Permutation-Based Short-Packet Transmissions Improve Secure URLLCs in the Internet of Things

Yuli Yang, *Senior Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—As a promising candidate for ultra-reliable and low-latency communications, the recent permutation-based transmission concept substantially improves the resource utilisation efficiency in the Internet of Things (IoT). In this context, the age of information (AoI) experienced in permutation-based short-packet transmissions is characterised in a wiretap channel, where eavesdroppers are wiretapping the status updates delivered over the legitimate link. The AoI of the legitimate link and the secrecy margin of the wiretap channel are formulated in closed forms within the regime of finite-blocklength information theory to quantify the data freshness and security of status updates in the IoT. The optimal packet structure to be delivered over the network interface is found by solving the optimisation problems of minimising the legitimate link's AoI and maximising the secrecy margin. Illustrative numerical results are provided for our permutation-based transmission to quantify its performance gains over the conventional encapsulation, specifically in short-packet communications.**

***Index Terms*—Age of information (AoI), finite-blocklength information theory, permutation-based transmission, physical-layer security, short-packet communications.**

I. Introduction

In the Internet of Things (IoT), the deployment of ultra-reliable and low-latency communications (URLLCs) faces two major challenges: *(i)* scarce resources to deal with myriads of end-to-end connections [1], [2], and *(ii)* growing security risks caused by sharing common resources among different subscribers [3], [4]. To address both challenges, the concept of permutation-based transmission [5] has been proposed as a promising transport-layer solution for URLLCs, specifically in the IoT [6].

In this work, the metrics of AoI and secrecy margin are developed in the finite-blocklength regime to quantify the performance of secure URLLCs in the IoT. In particular, the optimisation of both metrics will substantiate that the permutation-based transmission achieves better performance than conventional transport-layer encapsulation does in terms of data freshness and wireless security of status updates in the IoT.

A. Related Works

Short-packet transmissions are popular solutions to URLLCs, for accommodating ubiquitous connectivity of massive devices and supporting a wide range of mission-critical applications in the IoT, where the sensing-actuation-control infrastructure creates a foundation for the delivery of status updates [7]. For the design and optimisation of short-packet protocols in URLLCs, recent advances in finite-blocklength information theory have established a metric basis to specify the throughput limits in practice [8], [9].

The IoT has to keep the status updates fresh, for guaranteeing the accuracy and efficacy of the services. For quantifying the freshness of status updates in the IoT, the age of information (AoI) has been proposed as a useful tool to characterise the timestamp of the latest successfully decoded status update at the destination [10], [11]. The impacts of status sampling [12], source coding [13], and channel coding [14] on the AoI in various systems have been investigated. Moreover, the AoI is analysed in a dense IoT system where the carrier-sense multiple access protocol is used to deal with the intense competition among a large number of devices for the delivery of status updates [15]. As for the URLLCs which rely on short-packet transmissions, the AoI framework has been developed in the finite-blocklength regime and optimised by sophisticated packet management schemes; see e.g., [16]–[19] and references therein.

For specific IoT services, e.g., in military, medical and industrial applications, a secure sensing-actuation-control infrastructure is required to protect the status updates against the attacks of malicious eavesdroppers [20]. Due to the broadcasting nature of wireless channels, wireless connections in the IoT are very vulnerable and cannot be fully protected by traditional security protocols. Many research projects have been carried out to improve the wireless security in wiretap channels; see e.g., [21]–[24] and references therein, where secrecy rate, error probability difference, and secrecy energy efficiency are the major metrics for data security evaluation. In addition, energy-efficient computation offloading in the IoT has been conceived with an emphasis on wireless security [25], [26], to improve the edge computing security while reducing the service latency.

The AoI framework was exploited for the performance analysis of secure and timely status updates in the IoT. In [27], the covert AoI was defined as the time elapsed since the latest valid packet was originally generated, where a valid packet is a covertly transmitted and successfully decoded one. In [28], the secrecy age is defined as the positive difference

Y. Yang is with the School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K. (e-mail: yyang@lincoln.ac.uk).

L. Hanzo is with the school of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (email: lh@ecs.soton.ac.uk).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1 and EP/X01228X/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

between the eavesdropper's age and the legitimate receiver's age.

B. Motivation and Novelty

Within the permutation-based transmission, a certain portion of the application-layer data is no longer physically encapsulated into the transport-layer data units (DUs), but conveyed implicitly by the indexed permutations of various DU lengths in a group of packets. The delivery of this portion does not consume any communication resources, thus leading to higher resource utilisation efficiency, which meets the challenge *(i)*. As a successful application of the permutation philosophy in the transport layer, the permutation-based transmission effectively increases the goodput and reduces the latency of the conventional transport-layer encapsulation [5], [6].

From the perspective of wireless security, the CQI-mapped solutions [29]–[33] have been proposed for promoting the practical implementation of physical-layer security in contrast to those using artificial noise to jam the eavesdroppers' wiretapping. Through varying the CQI-based mapping pattern of the application-layer data conveyed by the permutations, permutation-based transmissions ensure that eavesdroppers are unable to successfully decode the data, which meets the challenge *(ii)*. With the mapping pattern interpreted as a secret key in the legitimate link, the secrecy rate of permutation-based transmissions has been analysed in [5] and [6].

The permutation-based transmission is particularly suitable for short-packet protocols in the finite-blocklength regime, because its key virtue is the redundancy reduction, i.e., using shorter packets to convey the given application-layer data. In contrast to the theoretical framework in the infinite-blocklength regime grounded upon Shannon's error-free channel capacity, the packet error probability has to be considered in the finite-blocklength regime. For those received packets with cyclic redundancy check (CRC) errors, the status updates can be either discarded or retransmitted. In comparison to discarding, the retransmission will save the computational resources in status sampling, source coding and channel coding as well as achieve better performance in terms of the AoI, especially when the status updates are generated at a relatively low rate [18].

Motivated by the aforementioned issues, we investigate the performance of permutation-based transmissions in the finite-blocklength regime, taking into account the packet error probability and retransmissions. For a single transmission, a shorter blocklength leads to lower latency. However, for the given amount of information, shorter blocklength means higher coding rate, which results in higher packet error probability and more retransmissions. Concerning the tradeoff between the latency of a single transmission and the total number of (re)transmissions, we formulate the AoI as a function of the blocklength to evaluate the data freshness in permutation-based short-packet transmissions.

Subsequently, based on the AoI framework, we formulate the secrecy margin of a wiretap channel as a function of the blocklength to numerically characterise the data security. In contrast to the secrecy rate achieved by varying the CQI-based mapping pattern in [5] and [6], this work is focused on the security contributed by the packet-length reduction with an emphasis of data freshness. The secrecy margin is defined as the positive difference between the AoI of the wiretapping link and the AoI of the legitimate link[1].

For achieving secure URLLCs, the optimal packet structure is determined by maximising the secrecy margin from the security perspective while minimising the legitimate AoI from the latency perspective. Based on the optimal packet design over the network interface, our secure and timely permutation-based short-packet transmission is compared to the conventional transport-layer encapsulation in the metrics of secrecy margin and legitimate AoI, to quantify the advantage of permutation-based transmissions in terms of secure and prompt status updates.

The novelties of this paper are boldly and explicitly contrasted to the state-of-the-art in Table I at a glance.

C. Contribution

The main contributions in this work are highlighted below.

- The system model of permutation-based short-packet transmissions over a wiretap channel is developed for quantifying the data security and freshness of status updates in the IoT.
- The metrics of legitimate AoI and secrecy margin are formulated in closed-form expressions within the finite-blocklength information theoretic regime, for the timely and secure delivery of status updates via permutation-based short-packet transmissions.
- The optimisation problems of the legitimate AoI minimisation and the secrecy margin maximisation are solved for permutation-based short-packet transmissions to find the optimal packet structure for the timely and secure delivery of status updates.
- The comparisons between our permutation-based transmission and conventional transport-layer encapsulation are carried out using the metrics of legitimate AoI and secrecy margin, for substantiating the benefits of permutation-based short-packet transmissions.

To detail the above contributions, the remainder of this paper is organized as follows. In Section II, the system model of permutation-based short-packet transmissions over a wiretap channel is presented, where our finite-blocklength information-theoretic analysis is introduced as preliminaries. In Section III, the metric of legitimate AoI is formulated and minimised for short-packet communications to find the optimal packet structure, from the perspective of data freshness. In Sections IV, the secrecy margin is formulated and maximised to find the optimal packet structure, from the perspective of data security. Subsequently, Section V provides illustrative numerical results for quantifying the performance gain obtained by our permutation-based transmission over the conventional transport-layer encapsulation, for the secure and

[1] Hereafter, the AoI of the wiretapping link spanning from the legitimate transmitter to the eavesdropper is referred to as "wiretapping AoI", and the AoI of the legitimate link spanning from the legitimate transmitter to the intended receiver is referred to as "legitimate AoI".

TABLE I
CONTRASTING THE NOVELTY OF OUR WORK TO THE LITERATURE

Contribution	**This Work**	[5], [6]	[10]–[15]	[16]–[19]	[21]–[26], [29]–[33]	[27], [28]
Age of Information (AoI)	✓		✓	✓		✓
Finite-Blocklength Regime	✓			✓		
Wiretap Channels in the IoT	✓	✓			✓	✓
Permutation-Based Transmissions	✓	✓				
Secrecy Margin	✓					

TABLE II
LIST OF ACRONYMS

Acronym	Full Form
ACK	ACKnowledgement
AoI	Age of Information
ARQ	Automatic Repeat reQuest
AWGN	Additive White Gaussian Noise
con	conventional transport-layer encapsulation
CQI	Channel Quality Indicator
CRC	Cyclic Redundancy Check
DU	Data Unit
IoT	Internet of Things
LDPC	Low-Density Parity-Check
LoS	Line-of-Sight
pbt	permutation-based transmission
PCDU	Permutation-Conveyed Data Unit
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
SNR	Signal-to-Noise power Ratio
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URLLC	Ultra-Reliable and Low-Latency Communication

prompt delivery of status updates in the IoT. Finally, Section VI concludes this paper.

Throughout this paper, the acronyms listed in Table II and the following mathematical notations are used: $f_X(x)$ and $F_X(x)$ stand for the probability density function (pdf) and the cumulative distribution function (cdf) of a random variable X, respectively. Moreover, $Q[x] = \int_x^\infty (1/\sqrt{2\pi}) \exp(-t^2/2)dt$ is the Q-function, and $[x]^+$ stands for $\max(0, x)$. Besides, $\mathbb{E}(\cdot)$ denotes the expectation (mean) operator, and $\Pr[\,\cdot\,]$ denotes the probability of an event. In addition, $\mathbb{N}$ represents the set of all natural numbers, and $\mathbb{R}$ represents the set of all real numbers. The least integer function is denoted by $\lceil\cdot\rceil$.

II. System Model and Preliminaries

In this section, firstly the system model of status updates within a wiretap channel is presented. Then, the design of permutation-based transmissions and the information-theoretic analysis of short-packet communications in the finite-blocklength regime are introduced.

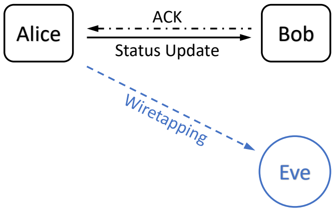


Fig. 1. The delivery of status updates in a wiretap channel.

A. Status Updates in a Wiretap Channel

Consider the IoT delivery architecture of status updates within a wiretap channel shown in Fig. 1, where the node Alice is monitoring and delivering status updates to the legitimate actuator Bob. Upon receiving a status update, Bob will decode and perform actions based on it. Meanwhile, the eavesdropper Eve is wiretapping Alice's transmissions and attempts to extract the status updates.

To guarantee the reliable delivery of status updates, the classic automatic repeat request (ARQ) mechanism is adopted in the legitimate link. For a given status update delivered from Alice to Bob, Bob will send an acknowledgement (ACK) to Alice once he successfully decodes the status update. The ACK triggers Alice to generate and commence the transmission of the next status update. If Alice does not receive an ACK before the predetermined timeout, she will retransmit the current status update until receiving an ACK.

The status updates are assumed to be independent of each other, so that Eve cannot utilise her decoded current or previous status updates to anticipate Bob's subsequent actions. In other words, the security of the IoT services is guaranteed as long as Bob decodes the status updates earlier than Eve does, since Bob can take appropriate actions before Eve correctly anticipates them.

As the majority of IoT infrastructures are deployed in rich scattering environments, there is no line-of-sight (LoS) component in the radio-frequency signal propagation and Rayleigh fading is the most applicable model for such a non-LoS scenario [34]. Herein, both the legitimate (Alice–Bob) and wiretapping (Alice–Eve) links are assumed to be Rayleigh fading channels, where the channel coefficients are modelled as random variables following a circularly-symmetric complex Gaussian distribution and, thus, their magnitudes are Rayleigh distributed. The magnitudes of legitimate and wiretapping channel coefficients are denoted by ξ_{B} and ξ_{E}, respectively.

The cdf of Rayleigh fading $\xi \in \{\xi_{\mathrm{B}}, \xi_{\mathrm{E}}\}$, i.e., the magnitude

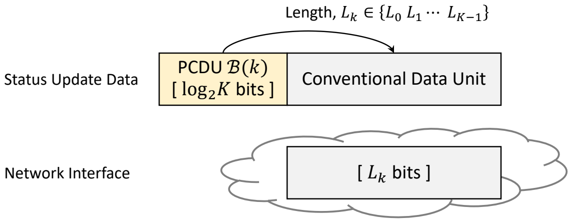


Fig. 2. The permutation-based encapsulation of a single status update at the transport layer of the legitimate link.

of a channel coefficient, is given by

$$F_\xi(x) = 1 - \exp(-x^2/G), \qquad \xi \geqslant 0, \tag{1}$$

where $G \in \{G_{\mathrm{B}}, G_{\mathrm{E}}\}$ is the variance of the legitimate or wiretapping channel coefficient, i.e., the average channel gain of the legitimate link, G_{B}, or of the wiretapping link, G_{E}.

For an arbitrary transmission, the received signal-to-noise power ratios (SNRs) at Bob and Eve are expressed as

$$\gamma_{\mathrm{B}} = \xi_{\mathrm{B}}^2 P_{\mathrm{A}}/\sigma^2 \tag{2}$$

and

$$\gamma_{\mathrm{E}} = \xi_{\mathrm{E}}^2 P_{\mathrm{A}}/\sigma^2, \tag{3}$$

respectively, where ξ_{B}^2 and ξ_{E}^2 are the channel gains of the links spanning from Alice to Bob and Eve, respectively. Moreover, Alice's transmit power is P_{A}, and the variance of additive white Gaussian noise (AWGN) is σ^2.

Substituting $\xi_{\mathrm{B}}^2 = \gamma_{\mathrm{B}}/(P_{\mathrm{A}}/\sigma^2)$ and $\xi_{\mathrm{E}}^2 = \gamma_{\mathrm{E}}/(P_{\mathrm{A}}/\sigma^2)$ into (1), we have the cdfs of the SNRs γ_{B} and γ_{E} given by

$$F_{\gamma_{\mathrm{B}}}(x) = \begin{cases} 1 - \exp\left(-x/\bar{\gamma}_{\mathrm{B}}\right), & x \geqslant 0, \\ 0, & x < 0, \end{cases} \tag{4}$$

and

$$F_{\gamma_{\mathrm{E}}}(x) = \begin{cases} 1 - \exp\left(-x/\bar{\gamma}_{\mathrm{E}}\right), & x \geqslant 0, \\ 0, & x < 0, \end{cases} \tag{5}$$

respectively. Elaborating slightly further, the received SNRs γ_{B} and γ_{E} follow the exponential distribution with means $\bar{\gamma}_{\mathrm{B}} = G_{\mathrm{B}} P_{\mathrm{A}}/\sigma^2$ and $\bar{\gamma}_{\mathrm{E}} = G_{\mathrm{E}} P_{\mathrm{A}}/\sigma^2$, respectively.

B. Permutation-Based Transmission

The permutation-based transport-layer design is proposed in our works [5] and [6] for improving the spectral efficiency of delivering the packets from a transmitter to a receiver. In this design, a portion of application-layer data, referred to as permutation-conveyed data unit (PCDU), is mapped onto the specific permutation associated with a legitimate tuple of various packet-lengths in a group, rather than being encapsulated into conventional DUs.

For prompt status updates, a permutation group at Alice consists of a single packet. The permutation-based encapsulation of a status update into a packet is presented in Fig. 2, where the status update data is divided into two portions for the delivery via a packet. The first portion is the PCDU of $\log_2 K$ bits, mapped onto assigning one of the K lengths $L_0, L_1, \cdots, L_{K-1}$ to the packet. The second portion, of the length determined by the first portion, is encapsulated into the packet in a conventional way and physically delivered through the network interface.

More specifically, our permutation-based design has $\log_2 K$ extra bits conveyed in a packet, compared with the conventional transport-layer encapsulation of the packet. In the network interface, Alice transmits the packet of length L_k, $k \in \{0, 1, \cdots, K-1\}$, conveying the PCDU through the selection of a particular one from a set of K various packet-lengths $L_0, L_1, \cdots, L_{K-1}$.

The K packet-lengths can be represented by an arithmetic sequence of $L_k = (M + kC)$ bits, $k = 0, 1, \cdots, K-1$, where the first term M is the shortest packet-length, and C is the common difference of successive lengths, $M, C \in \mathbb{N}$. The PCDU mapped onto the k^{th} length is calculated using $\mathcal{B}(k)$, where $\mathcal{B}(\cdot)$ stands for a $\log_2 K$-bit binary coded decimal function, and $k = 0, 1, \cdots, K-1$.

As each of the K packet-lengths is assumed to have the same probability of $1/K$, the mean length of a packet, in the unit of [bits], is obtained by

$$\bar{L} = \frac{1}{K} \sum_{k=0}^{K-1} L_k = M + \frac{(K-1)C}{2}. \tag{6}$$

In practice, the maximum packet-length, denoted by L_{max} in [bits], is determined by specific transport-layer protocols, e.g, the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), which leads to the limitation of

$$M + (K-1)C \leqslant L_{\text{max}}. \tag{7}$$

C. Short-Packet Communications

For short-packet communications within our permutation-based IoT design, the mean packet-length is $\bar{L}$, given in (6), which conveys a status update composed of $(\log_2 K + \bar{L})$ application-layer data bits. We remark that, with the conventional transport-layer encapsulation, a packet of length $\bar{L}$ conveys the status update composed of $\bar{L}$ application-layer data bits. Over the network interface, the coding rate is denoted by $R = \bar{L}/U \in (0, 1)$, where $U \in \mathbb{N}$ is the blocklength in the unit of physical channel uses.

In contrast to the infinite-blocklength regime rooted in Shannon's theory, where the optimal coding rate converges to the error-free channel capacity, short-packet communications suffer from decoding errors in the finite-blocklength regime. Herein, we adopt the normal approximation of the non-asymptotic bounds on the maximum number of information bits that can be encoded by the given blocklength U to formulate the expression of the maximal coding rate. The normal approximation obtained by [8, Eq. (296)] has been proven quite accurate when transmitting at a large fraction of channel capacity. On this basis, the maximal coding rate of permutation-based short-packet transmissions, R, in the finite-blocklength regime is expressed as

$$\bar{L}/U \approx \log_2(1+\gamma) - \frac{Q^{-1}(\epsilon)}{\ln 2} \sqrt{\frac{1-(1+\gamma)^{-2}}{U}} \tag{8}$$

at the packet error probability ϵ, where γ is the received SNR, and $Q^{-1}(\cdot)$ is the inverse function of $Q[x]$.

From (8), the packet error probability ϵ is formulated as

$$\begin{aligned}\epsilon &= Q\left[\frac{(\ln 2)\sqrt{U}\big(\log_2(1+\gamma)-\bar{L}/U\big)}{\sqrt{1-(1+\gamma)^{-2}}}\right]\\ &\triangleq Q\big[\theta(\bar{L},U,\gamma)\big], \end{aligned} \tag{9}$$

where the notation

$$\theta(\bar{L},U,\gamma) \triangleq \frac{(\ln 2)\sqrt{U}\big(\log_2(1+\gamma)-\bar{L}/U\big)}{\sqrt{1-(1+\gamma)^{-2}}}$$

is used for the simplicity of expression.

In a general block-fading channel, the average packet error probability is calculated using

$$\bar{\epsilon} = \int_0^{\infty} Q\big[\theta(\bar{L},U,x)\big] f_\gamma(x)\mathrm{d}x, \tag{10}$$

where $f_\gamma(x)$ is the pdf of the received SNR γ. A linear approximation of the Q-function $Q\big[\theta(\bar{L},U,x)\big]$ is validated in [19] and [35], expressed as

$$Q\big[\theta(\bar{L},U,x)\big] \approx \begin{cases} 1, & x \leqslant \mu-\nu, \\ \dfrac{1}{2}-\dfrac{x-\mu}{2\nu}, & \mu-\nu \leqslant x \leqslant \mu+\nu, \\ 0, & x \geqslant \mu+\nu, \end{cases} \tag{11}$$

given the parameters

$$\mu = 2^{\bar{L}/U}-1, \tag{12}$$

$$\nu = \sqrt{\pi(2^{2\bar{L}/U}-1)/(2U)}. \tag{13}$$

The linear approximation (11) is exploited to derive the closed-form expression of $\bar{\epsilon}$ through the calculation

$$\bar{\epsilon} = \frac{1}{2\nu}\int_{\mu-\nu}^{\mu+\nu} F_\gamma(x)\mathrm{d}x, \tag{14}$$

where $F_\gamma(x)$ is the cdf of the SNR γ.

III. Legitimate Age of Information

In this section, the metric of legitimate AoI is formulated to characterise the data freshness of status updates delivered by our permutation-based short-packet transmissions over the legitimate link, based on which the packet structure is optimised for minimising the legitimate AoI.

A. Formulation

An evolution of the legitimate AoI is illustrated in Fig. 3, where $\Delta(t)$ denotes the instantaneous AoI of the legitimate link, i.e. the time elapsed since Alice's generation of the latest status update that has been successfully decoded by Bob. If no status update is successfully decoded at Bob, the AoI increases linearly with time.

Alice generates and commences the transmission of the i^{th} status update at the time t_i^{A}, which is triggered by Bob's ACK on the $(i-1)^{\text{st}}$ status update. Bob successfully decodes the i^{th} status update at t_i^{B}. For simplicity, it is assumed that the ACK feedback from Bob to Alice requires no time, as the ACK duration is negligible in comparison to the retransmissions of a status update packet. More specifically, we have $t_i^{\text{B}} = t_{i+1}^{\text{A}}$, $i = 1, 2, \cdots$.

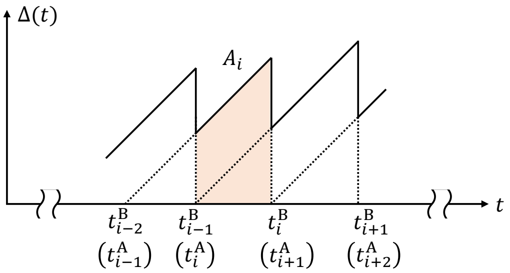


Fig. 3. An evolution of the legitimate AoI.

For the i^{th} status update to be decoded successfully, the number of total (re)transmissions requested by Bob is $K_{\text{B},i}$. Consequently, the time duration for Bob to successfully decode the i^{th} status update is

$$t_i^{\text{B}} - t_i^{\text{A}} = K_{\text{B},i}T, \tag{15}$$

where

$$T = U/W \tag{16}$$

is the time duration of a single transmission from Alice, with W denoting the bandwidth.

The number of (re)transmissions, $K_{\text{B},i}$, for the i^{th} status update requested by Bob, follows a Geometric distribution with the delivery success probability $(1-\bar{\epsilon}_{\text{B}})$, where $\bar{\epsilon}_{\text{B}}$ is the average packet error probability at Bob, obtained by substituting (4) into (14), i.e.,

$$\begin{aligned}\bar{\epsilon}_{\text{B}} &= \frac{1}{2\nu}\int_{\mu-\nu}^{\mu+\nu}\left[1-\exp\left(-x/\bar{\gamma}_{\text{B}}\right)\right]\mathrm{d}x\\ &= 1-\frac{\bar{\gamma}_{\text{B}}}{2\nu}\left[\exp\left(-\frac{\mu-\nu}{\bar{\gamma}_{\text{B}}}\right)-\exp\left(-\frac{\mu+\nu}{\bar{\gamma}_{\text{B}}}\right)\right], \end{aligned} \tag{17}$$

with $\bar{\gamma}_{\text{B}}$ denoting the mean received SNR at Bob.

Therefore, the mean and the second moment of the independent and identically distributed (i.i.d.) random variables $K_{\text{B},i}$, $i = 1, 2, \cdots$, are

$$\mathbb{E}(K_{\text{B}}) = \frac{1}{1-\bar{\epsilon}_{\text{B}}} \tag{18}$$

and

$$\mathbb{E}(K_{\text{B}}^2) = \frac{1+\bar{\epsilon}_{\text{B}}}{(1-\bar{\epsilon}_{\text{B}})^2}, \tag{19}$$

respectively, where the status update index i is omitted for the simplicity of expression.

In Fig. 3, the shaded area A_i under the (waiting plus) delivery time of the i^{th} status update decoded successfully at Bob is calculated using

$$\begin{aligned} A_i &= [(t_i^{\text{B}}-t_i^{\text{A}}) + 2(t_{i-1}^{\text{B}}-t_{i-1}^{\text{A}})](t_i^{\text{B}}-t_i^{\text{A}})/2 \qquad (20)\\ &= (K_{\text{B},i}T + K_{\text{B},i-1}T)K_{\text{B},i}T/2, \qquad (21)\end{aligned}$$

where $i = 1, 2, \cdots$ and (21) is obtained by substituting (15) into (20). Since the total number of (re)transmissions, $K_{\text{B},i}$, for the i^{th} status update, is independent of that for the $(i-1)^{\text{st}}$ status update, namely $K_{\text{B},i-1}$, the expectation of A_i is

$$\mathbb{E}(A) = \mathbb{E}(K_{\text{B}}^2)T^2/2 + [\mathbb{E}(K_{\text{B}})]^2T^2/2 \tag{22}$$

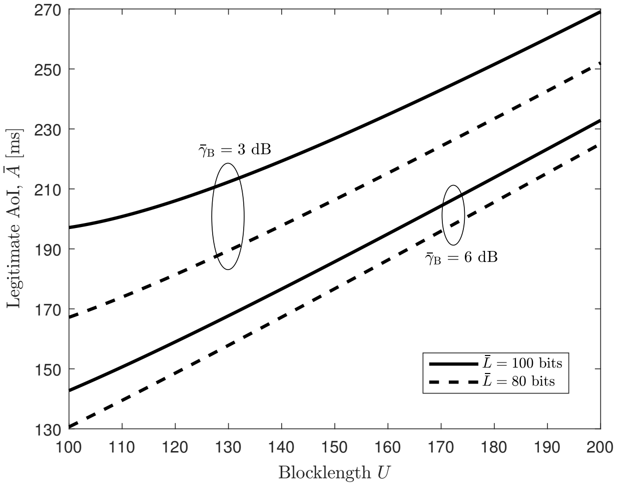


Fig. 4. The legitimate AoI $\bar{A}$ versus the blocklength U.

$$= \frac{(2+\bar{\epsilon}_{\rm B})T^2}{2(1-\bar{\epsilon}_{\rm B})^2}, \tag{23}$$

where (23) is obtained by substituting (18) and (19) into (22).

The average AoI of the legitimate link is defined as

$$\bar{A} = \lim_{t\to\infty} \frac{1}{t} \sum_{i=1}^{N(t)} A_i = \kappa \mathbb{E}(A), \tag{24}$$

where $N(t)$ is the number of status updates decoded successfully by Bob at time t and, thus, the rate of status updates decoded successfully at Bob is

$$\kappa = \lim_{t\to\infty} \frac{N(t)}{t} = \frac{1-\bar{\epsilon}_{\rm B}}{T}. \tag{25}$$

Upon substituting (23) and (25) into (24), we have the average AoI of the legitimate link expressed as

$$\bar{A} = \frac{(2+\bar{\epsilon}_{\rm B})T}{2(1-\bar{\epsilon}_{\rm B})}, \tag{26}$$

where Bob's average packet error probability $\bar{\epsilon}_{\rm B}$ is given by (17).

The average AoI of the legitimate link, $\bar{A}$, is plotted as a function of the blocklength U in Fig. 4, where the bandwidth is $W = 1$ kHz. As shown in this figure, the legitimate AoI is reduced upon decreasing the average packet-length $\bar{L}$ of a status update, or increasing Bob's received SNR $\bar{\gamma}_{\rm B}$. The main reason behind this trend can be found from the expression of $\bar{A}$.

The substitution of (16) into (26) yields the average AoI $\bar{A}$ written as the product of two items:

$$\bar{A} = \bar{A}_1 \bar{A}_2, \tag{27}$$

where

$$\bar{A}_1 = \frac{U}{2W}$$

and

$$\bar{A}_2 = \frac{2+\bar{\epsilon}_{\rm B}}{1-\bar{\epsilon}_{\rm B}}.$$

Obviously, the item $\bar{A}_2$ is reduced as the average packet error probability $\bar{\epsilon}_{\rm B}$ decreases. Given a blocklength U, the lower coding rate $\bar{L}/U$ due to the shorter packet-length $\bar{L}$ of a status update, or the higher received SNR $\bar{\gamma}_{\rm B}$ leads to a lower packet error probability $\bar{\epsilon}_{\rm B}$. As a result, the legitimate AoI $\bar{A}$ is reduced as $\bar{L}$ decreases or $\bar{\gamma}_{\rm B}$ increases.

B. Optimisation

Since the average packet-length $\bar{L}$ is determined by the upper-layer design for our permutation-based transmissions and Bob's received SNR $\bar{\gamma}_{\rm B}$ is determined by the channel condition of the legitimate link, the legitimate AoI is expressed as a function of the blocklength, denoted by $\bar{A}(U)$. Next, we will seek the optimal U^* for minimising the legitimate AoI.

Upon decreasing U, the item $\bar{A}_1 = U/(2W)$ in (27) is reduced. However, given the packet-length $\bar{L}$, a shorter blocklength U results in a higher coding rate $\bar{L}/U$ and, thereby, causes a higher packet error probability $\bar{\epsilon}_{\rm B}$, which eventually increases the item $\bar{A}_2$ in (27). The monotonicity of the function $\bar{A}(U)$ is verified in the following lemma, via relaxing the constraint $U \in \mathbb{N}$ and allowing the variable U to take real values, i.e., $U \in \mathbb{R}$.

Lemma 1. *The function*

$$\bar{A}(U) = \frac{[2+\bar{\epsilon}_{\rm B}(U)]U}{2[1-\bar{\epsilon}_{\rm B}(U)]W} \tag{28}$$

exhibits a monotonically increasing tendency versus U, where $\bar{\epsilon}_{\rm B}(U)$ is obtained by substituting (12) and (13) into (17).

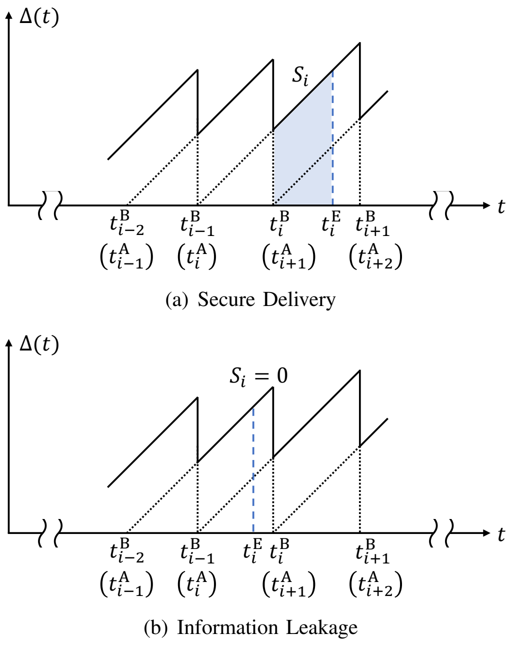
Proof: See Appendix A. ■

Both Lemma 1 and Fig. 4 reveal that the average AoI $\bar{A}$ is reduced upon decreasing the blocklength U. More specifically, for the purpose of legitimate AoI minimisation, the optimal blocklength is formulated as

$$\begin{aligned} U^* &= \mathop{\arg\min}_{U\in[U_{\min},U_{\max}]} \bar{A}(U) \\ &= U_{\min}, \end{aligned} \tag{29}$$

where the function $\bar{A}(U)$ is given by (28). The minimum blocklength $U_{\min}$ and the maximum blocklength $U_{\max}$ are determined by the specific physical-layer protocols. For example, in the 5G New Radio, a slot is composed of 14 symbols, and a mini-slot is comprised of 2, 4, or 7 symbols allocated for shorter transmissions [36]. The downlink control information is transmitted using quadrature phase shift keying (QPSK) and polar coding [37], where the minimum blocklength is $U_{\min} = 28$ bits in a slot and $U_{\min} = 4$ bits in a mini-slot. For the downlink data transmission and the uplink data/control transmission, quadrature amplitude modulation (QAM) orders are up to 256 and the low-density parity-check (LDPC) codes are used [37], where the minimum blocklength is $U_{\min} = 112$ bits in a slot and $U_{\min} = 16$ bits in a mini-slot. As the slots can be aggregated for longer transmissions, the maximum blocklength will be specified by the congestion control window or the transceiver's buffer size.

In addition, the coding rate $\bar{L}/U$ is prescribed by the adopted channel coding scheme, i.e., polar coding or LDPC.


$\Delta(t)$
S_i
t
t^{B}_{i-2} (t^{A}_{i-1})
t^{B}_{i-1} (t^{A}_{i})
t^{B}_{i} (t^{A}_{i+1})
t^{E}_{i}
t^{B}_{i+1} (t^{A}_{i+2})
$\Delta(t)$
$S_i = 0$
t
t^{B}_{i-2} (t^{A}_{i-1})
t^{B}_{i-1} (t^{A}_{i})
t^{E}_{i} t^{B}_{i} (t^{A}_{i+1})
t^{B}_{i+1} (t^{A}_{i+2})

(a) Secure Delivery

(b) Information Leakage

Fig. 5. An illustration of the secrecy margin.

Given the transport-layer packet-length $\bar{L}$, a higher coding rate is preferred so as to get a shorter blocklength for reducing the legitimate AoI. From the AoI perspective, the optimal blocklength balances the tradeoff between the latency of a single transmission and the total number of (re)transmissions. The solution (29) indicates that, in the legitimate AoI reduction, the contribution from the shorter latency of a single transmission dominates that from less (re)transmissions due to a higher packet error probability.

IV. Secrecy Margin

Based on the AoI framework, the metric of secrecy margin is developed in this section for characterising the data security of status updates, given that the data freshness has been guaranteed by minimising the legitimate AoI using our permutation-based short-packet transmissions.

A. Formulation

The secrecy margin is exemplified in Fig. 5, where Alice generates and commences the transmission of the i^{th} status update at the time t_i^{A}. Bob and Eve successfully decode the i^{th} status update at t_i^{B} and t_i^{E}, respectively. In Fig. 5(a), the secure delivery of the i^{th} status update is guaranteed, since Eve successfully decodes the i^{th} status update later than Bob does, i.e. $t_i^{\mathrm{E}} > t_i^{\mathrm{B}}$. In other words, Eve needs more retransmissions of the i^{th} status update than Bob does for successful decoding. However, Alice will not transmit this status update any more upon receiving Bob's ACK. This prevents Eve from unveiling this status update, thus leading to a secure delivery. In Fig. 5(b), Eve successfully decodes the i^{th} status update earlier than Bob does, i.e., $t_i^{\mathrm{E}} < t_i^{\mathrm{B}}$, where an information leakage of the i^{th} status update occurs because the wiretapping link is better than the legitimate one.

For the i^{th} status update to be decoded successfully, Eve would need $K_{\mathrm{E},i}$ (re)transmissions. That is, the time duration for Eve to unveil the i^{th} status update can be expressed as

$$t_i^{\mathrm{E}} - t_i^{\mathrm{A}} = K_{\mathrm{E},i} T, \tag{30}$$

where T is given by (16).

As shown in Fig. 5(a), the secrecy of the i^{th} status update is guaranteed if its successful delivery to Eve occurs later than that to Bob, i.e., the time durations obey $K_{\mathrm{E},i}T > K_{\mathrm{B},i}T$, where $K_{\mathrm{B},i}T$ is the time duration for Bob to successfully decode the i^{th} status update, given by (15).

The secrecy margin of the i^{th} status update is defined as the positive difference between the time durations for Eve and Bob to successfully decode this status update, denoted by

$$[t_i^{\mathrm{E}} - t_i^{\mathrm{B}}]^+ = [K_{\mathrm{E},i}T - K_{\mathrm{B},i}T]^+. \tag{31}$$

Then, the average secrecy margin of the wiretap channel under study is expressed as

$$\bar{S} = \lim_{t\to\infty} \frac{1}{t} \sum_{i=1}^{N(t)} S_i, \tag{32}$$

where $N(t)$ is the number of status updates decoded successfully by Bob at time t, and S_i, marked by the shaded area in Fig. 5(a), is the right trapezoid area under the secrecy margin of the i^{th} status update. Note that, $S_i = 0$ if $t_i^{\mathrm{E}} < t_i^{\mathrm{B}}$, as shown in Fig. 5(b).

Subsequently, the secrecy indicator of the i^{th} status update is introduced as

$$\eta_i = \begin{cases} 1, & S_i \neq 0, \\ 0, & S_i = 0, \end{cases} \tag{33}$$

and the cumulative number of secure status updates at time t is thus expressed as

$$N_{\mathrm{S}}(t) = \sum_{i=1}^{N(t)} \eta_i. \tag{34}$$

As such, the average secrecy margin, defined in (32), can be calculated using

$$\bar{S} = \lim_{t\to\infty} \frac{N_{\mathrm{S}}(t)}{t} \mathbb{E}(S) = \lambda \mathbb{E}(S), \tag{35}$$

where

$$\lambda = \lim_{t\to\infty} \frac{N_{\mathrm{S}}(t)}{t} \tag{36}$$

is defined as the rate of secure delivery from Alice to Bob, and $\mathbb{E}(S)$ denotes the expectation of S_i, omitting the status update index i, because S_i, $i = 1, 2, \cdots$, are i.i.d. random variables from the ergodic perspective.

We will now investigate the average secrecy margin in the finite-blocklength regime for permutation-based short-packet transmissions, via the formulations of $\mathbb{E}(S)$ and λ in (35).

In Fig. 5(a), the shaded area S_i under the secrecy margin of the i^{th} status update is written as

$$\begin{aligned} S_i &= [(t_i^{\mathrm{B}} - t_i^{\mathrm{A}}) + (t_i^{\mathrm{E}} - t_i^{\mathrm{A}})](t_i^{\mathrm{E}} - t_i^{\mathrm{B}})/2 \qquad (37) \\ &= (K_{\mathrm{B},i}T + K_{\mathrm{E},i}T)(K_{\mathrm{E},i}T - K_{\mathrm{B},i}T)/2 \qquad (38) \end{aligned}$$

$$= (K_{\mathrm{E},i}^2 - K_{\mathrm{B},i}^2)T^2/2, \tag{39}$$

where (38) is obtained by substituting (15), (30) and (31) into (37).

Similar to the statistics of $K_{\mathrm{B},i}$ given in (18) and (19), the number of (re)transmissions Eve would need for unveiling the i^{th} status update, namely $K_{\mathrm{E},i}$, follows a Geometric distribution with the delivery success probability $(1-\bar{\epsilon}_{\mathrm{E}})$, where $\bar{\epsilon}_{\mathrm{E}}$ is the average packet error probability at Eve, calculated by substituting (5) into (14), i.e.,

$$\begin{aligned}\bar{\epsilon}_{\mathrm{E}} &= \frac{1}{2\nu}\int_{\mu-\nu}^{\mu+\nu}\left[1-\exp\left(-x/\bar{\gamma}_{\mathrm{E}}\right)\right]\mathrm{d}x \\ &= 1-\frac{\bar{\gamma}_{\mathrm{E}}}{2\nu}\left[\exp\left(-\frac{\mu-\nu}{\bar{\gamma}_{\mathrm{E}}}\right)-\exp\left(-\frac{\mu+\nu}{\bar{\gamma}_{\mathrm{E}}}\right)\right], \end{aligned}\tag{40}$$

with $\bar{\gamma}_{\mathrm{E}}$ denoting the mean received SNR at Eve.

Therefore, the mean and the second moment of the i.i.d. random variables $K_{\mathrm{E},i}$, $i = 1, 2, \cdots$, are

$$\mathbb{E}(K_{\mathrm{E}}) = \frac{1}{1-\bar{\epsilon}_{\mathrm{E}}} \tag{41}$$

and

$$\mathbb{E}(K_{\mathrm{E}}^2) = \frac{1+\bar{\epsilon}_{\mathrm{E}}}{(1-\bar{\epsilon}_{\mathrm{E}})^2}, \tag{42}$$

respectively, where the status update index i is omitted for simplicity.

As a result, the expectation of S_i is expressed as

$$\begin{aligned}\mathbb{E}(S) &= \mathbb{E}(K_{\mathrm{E}}^2)T^2/2 - \mathbb{E}(K_{\mathrm{B}}^2)T^2/2 \\ &= \frac{(1+\bar{\epsilon}_{\mathrm{E}})T^2}{2(1-\bar{\epsilon}_{\mathrm{E}})^2} - \frac{(1+\bar{\epsilon}_{\mathrm{B}})T^2}{2(1-\bar{\epsilon}_{\mathrm{B}})^2}. \end{aligned}\tag{43}$$

Moreover, the rate of secure delivery from Alice to Bob, i.e., λ defined by (36), is formulated as

$$\lambda = \frac{\Pr[K_{\mathrm{B}} < K_{\mathrm{E}}]}{\mathbb{E}(K_{\mathrm{B}})T} = \frac{1-\bar{\epsilon}_{\mathrm{B}}}{T}\Pr[K_{\mathrm{B}} < K_{\mathrm{E}}], \tag{44}$$

where we have

$$\begin{aligned}\Pr[K_{\mathrm{B}} < K_{\mathrm{E}}] &= \sum_{k=1}^{\infty}(1-\bar{\epsilon}_{\mathrm{B}}^k)\bar{\epsilon}_{\mathrm{E}}^k \\ &= \frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}} - \frac{\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}. \end{aligned}\tag{45}$$

The substitution of (43) and (44) into (35) leads to the average secrecy margin expressed as

$$\begin{aligned}\bar{S} = \frac{T}{2}&\left[\frac{(1+\bar{\epsilon}_{\mathrm{E}})(1-\bar{\epsilon}_{\mathrm{B}})}{(1-\bar{\epsilon}_{\mathrm{E}})^2} - \frac{1+\bar{\epsilon}_{\mathrm{B}}}{1-\bar{\epsilon}_{\mathrm{B}}}\right] \\ &\times\left(\frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}} - \frac{\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}\right), \end{aligned}\tag{46}$$

where the average packet error probabilities at Bob and Eve, namely $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$, are given by (17) and (40), respectively.

The average secrecy margin, $\bar{S}$ given by (46), is plotted as a function of the blocklength U in Fig. 6, where the bandwidth is $W = 1$ kHz. As shown in this figure, the average secrecy margin $\bar{S}$ is improved with the increase in the average packet-length $\bar{L}$ of a status update, or with the decrease of the received SNRs $\bar{\gamma}_{\mathrm{B}}$ and $\bar{\gamma}_{\mathrm{E}}$. The main reason behind this can be observed from the expression of $\bar{S}$.

Based on (16) and (46), the average secrecy margin $\bar{S}$ can be written as the product of two items:

$$\bar{S} = \bar{S}_1\bar{S}_2, \tag{47}$$

where

$$\bar{S}_1 = \frac{U}{2W}$$

is determined by the blocklength U only, and

$$\bar{S}_2 = \left[\frac{(1+\bar{\epsilon}_{\mathrm{E}})(1-\bar{\epsilon}_{\mathrm{B}})}{(1-\bar{\epsilon}_{\mathrm{E}})(1-\bar{\epsilon}_{\mathrm{E}})} - \frac{1+\bar{\epsilon}_{\mathrm{B}}}{1-\bar{\epsilon}_{\mathrm{B}}}\right]\left(\frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}} - \frac{\bar{\epsilon}_{\mathrm{E}}}{1/\bar{\epsilon}_{\mathrm{B}}-\bar{\epsilon}_{\mathrm{E}}}\right)$$

is determined by the average packet error probabilities $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$. As $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$ increase, the item $\bar{S}_2$ will increase. Given a blocklength U, the higher coding rate $\bar{L}/U$ due to the longer packet-length $\bar{L}$ of a status update, or the lower received SNRs $\bar{\gamma}_{\mathrm{B}}$ and $\bar{\gamma}_{\mathrm{E}}$ will result in higher packet error probabilities $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$. Therefore, $\bar{S}$ is improved as the packet-length increases or as the SNRs decrease.

In addition, by comparing Figs. 6(a) and 6(b), we observe that the average secrecy margin $\bar{S}$ is improved as the ratio $\bar{\gamma}_{\mathrm{B}}/\bar{\gamma}_{\mathrm{E}}$ increases. This is because a higher ratio $\bar{\gamma}_{\mathrm{B}}/\bar{\gamma}_{\mathrm{E}}$ enlarges the difference between the packet error probabilities $\bar{\epsilon}_{\mathrm{E}}$ and $\bar{\epsilon}_{\mathrm{B}}$, thus leading to a higher difference between the wiretapping AoI and the legitimate AoI as well as a higher probability $\Pr[K_{\mathrm{B}} < K_{\mathrm{E}}]$.

B. Optimisation

As shown in (47), the average secrecy margin $\bar{S}$ depends both on the blocklength U and on the average packet error probabilities $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$. As seen in (17) and (40), $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$ depend on the received SNRs $\bar{\gamma}_{\mathrm{B}}$ and $\bar{\gamma}_{\mathrm{E}}$, respectively, in addition to the average packet-length $\bar{L}$ of a status update and the blocklength U. Naturally, the received SNRs $\bar{\gamma}_{\mathrm{B}}$ and $\bar{\gamma}_{\mathrm{E}}$ are determined by the channel conditions, while the average packet-length $\bar{L}$ is determined by the upper-layer design of our permutation-based transmissions. Therefore, the average secrecy margin, denoted by $\bar{S}(U)$, is a function of the blocklength U over the network interface, and we seek the optimal U^* for maximising the secrecy margin.

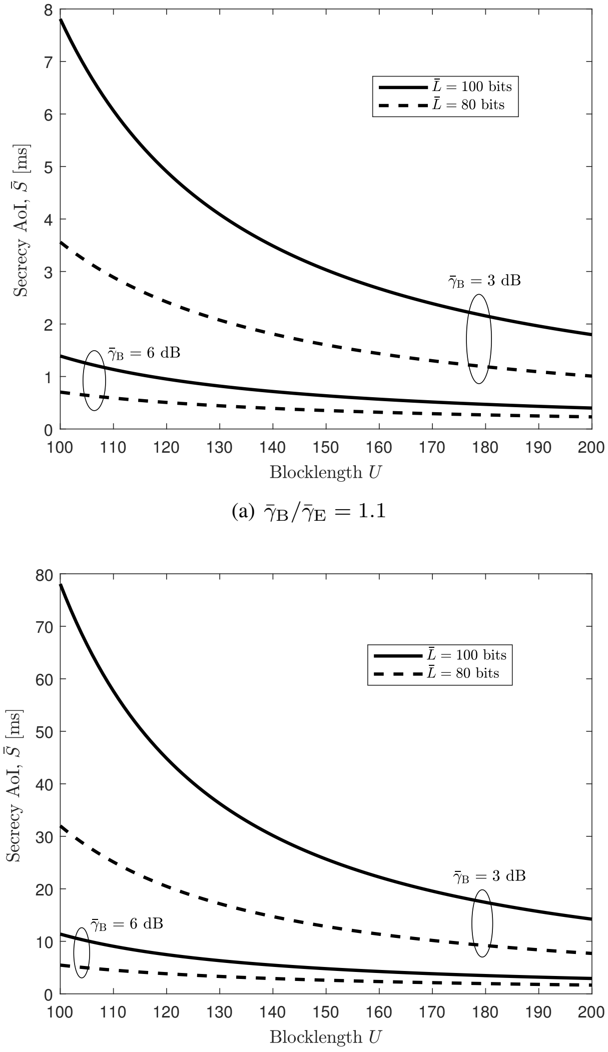
As U increases, the item $\bar{S}_1 = U/(2W)$ in (47) is increased. However, given the packet-length $\bar{L}$, a longer blocklength U reduces the coding rate $\bar{L}/U$, hence reducing the packet error probabilities $\bar{\epsilon}_{\mathrm{B}}$ and $\bar{\epsilon}_{\mathrm{E}}$, which accordingly reduces the item $\bar{S}_2$ in (47).

In the following lemma, the monotonicity of the function $\bar{S}(U)$ is verified through relaxing the constraint $U \in \mathbb{N}$ and allowing the variable U to take real values, i.e., $U \in \mathbb{R}$.

Lemma 2. *The function*

$$\begin{aligned}\bar{S}(U) = \frac{U}{2W}&\left(\frac{[1+\bar{\epsilon}_{\mathrm{E}}(U)][1-\bar{\epsilon}_{\mathrm{B}}(U)]}{[1-\bar{\epsilon}_{\mathrm{E}}(U)]^2} - \frac{1+\bar{\epsilon}_{\mathrm{B}}(U)}{1-\bar{\epsilon}_{\mathrm{B}}(U)}\right) \\ &\times\left(\frac{\bar{\epsilon}_{\mathrm{E}}(U)}{1-\bar{\epsilon}_{\mathrm{E}}(U)} - \frac{\bar{\epsilon}_{\mathrm{B}}(U)\bar{\epsilon}_{\mathrm{E}}(U)}{1-\bar{\epsilon}_{\mathrm{B}}(U)\bar{\epsilon}_{\mathrm{E}}(U)}\right) \end{aligned}\tag{48}$$

exhibits a monotonically decreasing tendency versus U, where $\bar{\epsilon}_{\mathrm{E}}(U)$ is obtained by substituting (12) and (13) into (40), and $\bar{\epsilon}_{\mathrm{B}}(U)$ is obtained by substituting (12) and (13) into (17).



(a) $\bar{\gamma}_{\mathrm{B}}/\bar{\gamma}_{\mathrm{E}} = 1.1$

(b) $\bar{\gamma}_{\mathrm{B}}/\bar{\gamma}_{\mathrm{E}} = 1.5$

Fig. 6. The secrecy margin $\bar{S}$ versus the blocklength U.

Proof: See Appendix B. ■

According to Lemma 2, a shorter blocklength U leads to a higher secrecy margin $\bar{S}$, which agrees with the trends observed in Fig. 6. More specifically, for the sake of average secrecy margin maximisation, the optimal blocklength is obtained by

$$\begin{aligned} U^* &= \underset{U \in [U_{\min}, U_{\max}]}{\arg\max} \; \bar{S}(U) \\ &= U_{\min}, \end{aligned} \tag{49}$$

where the function $\bar{S}(U)$ is given by (48).

As shown in (29) and (49), the optimal blocklength $U^* = U_{\min}$ not only minimises the legitimate AoI but also maximises the secrecy margin. The optimal solution (49) implies that, in the secrecy margin maximisation, the shorter transmission duration makes a better contribution than having fewer (re)transmissions. In other words, the shorter transmission duration is more likely to protect the status updates against the eavesdroppers' wiretapping, compared to using less (re)transmissions.

V. Performance Gains of Permutation-Based Transmission

To deliver a given number of application-layer data bits, the average packet-length $\bar{L}$ required by our permutation-based transmission is $\log_2 K$ bits shorter than that of the conventional transport-layer encapsulation. This is because the PCDU of $\log_2 K$ bits is not physically encapsulated into the packet but conveyed implicitly through the packet-length permutations.

In this section, the security and timeliness of our permutation-based transmission and of the conventional transport-layer encapsulation are compared in terms of their secrecy margin and legitimate AoI. To begin with, the scenario using optimal packet structure is investigated. Then, the scenario using fixed blocklength is investigated, where the permutation-based transmission utilises lower coding rate than the conventional transport-layer encapsulation to deliver the same application-layer data.

The default parameters in the IoT are set as follows:

- The network's bandwidth is $W = 1$ kHz, and the legitimate link SNR is 1.5 times higher than the wiretapping link SNR, i.e., $\bar{\gamma}_{\mathrm{B}}/\bar{\gamma}_{\mathrm{E}} = 1.5$.
- The average packet-length of a status update in our permutation-based transmissions is $\bar{L} = (K-1)C/2+M$, conveying $\bar{L} + \log_2 K$ application-layer data bits, where K is the number of legitimate packet-lengths, C is the common difference between the successive lengths, and M is the shortest packet-length.
- The packet-length of a status update in the conventional transport-layer encapsulation is $\bar{L} + \log_2 K$, which conveys the same amount of application-layer data as our permutation-based transmission.

A. Optimal Blocklength

Given the same coding rate $R \in (0,1)$, the optimal blocklength for our permutation-based transmission (pbt) is $U^*_{\mathrm{pbt}} = \lceil \bar{L}/R \rceil$, and that for the conventional (con) transport-layer encapsulation is $U^*_{\mathrm{con}} = \lceil (\bar{L} + \log_2 K)/R \rceil$.

According to Lemma 1 and Lemma 2 as well as Figs. 4 and 6, a shorter blocklength U will lead to higher secrecy margin and lower legitimate AoI. Thus, permutation-based transmissions enhance the security and timeliness of status updates within wiretap channels. Given that $U^*_{\mathrm{pbt}} < U^*_{\mathrm{con}}$ for the delivery of the same application-layer data contained in each status update, the average secrecy margin $\bar{S}_{\mathrm{pbt}}$ of our permutation-based transmission is higher than that of the conventional transport-layer encapsulation, denoted by $\bar{S}_{\mathrm{con}}$, and the average legitimate AoI $\bar{A}_{\mathrm{pbt}}$ of our permutation-based transmission is lower than that of the conventional transport-layer encapsulation, denoted by $\bar{A}_{\mathrm{con}}$, as it transpires from Lemma 1 and Lemma 2.

To elaborate, a higher secrecy margin indicates better security for the delivery of status updates within wiretap channels,

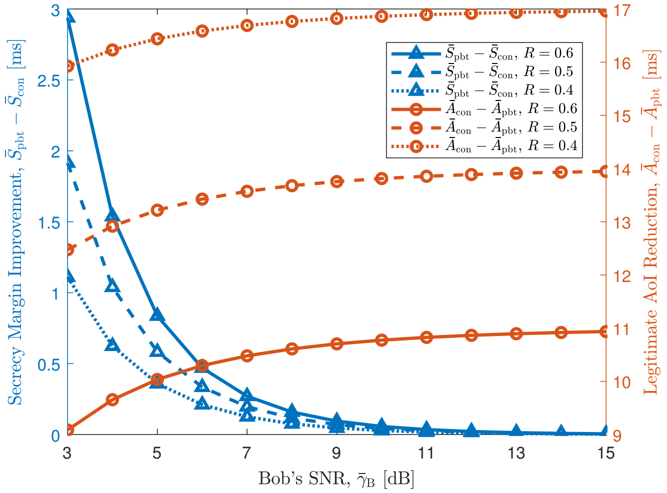
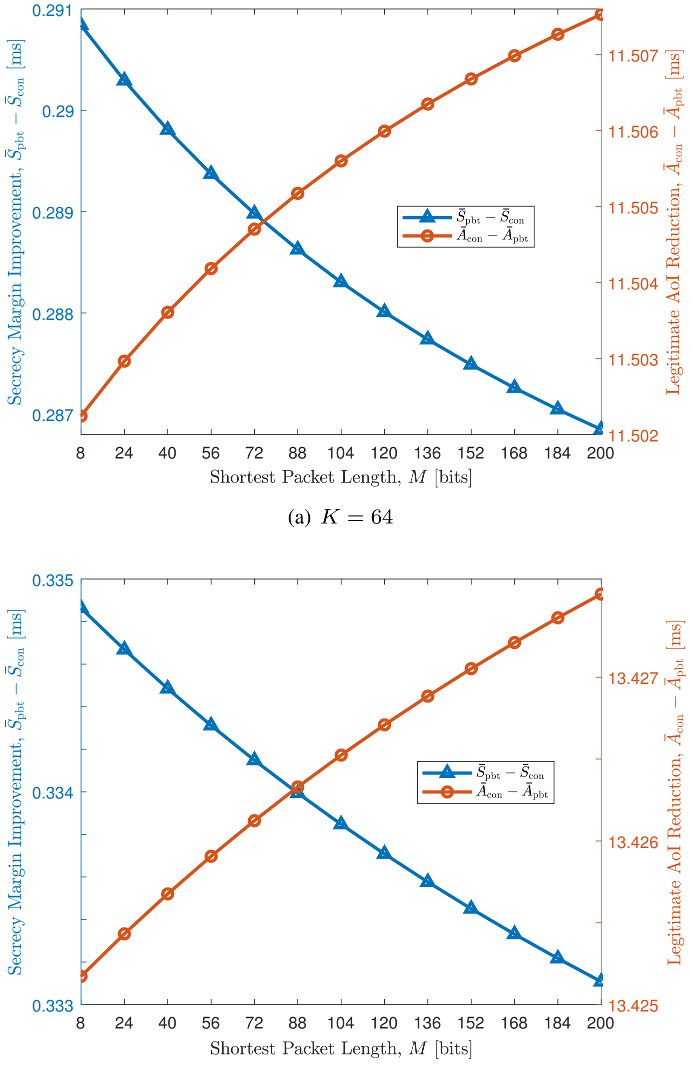


Fig. 7. The secrecy margin improvement $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ and the legitimate AoI reduction $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ versus Bob's received SNR $\bar{\gamma}_{\rm B}$, for fixed coding rate R with $K=128$, $M=32$, $C=8$.

while a lower legitimate AoI indicates better timeliness. Therefore, the security performance gain of our permutation-based transmission over the conventional transport-layer encapsulation is quantified in terms of the secrecy margin improvement $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$. By contrast, the AoI performance gain is quantified by the legitimate AoI reduction $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$.

In Fig. 7, the performance gains $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ and $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ are plotted versus Bob's received SNR $\bar{\gamma}_{\rm B}$, where $K=128$, $M=32$, $C=8$. This figure reveals that, given the amount of application-layer data to be delivered for a status update, i.e., $(K-1)C/2+M+\log_2 K$ bits, the secrecy margin improvement, $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$, is reduced and converges to 0 as the legitimate link SNR $\bar{\gamma}_{\rm B}$ increases. The main reason behind this is that, given $\bar{\gamma}_{\rm E}=\bar{\gamma}_{\rm B}/1.5$, the average packet error probabilities tend to $\bar{\epsilon}_{\rm B}=\bar{\epsilon}_{\rm E}=0$ when $\bar{\gamma}_{\rm B}$ goes to infinity. As such, both $\bar{S}_{\rm pbt}$ and $\bar{S}_{\rm con}$ approach 0 as $\bar{\gamma}_{\rm B}$ increases. On the other hand, given the coding rate R, the legitimate AoI reduction $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ increases and gradually saturates as $\bar{\gamma}_{\rm B}$ increases. This is because, when $\bar{\epsilon}_{\rm B}=0$, the legitimate AoI is the time duration of a single transmission from Alice. Hence, the legitimate AoI reduction $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ converges to the difference of a single transmission duration between using our permutation-based scheme and using the conventional encapsulation. Moreover, as the coding rate R increases, $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ is increased, while $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ is reduced. This indicates that, with the increase in R, the security improvement of our permutation-based transmission over the conventional encapsulation becomes more substantial. By contrast, its delivery latency of status updates is degraded.

In addition, the impact of the shortest packet-length M and the number of available packet-lengths, K, on $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ and $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ is investigated in Fig. 8, where $C=8$, $R=0.5$, $\bar{\gamma}_{\rm B}=6$ dB. We observe that, the secrecy margin improvement $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ gets smaller, while $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ gets slightly larger as M increases. The main reason behind this is that, the average packet-length of a status update, $\bar{L}$, gets longer with the increase of the shortest packet-length M. At the same time, the contribution of the blocklength reduction $U^*_{\rm con}-U^*_{\rm pbt}$ becomes less influential in comparison to the conventional scheme's blocklength $U^*_{\rm con}$. As seen in Fig. 6, the negative slope of the secrecy margin $\bar{S}(U)$ becomes steeper as $\bar{L}$ increases. Hence, the blocklength reduction cannot compensate for the reduction in the secrecy margin. By contrast, as shown in Fig. 4, the positive slope of the legitimate AoI $\bar{A}(U)$ is slightly reduced as $\bar{L}$ is increased from 80 to 100. Furthermore, by comparing Fig. 8(a) and Fig. 8(b), we find that both $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ and $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ are increased as K increases. This is because the number of available packet-lengths, K, is the very character that contributes to the blocklength reduction upon using our permutation-based transmission.



(a) $K=64$

(b) $K=128$

Fig. 8. The secrecy margin improvement $\bar{S}_{\rm pbt}-\bar{S}_{\rm con}$ and the legitimate AoI reduction $\bar{A}_{\rm con}-\bar{A}_{\rm pbt}$ versus the shortest packet-length M, for the fixed coding rate $R=0.5$ with $C=8$ and $\bar{\gamma}_{\rm B}=6$ dB.

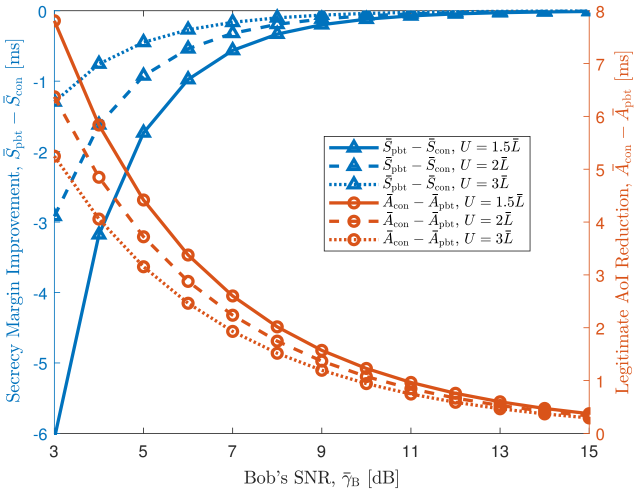


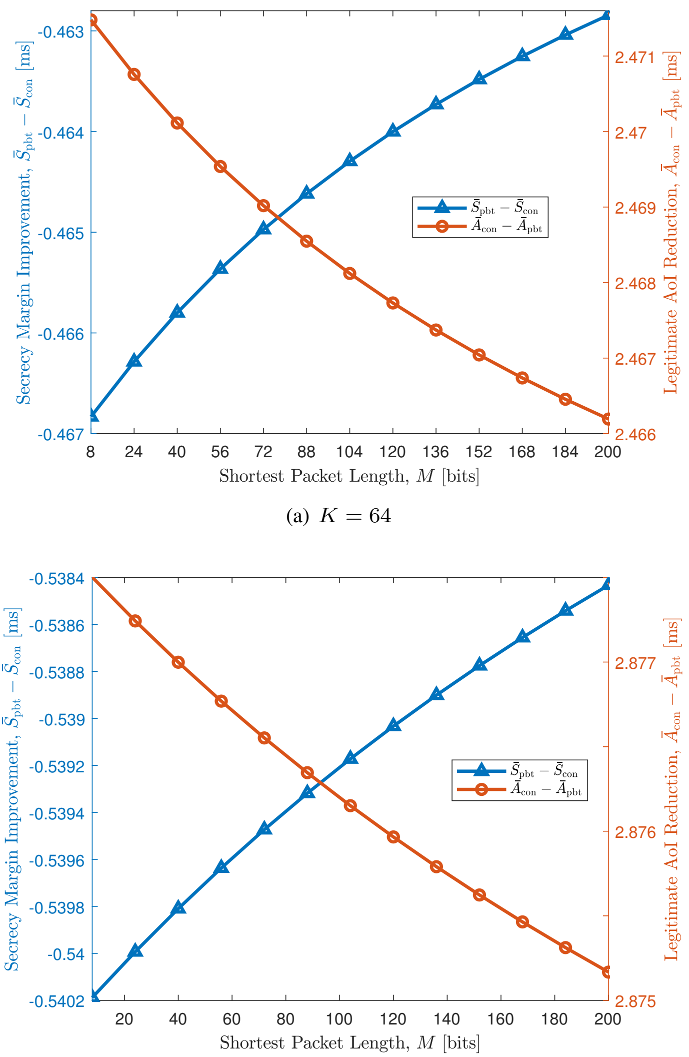
Fig. 9. The secrecy margin improvement $\bar{S}_{\mathrm{pbt}} - \bar{S}_{\mathrm{con}}$ and the legitimate AoI reduction $\bar{A}_{\mathrm{con}} - \bar{A}_{\mathrm{pbt}}$ versus Bob's received SNR $\bar{\gamma}_{\mathrm{B}}$, for fixed blocklength U with $K = 128$, $M = 32$, $C = 8$.

B. Fixed Blocklength

To deliver the same application-layer data of $\bar{L} + \log_2 K$ bits using the same blocklength U, the coding rate of permutation-based transmissions is $\bar{L}/U$ while the coding rate of conventional transport-layer encapsulation is $(\bar{L} + \log_2 K)/U$.

In this scenario, Fig. 9 plots $\bar{S}_{\mathrm{pbt}} - \bar{S}_{\mathrm{con}}$ and $\bar{A}_{\mathrm{con}} - \bar{A}_{\mathrm{pbt}}$ versus Bob's SNR $\bar{\gamma}_{\mathrm{B}}$, with $K = 128$, $M = 32$, $C = 8$. As shown in this figure, using fixed blocklength, the permutation-based transmission is still superior to conventional transport-layer encapsulation in terms of legitimate AoI, but it is inferior in terms of security margin. According to (29) and (49), the shorter latency of a single transmission has more contribution than using less (re)transmissions, to both the legitimate AoI reduction and the secrecy margin improvement. Therefore, using the same blocklength U, the legitimate AoI difference between the permutation-based and conventional schemes solely arises from the packet error probability difference. As the SNR increases, the packet error probability decreases, which causes the decay in $\bar{A}_{\mathrm{con}} - \bar{A}_{\mathrm{pbt}}$. For the secrecy margin, the higher coding rate in the conventional scheme generates higher error probability and more (re)transmissions, which therefore results in a longer AoI in both the legitimate link and the wiretapping link. As such, $\bar{S}_{\mathrm{con}} > \bar{S}_{\mathrm{pbt}}$ and the difference between them gets smaller with the decrease in the error probability, i.e., with the increase in the SNR.

Furthermore, Fig. 10 depicts $\bar{S}_{\mathrm{pbt}} - \bar{S}_{\mathrm{con}}$ and $\bar{A}_{\mathrm{con}} - \bar{A}_{\mathrm{pbt}}$ versus the shortest packet-length M, where $K = 64, 128$, $C = 8$, $\bar{\gamma}_{\mathrm{B}} = 6$ dB, and the fixed blocklength $U = 2\bar{L}$. As shown in this figure, a longer packet-length results in less legitimate AoI reduction. The main reason behind this is that the difference between the permutation-based coding rate $(M + (K-1)C/2)/U$ and the conventional coding rate $(M + (K-1)C/2 + \log_2 K)/U$ gets smaller as M increases.



(a) $K = 64$

(b) $K = 128$

Fig. 10. The secrecy margin improvement $\bar{S}_{\mathrm{pbt}} - \bar{S}_{\mathrm{con}}$ and the legitimate AoI reduction $\bar{A}_{\mathrm{con}} - \bar{A}_{\mathrm{pbt}}$ versus the shortest packet-length M, for the fixed blocklength $U = 2\bar{L}$ with $C = 8$ and $\bar{\gamma}_{\mathrm{B}} = 6$ dB.

VI. Conclusions

A. Summary

To promote the secure and timely delivery of status updates in the IoT, permutation-based short-packet transmissions have been conceived, where eavesdroppers are wiretapping the status updates delivered over the legitimate link. Through adopting the AoI framework and harnessing recent advances in finite-blocklength information theory, we formulated the average AoI of the legitimate link and the average secrecy margin of a wiretap channel in closed forms for quantifying the data freshness and security of status updates. Based on them, the optimal packet structure over the network interface was determined by maximising the secrecy margin while minimising the legitimate AoI. Both our theoretical analysis and numerical results substantiated the secrecy and latency gains achieved by our permutation-based transmission over the conventional transport-layer encapsulation.

B. Observation

In particular, several important insights were gleaned for facilitating the system design of permutation-based short-packet transmissions:

- The optimal blocklength U^* over the network interface is the minimum value in the blocklength range, which leads to legitimate AoI minimisation and secrecy margin maximisation, given the average packet-length $\bar{L}$ of a status update.
- The secrecy margin is improved by our permutation-based transmission, upon reducing the legitimate link SNR $\bar{\gamma}_{\mathrm{B}}$, increasing the coding rate R, reducing the shortest packet-length M, or increasing the number of available lengths, K.
- The legitimate AoI is reduced by our permutation-based transmission, upon increasing the legitimate link SNR $\bar{\gamma}_{\mathrm{B}}$, reducing the coding rate R, extending the shortest packet-length M, or increasing the number of available lengths, K.

C. Future Work

The studies we initiated here are the beginning of our research on the application of the AoI framework in secure URLLCs. The following directions are being pursued to apply the concept of secrecy margin in more complicated scenarios:

- The interactions and combinations of the permutation-based transmission with physical-layer security techniques, such as artificial noise and varied mapping patterns, are to be carried out and evaluated in the secrecy margin framework.
- Advanced physical-layer security solutions are to be addressed against the collaboration among multiple eavesdroppers possessing powerful computational ability, from the perspective of secrecy margin.
- The intense competition among a large number of devices and the delivery of massive status updates in the dense IoT are to be addressed for achieving secure URLLCs in the secrecy margin framework.

Appendix A
Proof of Lemma 1

The first-order derivative of the function $\bar{A}(U)$ with respect to U is given by

$$\begin{aligned}\frac{\mathrm{d}\bar{A}(U)}{\mathrm{d}U} &= \frac{2+\bar{\epsilon}_{\mathrm{B}}}{2W(1-\bar{\epsilon}_{\mathrm{B}})} + \frac{3U\bar{\epsilon}'_{\mathrm{B}}}{2W(1-\bar{\epsilon}_{\mathrm{B}})^2} \\ &> \frac{2+(\bar{\epsilon}_{\mathrm{B}}+U\bar{\epsilon}'_{\mathrm{B}})+2U\bar{\epsilon}'_{\mathrm{B}}}{2W(1-\bar{\epsilon}_{\mathrm{B}})}. \end{aligned} \tag{50}$$

The average packet error probability at Bob, $\bar{\epsilon}_{\mathrm{B}}$, is expressed by (17), which is further reformulated as

$$\begin{aligned}\bar{\epsilon}_{\mathrm{B}} &= 1 - \frac{\bar{\gamma}_{\mathrm{B}}}{2\nu}\left[\exp\left(-\frac{\mu-\nu}{\bar{\gamma}_{\mathrm{B}}}\right) - \exp\left(-\frac{\mu+\nu}{\bar{\gamma}_{\mathrm{B}}}\right)\right] \\ &\overset{(\mathrm{a})}{\approx} \mu/\bar{\gamma}_{\mathrm{B}} = (2^{\bar{L}/U}-1)/\bar{\gamma}_{\mathrm{B}}, \end{aligned} \tag{51}$$

where (a) is achieved through the Taylor approximation of degree 2, i.e., $e^{\alpha} \approx 1+\alpha+\alpha^2/2$, and the parameter $\mu \in (0,1)$ is given by (12).

The first-order derivative of $\bar{\epsilon}_{\mathrm{B}}$ with respect to U is expressed as

$$\bar{\epsilon}'_{\mathrm{B}} = -\bar{L}(\ln 2)2^{\bar{L}/U}/(\bar{\gamma}_{\mathrm{B}}U^2) < 0. \tag{52}$$

Then, we have

$$U\bar{\epsilon}'_{\mathrm{B}} = -R(\ln 2)2^{R}/\bar{\gamma}_{\mathrm{B}} < 0 \tag{53}$$

and

$$\bar{\epsilon}_{\mathrm{B}} + U\bar{\epsilon}'_{\mathrm{B}} = [2^{R}(1-R\ln 2)-1]/\bar{\gamma}_{\mathrm{B}} < 0, \tag{54}$$

where $R = \bar{L}/U \in (0,1)$ is the coding rate, and

$$0 < R(\ln 2)2^{R} < 2\ln 2 \approx 1.39, \tag{55}$$

$$0.61 \approx 2(1-\ln 2) < 2^{R}(1-R\ln 2) < 1. \tag{56}$$

Based on (53), (54), (55), and (56), the inequality (50) is written as

$$\begin{aligned}\frac{\mathrm{d}\bar{A}(U)}{\mathrm{d}U} &> \frac{2+(0.61-1)/\bar{\gamma}_{\mathrm{B}} - 1.39/\bar{\gamma}_{\mathrm{B}}}{2W(1-\bar{\epsilon}_{\mathrm{B}})} \\ &= \frac{2-1.78/\bar{\gamma}_{\mathrm{B}}}{2W(1-\bar{\epsilon}_{\mathrm{B}})} > 0. \end{aligned} \tag{57}$$

As a consequence, the function $\bar{A}(U)$ is a monotonically increasing function of U, which completes the proof of **Lemma 1**.

■

Appendix B
Proof of Lemma 2

The first-order derivative of the function $\bar{S}(U)$ with respect to U is obtained by (58) at the top of next page.

Similar to $\bar{\epsilon}_{\mathrm{B}}$, Eve's average packet error probability $\bar{\epsilon}_{\mathrm{E}}$, of (40), is further reformulated as

$$\begin{aligned}\bar{\epsilon}_{\mathrm{E}} &= 1 - \frac{\bar{\gamma}_{\mathrm{E}}}{2\nu}\left[\exp\left(-\frac{\mu-\nu}{\bar{\gamma}_{\mathrm{E}}}\right) - \exp\left(-\frac{\mu+\nu}{\bar{\gamma}_{\mathrm{E}}}\right)\right] \\ &\overset{(\mathrm{f})}{\approx} \mu/\bar{\gamma}_{\mathrm{E}} = (2^{\bar{L}/U}-1)/\bar{\gamma}_{\mathrm{E}}, \end{aligned} \tag{59}$$

where (f) is achieved through the Taylor approximation of degree 2. The first-order derivative of $\bar{\epsilon}_{\mathrm{E}}$ with respect to U is given by

$$\bar{\epsilon}'_{\mathrm{E}} = -\bar{L}(\ln 2)2^{\bar{L}/U}/(\bar{\gamma}_{\mathrm{E}}U^2) < 0. \tag{60}$$

Thus, we have

$$U\bar{\epsilon}'_{\mathrm{E}} = -R(\ln 2)2^{R}/\bar{\gamma}_{\mathrm{E}} < 0 \tag{61}$$

and

$$\bar{\epsilon}_{\mathrm{E}} + U\bar{\epsilon}'_{\mathrm{E}} = [2^{R}(1-R\ln 2)-1]/\bar{\gamma}_{\mathrm{E}} < 0. \tag{62}$$

Given that $\bar{\gamma}_{\mathrm{E}} < \bar{\gamma}_{\mathrm{B}}$, we have $1 > \bar{\epsilon}_{\mathrm{E}} > \bar{\epsilon}_{\mathrm{B}} > 0$ and $\bar{\epsilon}'_{\mathrm{E}} < \bar{\epsilon}'_{\mathrm{B}} < 0$. Based on (54), (55), (56), (61) and (62), the items in (58) are written as follows:

$$(\mathrm{b}) < \frac{\bar{\epsilon}'_{\mathrm{E}}(1-\bar{\epsilon}_{\mathrm{B}}) - \bar{\epsilon}'_{\mathrm{B}}(1+\bar{\epsilon}_{\mathrm{E}}) + 2(1+\bar{\epsilon}_{\mathrm{E}})\bar{\epsilon}'_{\mathrm{E}} - 2\bar{\epsilon}'_{\mathrm{B}}}{(1-\bar{\epsilon}_{\mathrm{B}})^2}$$

$$\begin{aligned}\frac{\mathrm{d}\bar{S}(U)}{\mathrm{d}U} = {} & \frac{U}{2W}\underbrace{\left[\frac{\bar{\epsilon}'_{\mathrm{E}}(1-\bar{\epsilon}_{\mathrm{B}})-\bar{\epsilon}'_{\mathrm{B}}(1+\bar{\epsilon}_{\mathrm{E}})}{(1-\bar{\epsilon}_{\mathrm{E}})^2}+\frac{2(1+\bar{\epsilon}_{\mathrm{E}})(1-\bar{\epsilon}_{\mathrm{B}})\bar{\epsilon}'_{\mathrm{E}}}{(1-\bar{\epsilon}_{\mathrm{E}})^3}-\frac{2\bar{\epsilon}'_{\mathrm{B}}}{(1-\bar{\epsilon}_{\mathrm{B}})^2}\right]}_{\text{(b)}}\underbrace{\left(\frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}}-\frac{\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}\right)}_{\text{(c)}} \\ & +\frac{1}{2W}\underbrace{\left[\frac{(1+\bar{\epsilon}_{\mathrm{E}})(1-\bar{\epsilon}_{\mathrm{B}})}{(1-\bar{\epsilon}_{\mathrm{E}})^2}-\frac{1+\bar{\epsilon}_{\mathrm{B}}}{1-\bar{\epsilon}_{\mathrm{B}}}\right]}_{\text{(d)}}\underbrace{\left[\frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}}-\frac{\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}}+\frac{U\bar{\epsilon}'_{\mathrm{E}}}{(1-\bar{\epsilon}_{\mathrm{E}})^2}-\frac{U(\bar{\epsilon}'_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}+\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}'_{\mathrm{E}})}{(1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}})^2}\right]}_{\text{(e)}}\end{aligned} \tag{58}$$

$$\begin{aligned} & = \frac{\bar{\epsilon}'_{\mathrm{E}}(3-\bar{\epsilon}_{\mathrm{B}})-\bar{\epsilon}'_{\mathrm{B}}(3+\bar{\epsilon}_{\mathrm{E}})+2\bar{\epsilon}_{\mathrm{E}}\bar{\epsilon}'_{\mathrm{E}}}{(1-\bar{\epsilon}_{\mathrm{B}})^2} \\ & < \frac{(\bar{\epsilon}'_{\mathrm{E}}-\bar{\epsilon}'_{\mathrm{B}})(3-\bar{\epsilon}_{\mathrm{E}})}{(1-\bar{\epsilon}_{\mathrm{B}})^2} < 0, \qquad (63) \\ \text{(c)} & > \frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}}-\frac{\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}} = 0, \qquad (64) \\ \text{(d)} & > \frac{1+\bar{\epsilon}_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{E}}}-\frac{1+\bar{\epsilon}_{\mathrm{B}}}{1-\bar{\epsilon}_{\mathrm{B}}} > 0, \qquad (65) \\ \text{(e)} & < \frac{\bar{\epsilon}_{\mathrm{E}}+U\bar{\epsilon}'_{\mathrm{E}}}{(1-\bar{\epsilon}_{\mathrm{E}})^2}-\frac{\bar{\epsilon}_{\mathrm{E}}(\bar{\epsilon}_{\mathrm{B}}+U\bar{\epsilon}'_{\mathrm{B}})+\bar{\epsilon}_{\mathrm{B}}U\bar{\epsilon}'_{\mathrm{E}}}{1-\bar{\epsilon}_{\mathrm{B}}\bar{\epsilon}_{\mathrm{E}}} < 0. \qquad (66) \end{aligned}$$

As a result, we have

$$\frac{\mathrm{d}\bar{S}(U)}{\mathrm{d}U} < 0. \tag{67}$$

Therefore, the function $\bar{S}(U)$ is a monotonically decreasing function of U, which completes the proof of **Lemma 2**.

■

References

[1] A. Cirik, *et al.*, "Toward the Standardization of Grant-Free Operation and the Associated NOMA Strategies in 3GPP", *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 60-66, Dec. 2019.

[2] N. Varsier, *et al.*, "A 5G New Radio for Balanced and Mixed IoT Use Cases: Challenges and Key Enablers in FR1 Band", *IEEE Commun. Mag.*, vol. 59, no. 4, pp. 82-87, Apr. 2021.

[3] F. Montori, L. Bedogni, and L. Bononi, "A collaborative internet of things architecture for smart cities and environmental monitoring," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 592–605, Apr. 2018.

[4] R. Du, P. Santi, M. Xiao, A. V. Vasilakos, and C. Fischione, "The sensable city: A survey on the deployment and management for smart city monitoring," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1533-1560, 2nd Quart. 2019.

[5] Y. Yang, "Permutation-based transmissions in ultra-reliable and low-latency communications", *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 1024-1028, March 2021.

[6] Y. Yang and L. Hanzo, "Permutation-based TCP and UDP transmissions to improve goodput and latency in the Internet-of-Things", *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14276-14286, Sep. 2021.

[7] F. Guo, *et al.*, "Enabling massive IoT toward 6G: A comprehensive survey", *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891-11915, Aug. 2021.

[8] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[9] G. Durisi, T. Koch, and P. Popovski, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sept. 2016.

[10] S. Kaul, M. Gruteser, V. Rai, and J. Kenney, "Minimizing age of information in vehicular networks", in *Proc. IEEE Conf. Sensor, Mesh Ad Hoc Commun. Netw. (SECON)*, Salt Lake City, UT, USA, Jun. 2011, pp. 350-358.

[11] R. Yates, *et al.*, "Age of information: An introduction and survey", *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1183-1210, May 2021.

[12] B. Zhou and W. Saad, "Joint Status Sampling and Updating for Minimizing Age of Information in the Internet of Things", *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7468-7482, Nov. 2019.

[13] P. Mayekar, P. Parag, and H. Tyagi, "Optimal source codes for timely updates," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3714-3731, Jun. 2020.

[14] A. Arafa, K. Banawan, K. G. Seddik, and H. V. Poor, "On timely channel coding with hybrid ARQ," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[15] B. Zhou and W. Saad, "Performance Analysis of Age of Information in Ultra-Dense Internet of Things (IoT) Systems With Noisy Channels", *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3493-3507, May 2022.

[16] R. Wang, *et al.*, "On the age of information of short-packet communications with packet management", in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1-6.

[17] H. Pan and S. Liew, "Information update: TDMA or FDMA?", *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 856-860, Jun. 2020.

[18] B. Yu, Y. Cai, D. Wu, and Z. Xiang, "Average age of information in short packet based machine type communication", *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10306-10319, Sep. 2020.

[19] D. Zheng, Y. Yang, L. Wei and B. Jiao, "Decode-and-forward short-packet relaying in the Internet of Things: Timely status updates", *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 8423-8437, Dec. 2021.

[20] C. Feng, H. Wang and H. V. Poor, "Reliable and Secure Short-Packet Communications", *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1913-1926, Mar. 2022.

[21] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[22] L. Wei, Y. Yang and B. Jiao, "Secrecy Throughput in Full-Duplex Multiuser MIMO Short-Packet Communications", *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1339-1343, Jun. 2021.

[23] H. Bastami, *et al.*, "Maximizing the Secrecy Energy Efficiency of the Cooperative Rate-Splitting Aided Downlink in Multi-Carrier UAV Networks", *IEEE Trans. Veh. Tech.*, 2022.

[24] Z. Zheng, *et al.*, "Secure UAV-to-Ground MIMO Communications: Joint Transceiver and Location Optimization", *IEEE Trans. Veh. Tech.*, 2022.

[25] T. Bai, J. Wang, Y. Ren and L. Hanzo, "Energy-Efficient Computation Offloading for Secure UAV-Edge-Computing Systems", *IEEE Trans. Veh. Tech.*, vol. 68, no. 6, pp. 6074-6087, Jun. 2019.

[26] L. Qian, *et al.*, "Secrecy-Based Energy-Efficient Mobile Edge Computing via Cooperative Non-Orthogonal Multiple Access Transmission", *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4659-4677, Jul. 2021.

[27] W. Yang, *et al.*, "Age of Information for Short-Packet Covert Communication", *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1890-1894, Sep. 2021.

[28] H. Chen, Q. Wang, P. Mohapatra, and N. Pappas, "Secure Status Updates under Eavesdropping: Age of Information-based Physical Layer Security Metrics", arXiv:2002.07340.

[29] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate", *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 877-889, Apr. 2018.

[30] Y. Yang, M. Ma, S. Aissa and L. Hanzo, "Physical-layer secret key generation via CQI-mapped spatial modulation in multi-hop wiretap ad-hoc networks", *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1322-1334, 2021.

[31] M. Yin, Y. Yang and B. Jiao, "Security-oriented trellis code design for spatial modulation", *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1875-1888, Mar. 2021.

[32] Y. Liu, Y. Yang, L. Yang and L. Hanzo, "Physical layer security of spatially modulated sparse-code multiple access in aeronautical ad-hoc networking", *IEEE Trans. Veh. Tech.*, vol. 70, no. 3, pp. 2436-2447, Mar. 2021.

[33] Y. Yang and W. Li, “Security-oriented polar coding based on channel-gain-mapped frozen bits”, *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 6584-6596, Aug. 2022.

[34] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[35] B. Makki, T. Svensson, and M. Zorzi, “Finite block-length analysis of the incremental redundancy HARQ”, *IEEE Wireless Commun. Lett.*, vol. 3, no. 5, pp. 529–532, Oct. 2014.

[36] A. Ghosh, “5G New Radio (NR) : Physical Layer Overview and Performance”, in *IEEE Commun. Theory Workshop*, May 2018. [Online Available] https://ctw2018.ieee-ctw.org/files/2018/05/5G-NR-CTW-final.pdf

[37] F. W. Vook, A. Ghosh, E. Diarte and M. Murphy, “5G New Radio: Overview and Performance”, in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, USA, 2018, pp. 12471251.

Yuli Yang (S’04-M’08-SM’19) received her Ph.D. degree in Communications & Information Systems from Peking University in July 2007. Since Dec 2019, she has been with the University of Lincoln as a Senior Lecturer in Electrical/Electronic Engineering. From Jan 2010 to Dec 2019, she was with King Abdullah University of Science & Technology, Melikşah University, and the University of Chester on various academic positions. Her industry experience includes working as a Research Scientist with Bell Labs Shanghai, from Aug 2007 to Dec 2009, and an Intern Researcher with Huawei Technologies, from June 2006 to July 2007. Her research interests include modelling, design, analysis and optimization of wireless systems and networks.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) (FIEEE’04, Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP), received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He has published widely at IEEE Xplore, coauthored 19 Wiley-IEEE Press books and has helped the fast-track career of 123 PhD students. He holds the Eric Sumner Technical Field Award.