probability, and goodput. Furthermore, we provide a comprehensive comparison in terms of system complexity, data loss, and security performance. Finally, we validate our approach through a case study involving Starlink LEO satellites and moving vehicles in Japan.

II. System Descriptions

A. System Model

Figure 1 illustrates the LEO satellite system providing high-speed Internet connectivity to IoV applications, such as self-driving cars, via FSO communications. Additionally, we assume the presence of a passive eavesdropper within the FSO beam footprint of the LEO satellite. For the sake of explicit clarity, we refer to the legitimate LEO satellite, legitimate self-driving car, and eavesdropper as Alice, Bob, and Eve, respectively.

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. DOI: 10.1109/APWCS67981.2025.11151914

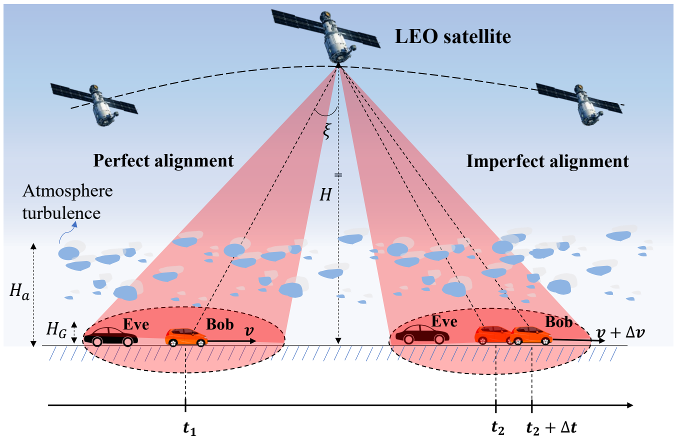

Fig. 1. An illustration of FSO-based satellite-assisted IoV systems in the presence of an eavesdropper.

To ensure reliable space-based Internet connectivity, a type-I (TI) HARQ protocol[1], integrating sliding window ARQ and Reed–Solomon (RS) coding, is employed to mitigate the impact of FSO turbulence channels [4]. The HARQ protocol retransmits uncorrected data frames up to a maximum of M attempts (persistent level), improving system reliability. However, these retransmissions raise security concerns. To address this, a HARQ-based network coding scheme is employed to improve both reliability and security in FSO-based satellite-assisted IoV systems. HARQ-NC design is introduced, with detailed operational descriptions provided in Sec. III.

Data are transmitted in bursts within fixed-duration time slots, each shorter than the channel coherence time. Each burst comprises a fixed number of frames. Upon receiving feedback (ACK/NAK), new and retransmitted frames are scheduled at the start of the next time slot. The feedback channels, which carry channel state information (CSI) and ACK/NAK, are assumed to be reliable.

B. Optical Satellite-to-Bob/Eve Channel Models

Let $i \in \{\mathrm{B}, \mathrm{E}\}$ represent Bob and Eve, respectively. In FSO-based satellite-to-Bob/Eve channels, key impairments such as atmospheric attenuation $h_{\mathrm{a},i}$, atmospheric turbulence $h_{\mathrm{t},i}$, and pointing misalignment $h_{\mathrm{p},i}$, are taken into account. The resulting composite coefficient is given by $h_i = h_{\mathrm{a},i} h_{\mathrm{t},i} h_{\mathrm{p},i}$. The details of these impairments are outlined as follows.

1) Atmospheric attenuation: It is caused by molecular absorption and aerosol scattering in the air given as [9]

$$h_{\mathrm{a}_i} = \exp(-\sigma_i L_i), \tag{1}$$

where $L_i = (H_\mathrm{a} - H_\mathrm{G}) \sec(\xi_i)$ is the distance between the LEO satellite and the vehicle i, with H_a, H_G, and ξ_i respectively the atmospheric altitude, vehicle's altitude, and zenith angle. Additionally, σ_i is the attenuation coefficient found in [9, (2)].

[1]Enhanced HARQ versions, such as chase combining and incremental redundancy HARQ protocols, will be considered in future extensions of this work.

2) Atmospheric Turbulence: It causes the scintillation effect, resulting in the received power fluctuation. The PDF of $h_{\mathrm{t},i}$ modeled by Log-Normal distribution is expressed by [10]

$$f_{h_{\mathrm{t},i}}(h_{\mathrm{t},i}) = \frac{1}{h_{\mathrm{t},i}\sigma_{\mathrm{R},i}\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{\ln h_{\mathrm{t},i} + \sigma^2_{\mathrm{R},i}/2}{\sigma_{\mathrm{R},i}}\right)^2\right], \tag{2}$$

where $\sigma^2_{\mathrm{R},i}$ is the Rytov variance found in [10, (3)].

3) Pointing Misalignment Model: LEO's satellite vibration and variations in the vehicle's velocity lead to the misalignment between the center of the satellite's beam footprint and the vehicle's detector. Notably, the LEO satellite cannot keep track of Bob's detector over a short period when sudden velocity changes occur. As illustrated in Fig. 1, Bob's velocity slightly changes by Δv in a short interval of Δt, causing the misalignment with the beam footprint center. This misalignment distance is, thus, given as $\Delta s = \frac{\Delta v \Delta t}{2}$.

Considering the Gaussian beam, $h_{\mathrm{p},i}$ is approximated as [10]

$$h_{\mathrm{p},i} \approx A_{0,i} \exp\left(-\frac{2r_i^2}{\omega^2_{\mathrm{zeq},i}}\right), \tag{3}$$

where $A_{0,i}$ is the collected power fraction at $r_i = 0$, and $\omega_{\mathrm{zeq},i}$ is the equivalent beamwidth, which are found in [10, (6)]. Using the model reported in [10], the PDF of $h_{\mathrm{p},i}$ is given as

$$f_{h_{\mathrm{p},i}}(h_{\mathrm{p},i}) = \frac{\varphi^2_{\mathrm{Rmod},i}}{A_{\mathrm{Rmod},i}^{\varphi^2_{\mathrm{Rmod},i}}} (h_{\mathrm{p},i})^{\varphi^2_{\mathrm{Rmod},i}-1}, \tag{4}$$

where $\varphi_{\mathrm{Rmod},i} = \frac{\omega_{\mathrm{zeq},i}}{2\sigma_{\mathrm{Rmod},i}}$. Here, $\sigma_{\mathrm{Rmod},i}$ is the jitter standard deviation found in [10, Sec. III-A-3], which is a function of the satellite's jitter angle θ_t and velocity deviation $\sigma_{v,i}$. Also, $A_{\mathrm{Rmod},i}$ is found in [10, Sec. III-A-3].

Remark 1: We assume that Eve maintains an approximate distance of d_E from Bob. The power fraction collected by Eve is also affected by misalignment caused by the satellite's inherent vibrations and velocity variations.

III. Proposal of HARQ-based Network Coding

This section introduces the HARQ-based network coding for secure optical satellite systems.

A. Network Coding Method

First, we describe the network coding method used in this study. The LEO satellite (Alice) sends N data frames to the legitimate vehicle (Bob), represented as $\mathbf{s} = \{s_1, s_2, \cdots, s_N\}$, where each frame s_k is of equal size. These frames are then encoded using the network coding reported in [6], generating a set of network-coded frames denoted as $\mathbf{F} = \{F_1, F_2, \cdots, F_N\}$ as follows:

- **If N is odd**:

$$\begin{aligned} F_i &= s_1 \oplus s_{i+1}, \quad i = 1, \ldots, N-1, \\ F_N &= s_1 \oplus s_2 \oplus \cdots \oplus s_N. \end{aligned} \tag{5}$$

- **If N is even**:

$$\begin{aligned} F_i &= s_1 \oplus s_{i+1}, \quad i = 1, \ldots, N-1, \\ F_N &= s_2 \oplus s_3 \oplus \cdots \oplus s_N. \end{aligned} \tag{6}$$

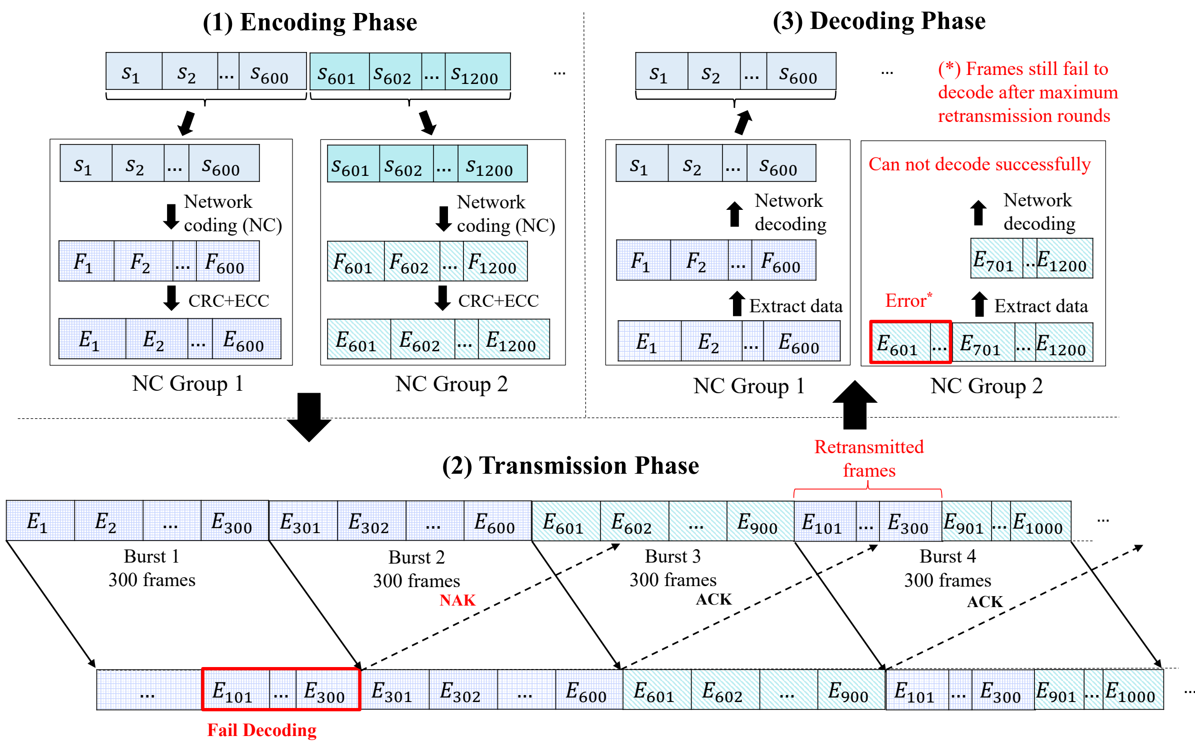

Fig. 2. An illustrative example of the operation of the proposed design.

where $\oplus$ denotes the XOR operator. In summary, the matrix for coded frames $\mathbf{F}$ can be expressed as

$$\mathbf{F} = (\mathbf{G}\mathbf{s}) \bmod 2, \tag{7}$$

where $\mathbf{G}$ is a $N \times N$ encoding matrix. As for decoding, the original frames $\mathbf{s}$ is recovered from $\mathbf{F}$ expressed as

$$\mathbf{s} = \mathbf{G}^{-1}\mathbf{F} \bmod 2, \tag{8}$$

where the inverse matrix $\mathbf{G}^{-1}$ is given as

$$\mathbf{G}^{-1} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ & & & & \\ 1 & 1 & \ddots & 1 & 1 \\ 1 & \cdots & 1 & 0 & 1 \end{bmatrix}_{N\times N}. \tag{9}$$

Remark 2: The matrix indicates that Bob needs N equations to decode s_1, while each subsequent frame $s_2, s_3, \cdots, s_N$ requires $N-1$ equations for successful decoding. In other words, if Bob receives fewer than $N-1$ frames correctly, none of the frames can be decoded.

B. HARQ-Based Network Coding for Secure Systems

1) HARQ-Based Network Coding (HARQ-NC): Figure 2 provides an illustrative example of the proposed design's three-phase operation: (1) Encoding Phase, (2) Transmission Phase, and (3) Decoding Phase. This figure clearly demonstrates how network coding and retransmissions are utilized to ensure successful data delivery, highlighting scenarios of both successful and failed decoding at the receiver. Building upon this visual overview, we now present the design framework for HARQ-based network coding schemes, detailing their structure and operation.

Phase I - Encoding at LEO Satellite: The LEO satellite (Alice) applies network coding to secure data frames before transmission. Each network coding group consists of N data frames, encoded using the encoding matrix $\mathbf{G}$. We assume that the LEO satellite transmits a total of K network coding groups to the legitimate vehicle (Bob) via the FSO link. To enhance reliability, network-coded frames are appended with a CRC for error detection and encoded using an RS code for error correction.

Phase II - (Re)Transmission: Each network coding group is transmitted in multiple bursts. If Bob detects errors and fails to correct corrupted frames, he sends an NAK message to request retransmission from Alice. Each burst may contain new and retransmitted frames. If a frame remains unsuccessfully transmitted after M attempts, the HARQ-NC scheme terminates further retransmissions, and the frame is declared lost.

Phase III - Decoding at Vehicle: Bob can successfully decode the original frame s_k only if all required network-coded frames in the group are received. Specifically, for $s_k = s_1$, all N network-coded frames $\{F_z\}_{z=1}^{z=N}$ must be received, whereas, for $s_k \neq s_1$, $\{F_z\}_{z=1, z\neq k-1}^{z=N}$ must be available. With HARQ-NC, Bob can eventually decode all frames in a network coding group, provided sufficient retransmissions are received. However, as a passive eavesdropper, Eve cannot request retransmissions from Alice. Thus, Eve may miss some frames, preventing her from reconstructing any data within the network coding group. This inability to decode the original frames ensures the security of s_k.

C. Performance Analysis

To evaluate the security performance, we analyze frame leakage probability first, followed by frame loss probability and goodput.

1) Frame leakage Probability: It is defined as the likelihood that Eve successfully decodes an original frame. Specifically, for Eve to decode s_k correctly, she must successfully decode all frames $\{F_z\}_{z=1}^{N}$ when $s_k = s_1$, and $\{F_z\}_{z=1,z\neq k-1}^{N}$ when $s_k \neq s_1$. As a result, the frame leakage probability is given by

$$P_{\text{leak}} \approx \left(P_{k,\text{E}}\right)^N , \tag{10}$$

where $P_{k,\text{E}}$ is the probability that Eve successfully decodes the network-coded frame F_k, occurring when she requires fewer transmission rounds than Bob. Let $m_{k,\text{B}}$ and $m_{k,\text{E}}$ be the transmission rounds needed for Bob and Eve to decode F_k by, respectively, where $m_{k,\text{B}}$ and $m_{k,\text{E}} \in \{1, 2, \cdots, M\}$ and M is the HARQ's persistent level. $P_{k,\text{E}}$ is thus given by

$$\begin{aligned} P_{k,\text{E}} =& \Pr\{m_{k,\text{E}} \leq m_{k,\text{B}}\}, \\ =& \sum_{m=1}^{M-1} \Pr\{m_{k,\text{B}} \geq m\}\Pr\{m_{k,\text{E}} = m\} \\ &+ \Pr\{m_{k,\text{B}} = M\}\Pr\{m'_{k,\text{E}} = M\}, \\ =& \sum_{m=1}^{M-1}\sum_{l=m}^{M} \Pr\{m_{k,\text{B}} = l\}\Pr\{m_{k,\text{E}} = m\} \\ &+ \Pr\{m_{k,\text{B}} = M\}\Pr\{m'_{k,\text{E}} = M\}, \end{aligned} \tag{11}$$

where $\Pr\{m'_{k,\text{E}} = M\}$ is the probability that Eve successfully decodes frame F_k on the M-th transmission round. Additionally, $\Pr\{m_{k,\text{B}} = l\}$ and $\Pr\{m_{k,\text{E}} = m\}$, where $m, l \in \{1, 2, \cdots, M\}$, are determined based on the frame error rate over FSO turbulence channels, as mentioned in Sec. II-B.

2) Frame Loss Probability: It is defined as the probability that Bob fails to decode an original frame. Since the loss of s_1 and $s_k \neq s_1$ corresponds to the loss of at least one network-coded frame among N and $N-1$ frames, respectively. Thus, this probability can be computed as

$$P_{\text{loss}} \approx 1 - (1 - \text{FLR}_k)^N, \tag{12}$$

where FLR_k is the probability that Bob discards the network-coded frame F_k, as given in [10, (36)].

3) Goodput: It is defined as the average total number of successfully received data bits over the total number of transmitted time slots. It is, then, calculated as

$$G_{\text{s}} = \frac{E_{\text{f}} \times N_{\text{f}} \times r_{\text{c}}}{E_{\text{T}} \times T_{\text{slot}}}, \tag{13}$$

where E_{f} and E_{T} are the total number of successfully received data bits and total transmitted time slots, respectively. Additionally, N_{f} is the frame size, r_{c} is the coding rate, and T_{slot} is the time slot duration.

IV. Numerical Results and Discussions

This section evaluates the performance of the proposed design via Monte Carlo simulations. The system parameters, unless otherwise noted, are as follows. *As for the LEO satellite (Alice)*: altitude H = 500 km, zenith angle $\xi_i = 60°$, full divergence angle $\theta = 20\mu$rad, wavelength $\lambda = 1.55\mu$m, vibration jitter angle $\theta_{\text{t}} = 3\mu$rad. *Regarding the vehicles (Bob/Eve)*: altitude $H_{\text{G,B}} = H_{\text{G,B}} = 1.5$m, receiver's aperture diameter $D_{\text{T,B}} = D_{\text{T,E}}$ = 10 cm, detector responsivity $\Re_{\text{B}} = \Re_{\text{E}}$ = 0.9, and velocity variation variance $\sigma_{v,\text{B}} = \sigma_{v,\text{E}}$ = 3 m/s. *For other parameters*: noise standard deviation $\sigma_N = 10^{-7}$ A/Hz, frame size N_f = 2550 bits [11], code rate r_c = 0.9, burst size n_{b} = 300 frames/burst, network coding size 600 frames/group, HARQ's persistent level M = 3, atmospheric altitude H_a = 20 km, ground turbulence $C_n^2 = 10^{-14}\text{m}^{2/3}$, visibility $V = 50$ km.

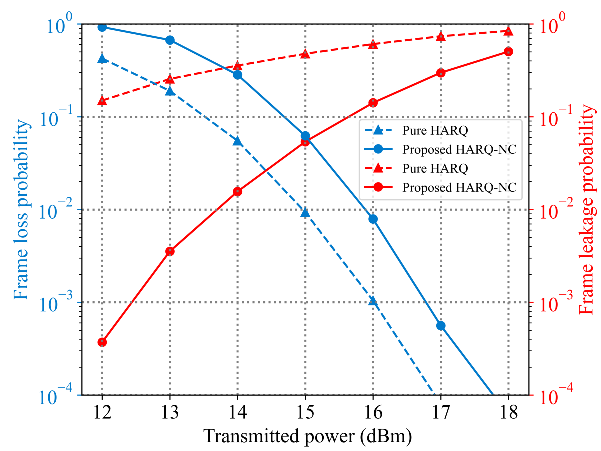

Fig. 3. Performance comparison with different transmitted power levels.

Fig. 3 shows a quantitative performance comparison of different schemes, including pure HARQ (without network coding) and HARQ-NC. Additionally, different satellites' transmitted power levels are considered. As expected, the proposed HARQ-NC schemes outperform the pure HARQ in terms of frame leakage probability. However, this security enhancement comes at the cost of an increased frame loss probability. This is because, in HARQ-NC, Bob must successfully receive and decode all frames within a network coding group to reconstruct the original data. The trade-off between security and reliability is evident in the results, highlighting the importance of selecting an appropriate transmitted power level (P_{t}) to achieve a targeted performance balance. For instance, when using HARQ-NC, to simultaneously maintain a frame leakage probability P_{leak} of 10^{-1} and frame loss probability P_{loss} of 10^{-2}, P_{t} should be set to 16 dBm. This figure thus serves as a critical reference for determining P_{t} in practical implementations.

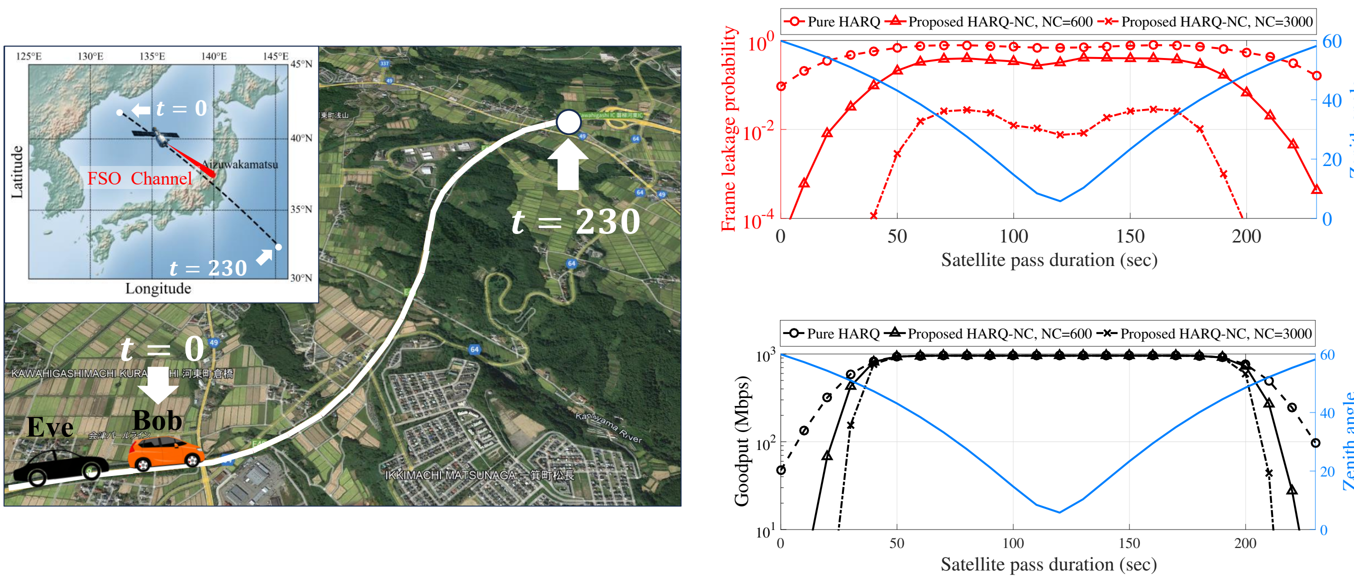

Fig. 4. Frame leakage probability and goodput vs. Starlink's LEO satellite pass duration.

Next, given $P_t = 16$ dBm, we investigate the performance of the proposed HARQ-NC scheme using the STARLINK-1293 satellite over Japan (with satellite pass data in [8, Table IV]). We analyze the security performance and goodput of pure HARQ and HARQ-NC with two different network coding group sizes over a complete satellite pass, as shown in Fig. 4. As expected, the proposed scheme employing network coding enhances the security of the system throughout the entire satellite pass duration. The simulation results also reveal a clear trade-off between throughput and security among the two transmission schemes under varying satellite pass durations. Pure HARQ achieves the highest goodput but suffers from a significantly higher frame leakage probability, making it the least secure option. In contrast, HARQ-NC with a large coding group size (NC $= 3000$) offers the best security performance by minimizing the frame leakage probability; however, this comes at the cost of lower goodput due to the increased frame loss probability associated with larger coding sizes. HARQ-NC with a moderate coding group size (NC $= 600$) achieves a balanced performance, moderately improving security while maintaining reasonable throughput. These findings highlight the importance of selecting an appropriate network coding size in HARQ-NC to effectively balance the trade-off between transmission efficiency and security.

V. Conclusion

This paper proposed and thoroughly analyzed the performance of a HARQ-based network coding (NC) design to enhance the security and reliability of secure optical satellite-assisted IoV systems. The evaluation results demonstrated that this scheme outperforms existing solutions in both security and reliability metrics. Furthermore, a case study involving the Starlink satellite and moving vehicles was conducted to validate the practical applicability of the proposed design.

Acknowledgment

This work was supported by the Telecommunications Advancement Foundation (TAF) and the JSPS KAKENHI Grant number 24K14918.

References

[1] M. Neinavaie, J. Khalife, and Z. M. Kassas, "Acquisition, doppler tracking, and positioning with starlink LEO satellites: First results," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 2606–2610, Jun. 2022.

[2] M. Toyoshima, "Recent trends in space laser communications for small satellites and constellations," *IEEE/Optica J. Lightw. Technol.*, vol. 39, no. 3, pp. 693–699, Feb. 2021.

[3] A. U. Chaudhry and H. Yanikomeroglu, "Free space optics for next-generation satellite networks," *IEEE Consum. Electron. Mag.*, vol. 10, no. 6, pp. 21–31, Nov. 2021.

[4] H. D. Le and A. T. Pham, "Link-layer retransmission-based error-control protocols in FSO communications: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1602–1633, Thirdquarter 2022.

[5] J. Jiao, Z. Ni, S. Wu, Y. Wang, and Q. Zhang, "Energy efficient network coding HARQ transmission scheme for S-IoT," *IEEE Tran. Green Commun. Netw.*, vol. 5, no. 1, pp. 308–321, Mar. 2021.

[6] H. He and P. Ren, "Secure ARQ protocol for wireless communications: Performance analysis and packet coding design," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7158–7169, Aug. 2018.

[7] H. He, P. Ren, and X. Tang, "Joint network coding and ARQ design toward secure wireless communications," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3351–3362, May 2019.

[8] C. T. Nguyen, H. D. Le, C. T. Nguyen, and A. T. Pham, "Toward practical HARQ-Based RC-LDPC design for optical satellite-assisted vehicular networks," *IEEE Trans. Aeros. Electron. Syst.*, vol. 60, no. 6, pp. 8619–8634, Dec. 2024.

[9] Y. Ata and M.-S. Alouini, "Performance of integrated ground-air-space FSO links over various turbulent environments," *IEEE Photon. J.*, vol. 14, no. 6, pp. 1–16, Dec. 2022.

[10] H. D. Le, C. T. Nguyen, T. K. Nguyen, and A. T. Pham, "Hybrid FSO/Sub-THz-based vertical networks for internet of vehicles," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 2, pp. 1865–1881, Apr. 2024.

[11] S. Choi and K. Shin, "A class of adaptive hybrid ARQ schemes for wireless links," *IEEE Trans. Veh. Technol.*, vol. 50, no. 3, pp. 777–790, May 2001.