Secure and Timely Status Updates in the IoT using Short-Packet Permutation-Based Transmissions

Yuli Yang
School of Computer Science and Electronic Engineering
University of Essex
Colchester CO4 3SQ, U.K.
yuli.yang@essex.ac.uk
ORCID: 0000-0002-6634-5349

***Abstract*—The permutation-based transmission has been recently proposed as an efficient transport-layer design strategy to achieve ultra-reliable and low-latency communications (URLLCs) in the Internet of Things (IoT). In this paper, the age of information (AoI) is exploited as a framework to characterise the performance of short-packet permutation-based transmissions in a wiretap channel, and the concept of secrecy margin is formulated to quantify the data security while guaranteeing the data freshness of status updates. In solving the optimisation problem of secrecy margin maximisation within the regime of finite-blocklength information theory, the optimal packet structure over the network interface is obtained in the IoT using short-packet permutation-based transmission. Illustrative numerical results on the comparisons between the permutation-based transmission and the conventional encapsulation not only substantiate the performance gains achieved by the former, but also provide useful references for its system design for achieving secure URLLCs.**

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

I. Introduction

GIVING rise to the Internet of Things (IoT), the implementation of ultra-reliable and low-latency communications (URLLCs) needs to address a huge amount of end-to-end connectivities through scarce resources. The collaboration among different subscribers over common resources increases the security risks [1], [2]. Recently, the permutation-based transmission [3] has been proposed as a promising solution to the fundamental infrastructure for URLLCs, specifically in the IoT [4].

The permutation-based transmission is a transport-layer design strategy, where a portion of application-layer data is not physically encapsulated into the transport-layer data units (DUs) but conveyed by the permutation with repetition of various DU lengths in a group of packets. Moreover, in [5], the transmission order arrangement is utilised as a transport-layer resource for the permutation, where a portion of information bits in the DU of a packet, referred to as opportunistic bits, are conveyed by the index of the time slot when the packet is transmitted.

In addressing the challenge of scarce resources, the permutation-based transmission has been proven to be a successful application of the permutation philosophy in the transport layer, which effectively improves the spectral efficiency and energy efficiency while increasing the goodput and reducing the latency, compared with conventional transport-layer encapsulation [3], [4]. Concerning short-packet communications over wireless channels contribute to the practical requirements associated with URLLCs, the performance of permutation-based transmissions has been investigated in terms of maximal payload rate, latency reduction, spectral efficiency gain, and energy efficiency gain based on the advances of finite-blocklength information theory [5], [6].

In addressing the challenge of security risks, the secrecy rate of permutation-based transmissions has been analysed in [3] and [4], where the mapping pattern of the application-layer data conveyed by the permutations is interpreted as a secret key in the legitimate link and, therefore, eavesdroppers are unable to successfully decode these data since they have no knowledge on the secret key.

Within the IoT, various types of sensors are deployed to monitor specific physical parameters such as temperature, humidity, wind strength, etc., and deliver the status updates to actuators for performing subsequent actions [7], [8]. To guarantee the accuracy and efficacy of the actions, the IoT needs to keep the status updates fresh. The age of information (AoI) was proposed in [9] and [10] as a metric to measure the freshness of the status updates, which is used to characterise the timestamp of the latest successfully decoded status update at the legitimate destination [11], [12].

Recent advances in the finite-blocklength information theory have established a basis for the design of short-packet protocols to achieve URLLCs [13], [14]. Specifically for the delivery of status updates in the IoT, the AoI framework of short-packet communications has been developed in the finite-blocklength regime and optimised with various packet management schemes; see e.g., [15]–[18] and references therein, where the average AoI is used as a key metric to evaluate the data freshness from an ergodic perspective.

In this paper, the AoI framework of short-packet communications is exploited to evaluate the data security of status updates in wiretap channels given that the IoT has to maintain the data freshness of status updates. For the delivery of a single packet, the secrecy margin over a wiretap channel

This work was supported in part by the Engineering and Physical Sciences Research Council Project under Grant EP/X04047X/1.

is defined as the positive difference between the legitimate AoI and the wiretapping AoI [19]. Herein, we formulate the average secrecy margin for short-packet permutation-based transmissions in the finite-blocklength regime. On one hand, the way to enhance the data security is to maximise the secrecy margin, which achieves the optimal packet structure from a security perspective. On the other hand, the way to guarantee the data freshness is to minimise the legitimate AoI, which drives the optimal packet structure from the timeliness perspective. Based on the optimal packet design over the network interface, the secure and timely performance of short-packet permutation-based transmissions is compared with that of conventional transport-layer encapsulation in terms of the secrecy margin and the legitimate AoI, to verify the advantage of permutation-based transmissions in secure and timely status updates.

The contributions of this paper are three-fold. Firstly, we present the system model of short-packet permutation-based transmissions over a wiretap channel. Secondly, we formulate the average secrecy margin in the finite-blocklength regime for the secure and timely delivery of status updates via short-packet permutation-based transmissions. Thirdly, we solve the optimisation problem of the average secrecy margin maximisation for short-packet permutation-based transmissions to achieve optimal packet structure over the network interface in wiretap channels.

The remainder of this paper is organized as follows. Section II presents the system model of short-packet permutation-based transmissions over a wiretap channel. Section III formulates the average secrecy margin of short-packet permutation-based communications and achieves the optimal packet structures over the network interface for data security. Section IV provides illustrative numerical results to demonstrate the performance gain obtained by the permutation-based transmission over the conventional transport-layer encapsulation. Finally, Section V concludes this paper.

Notations: $f_X(x)$ 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. Besides, $\mathbb{E}(\cdot)$ denotes the expectation (mean) operator, and $\Pr[\cdot]$ denotes the probability of an event. In addition, $\mathbb{N}$ stands for the set of all natural numbers, and $\lceil \cdot \rceil$ denotes the least integer function.

II. System Model

Consider a wiretap channel in the IoT, where Alice monitors the status updates and delivers them to Bob. Bob is the legitimate actuator who takes actions upon decoding his received status updates. Meanwhile, an unauthorised eavesdropper Eve attempts to extract the status updates by wiretapping Alice's transmissions. All the nodes, i.e., Alice, Bob, and Eve, are single-antenna devices.

The automatic repeat request (ARQ) mechanism is adopted in the legitimate link, i.e., from Alice to Bob, for guaranteeing the reliable delivery of status updates. For the delivery of a given status update over the legitimate link, Bob will send an acknowledgement (ACK) to Alice once successfully decoding the status update. The ACK triggers Alice to generate the next status update and commence with the delivery of the new one. If Alice does not receive an ACK before the predetermined timeout, she will retransmit the current status update until receiving an ACK.

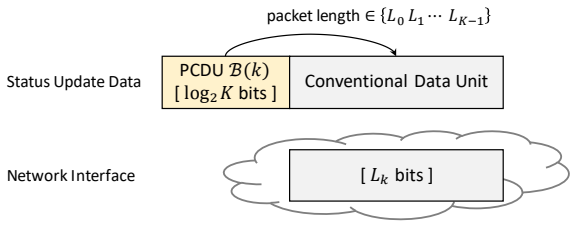


Fig. 1. The permutation-based encapsulation of a single status update at the transport layer of the legitimate link.

Alice utilises the permutation-based transport-layer design for improving the spectral efficiency and energy efficiency of the delivery. The permutation-based encapsulation of a status update into a packet is presented in Fig. 1, where the status update data is divided into two portions for the delivery via a packet. The portion referred to as permutation-conveyed data unit (PCDU) is mapped onto the packet length rather than encapsulated into the conventional DU. More specifically, the PCDU consists of $\log_2 K$ bits, mapped onto assigning one of the K lengths $L_0, L_1, \cdots, L_{K-1}$ to the packet. Then, the conventional DU, of the length determined by the PCDU, is encapsulated into the packet in a conventional way and physically delivered through the network interface. In this way, the 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 delivers the packet of length L_k, $k \in \{0, 1, \cdots, K-1\}$, conveying the PCDU through the selection among the K various packet lengths $L_0, L_1, \cdots, L_{K-1}$.

The K lengths can be set to an arithmetic sequence of $L_k = M + kC$ bits, $k = 0, 1, \cdots, K-1$, where the initial 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 $\mathcal{B}(\cdot)$ represents a $\log_2 K$-bit binary coded decimal function, and $k = 0, 1, \cdots, K-1$.

Without loss of generality, the K lengths are assigned to a packet at the same probability $1/K$. Thus, the mean length of a packet, in the unit of [bits], is

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

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

$$L_{K-1} = M + (K-1)C \leqslant L_{\max}. \tag{2}$$

In particular, we consider short-packet communications with the permutation-based transmission in the IoT, where a packet is of mean length $\bar{L}$, given in (1), conveying a status update characterised by $\log_2 K + \bar{L}$ information bits. We remark that, with the conventional transport-layer encapsulation, a packet of length $\bar{L}$ conveys the status update characterised by $\bar{L}$ information bits.

Over the network interface, the coding rate is denoted by $R = \bar{L}/U \in (0,1)$, where U is the blocklength in the unit of physical channel uses. Given a packet error probability, denoted by ϵ, the maximal coding rate of short-packet permutation-based transmissions, R, in the finite-blocklength regime is approximated by [13]

$$\bar{L}/U \approx \log_2(1+\gamma) - \frac{Q^{-1}(\epsilon)}{\ln 2}\sqrt{\frac{1-(1+\gamma)^{-2}}{U}}, \quad (3)$$

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

From (3), the packet error probability ϵ is written as

$$\epsilon \triangleq Q\big[\theta(\bar{L}, U, \gamma)\big], \quad (4)$$

with the notation

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

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

$$\bar{\epsilon} = \int_0^\infty Q\big[\theta(\bar{L}, U, x)\big] f_\gamma(x) \mathrm{d}x, \quad (5)$$

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 expressed as [19]

$$Q\big[\theta(\bar{L}, U, x)\big] \approx \begin{cases} 1, & x \leqslant \mu - \nu, \\ \dfrac{1}{2} - \dfrac{x-\mu}{2\nu}, & \mu - \nu \leqslant x \leqslant \mu + \nu, \\ 0, & x \geqslant \mu + \nu, \end{cases} \quad (6)$$

where

$$\mu = 2^{\bar{L}/U} - 1, \quad (7)$$

$$\nu = \sqrt{\pi(2^{2\bar{L}/U} - 1)/(2U)}. \quad (8)$$

Using the linear approximation (6), the closed-form expression of $\bar{\epsilon}$ can be obtained by

$$\bar{\epsilon} = \frac{1}{2\nu}\int_{\mu-\nu}^{\mu+\nu} F_\gamma(x) \mathrm{d}x, \quad (9)$$

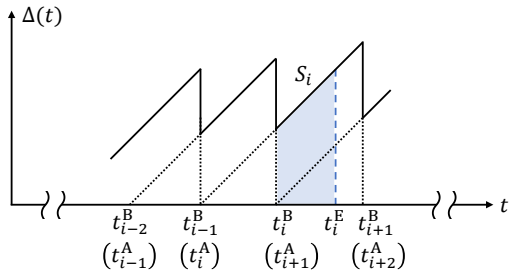
where

$$F_\gamma(x) = \begin{cases} 1 - \exp(-x/\bar{\gamma}), & x \geqslant 0 \\ 0, & x < 0 \end{cases} \quad (10)$$

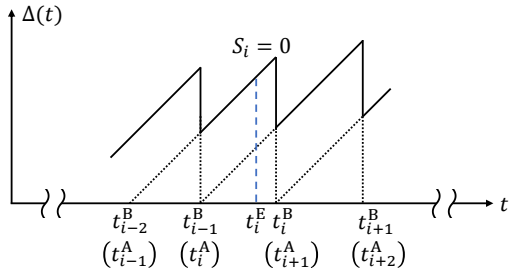
is the cdf of the SNR γ over Rayleigh fading channels.

III. Secrecy Margin

An evolution of the secrecy margin is shown in Fig. 2, where $\Delta(t)$ denotes the instantaneous AoI, i.e., the time elapsed since Alice's generation of the latest status update that has been successfully decoded at Bob. If there is no status update decoded successfully at Bob, the AoI increases linearly with time.



(a) Secure Delivery



(b) Information Leakage

Fig. 2. An evolution of secrecy margin, S_i.

Alice generates and commences with the transmission of the i^{th} status update at the time t_i^{A}, which is triggered by Bob's ACK on the $(i-1)^{\text{th}}$ status update. Bob and Eve successfully decode the i^{th} status update at t_i^{B} and t_i^{E}, respectively. 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 $t_i^{\text{B}} = t_{i+1}^{\text{A}}$, $i = 1, 2, \cdots$.

In Fig. 2(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., $t_i^{\text{E}} > t_i^{\text{B}}$. In other words, Eve needs more retransmissions of the i^{th} status update than Bob does for the successful decoding. However, Alice will not transmit this status update any more upon receiving Bob's ACK. This disables Eve from unveiling this status update.

In Fig. 2(b), Eve successfully decodes the i^{th} status update earlier than Bob does, i.e., $t_i^{\text{E}} < t_i^{\text{B}}$, 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 decoded successfully, the number of total (re)transmissions requested by Bob is $K_{\text{B},i}$, whilst Eve needs $K_{\text{E},i}$ (re)transmissions. Consequently, the time duration for Bob to successfully decode the i^{th} status update is

$$t_i^{\text{B}} - t_i^{\text{A}} = K_{\text{B},i} T, \quad (11)$$

and the time duration for Eve to unveil this status update is

$$t_i^{\text{E}} - t_i^{\text{A}} = K_{\text{E},i} T, \quad (12)$$

where

$$T = U/W \tag{13}$$

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

As shown in Fig. 2(a), the secrecy of the i^{th} status update is guaranteed if its successful delivery to Eve is later than that to Bob, i.e., the time duration $K_{\text{E},i}T > K_{\text{B},i}T$.

The average secrecy margin is defined as

$$\bar{S} = \lim_{t\to\infty} \frac{1}{t} \sum_{i=1}^{N(t)} S_i, \tag{14}$$

where $N(t)$ is the number of status updates decoded successfully by Bob at time t, and S_i, marked by the shadow in Fig. 2(a), is calculated using

$$\begin{aligned} S_i &= [(t_i^{\text{B}} - t_i^{\text{A}}) + (t_i^{\text{E}} - t_i^{\text{A}})](t_i^{\text{E}} - t_i^{\text{B}})/2 \\ &= (K_{\text{B},i}T + K_{\text{E},i}T)(K_{\text{E},i}T - K_{\text{B},i}T)/2 \\ &= (K_{\text{E},i}^2 - K_{\text{B},i}^2)T^2/2. \end{aligned} \tag{15}$$

Note that, $S_i = 0$ if $t_i^{\text{E}} < t_i^{\text{B}}$, as shown in Fig. 2(b).

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

$$\eta_i = \begin{cases} 1, & S_i \neq 0, \\ 0, & S_i = 0, \end{cases} \tag{16}$$

and the accumulative total number of secure status updates is thus expressed as

$$N_{\text{S}}(t) = \sum_{i=1}^{N(t)} \eta_i. \tag{17}$$

As such, the average secrecy margin, defined in (14), can be calculated using

$$\bar{S} = \lim_{t\to\infty} \frac{N_{\text{S}}(t)}{t} \mathbb{E}(S) = \lambda \mathbb{E}(S), \tag{18}$$

where

$$\lambda = \lim_{t\to\infty} \frac{N_{\text{S}}(t)}{t}$$

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 independent and identically distributed (i.i.d.) random variables from the ergodic perspective.

Obviously, the number of (re)transmissions for the i^{th} status update requested by Bob or needed by Eve, $K_{\Psi,i}$, $\Psi \in \{\text{B}, \text{E}\}$, follows a Geometric distribution with the delivery success probability $(1 - \bar{\epsilon}_\Psi)$, where $\bar{\epsilon}_\Psi$ is the average packet error probability at Bob or Eve, calculated using (9). Therefore, the mean and the second moment of the i.i.d. random variables $K_{\Psi,i}$, $i = 1, 2, \cdots$, are

$$\mathbb{E}(K_\Psi) = \frac{1}{1 - \bar{\epsilon}_\Psi} \tag{19}$$

and

$$\mathbb{E}(K_\Psi^2) = \frac{1 + \bar{\epsilon}_\Psi}{(1 - \bar{\epsilon}_\Psi)^2}, \tag{20}$$

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

As a result, the expectation of S_i is expressed as

$$\begin{aligned} \mathbb{E}(S) &= \mathbb{E}(K_{\text{E}}^2)T^2/2 - \mathbb{E}(K_{\text{B}}^2)T^2/2 \\ &= \frac{(1 + \bar{\epsilon}_{\text{E}})T^2}{2(1 - \bar{\epsilon}_{\text{E}})^2} - \frac{(1 + \bar{\epsilon}_{\text{B}})T^2}{2(1 - \bar{\epsilon}_{\text{B}})^2}. \end{aligned} \tag{21}$$

Moreover, the rate of secure delivery from Alice to Bob, λ, is achieved at

$$\lambda = \frac{\Pr[K_{\text{B}} < K_{\text{E}}]}{\mathbb{E}(K_{\text{B}})T} = \frac{1 - \bar{\epsilon}_{\text{B}}}{T} \Pr[K_{\text{B}} < K_{\text{E}}], \tag{22}$$

where the probability

$$\begin{aligned} \Pr[K_{\text{B}} < K_{\text{E}}] &= \sum_{k=1}^{\infty} (1 - \bar{\epsilon}_{\text{B}}^k)\bar{\epsilon}_{\text{E}}^k \\ &= \frac{\bar{\epsilon}_{\text{E}}}{1 - \bar{\epsilon}_{\text{E}}} - \frac{\bar{\epsilon}_{\text{B}}\bar{\epsilon}_{\text{E}}}{1 - \bar{\epsilon}_{\text{B}}\bar{\epsilon}_{\text{E}}}. \end{aligned} \tag{23}$$

Substituting (21) and (22) into (18), we have the average secrecy margin written as

$$\begin{aligned} \bar{S} = \frac{T}{2} &\left[\frac{(1 + \bar{\epsilon}_{\text{E}})(1 - \bar{\epsilon}_{\text{B}})}{(1 - \bar{\epsilon}_{\text{E}})^2} - \frac{1 + \bar{\epsilon}_{\text{B}}}{1 - \bar{\epsilon}_{\text{B}}} \right] \\ &\times \left(\frac{\bar{\epsilon}_{\text{E}}}{1 - \bar{\epsilon}_{\text{E}}} - \frac{\bar{\epsilon}_{\text{B}}\bar{\epsilon}_{\text{E}}}{1 - \bar{\epsilon}_{\text{B}}\bar{\epsilon}_{\text{E}}} \right), \end{aligned} \tag{24}$$

where the average packet error probability at Bob or Eve, $\bar{\epsilon}_\Psi$, $\Psi \in \{\text{B}, \text{E}\}$, is

$$\begin{aligned} \bar{\epsilon}_\Psi &= \frac{1}{2\nu} \int_{\mu-\nu}^{\mu+\nu} \left[1 - \exp\left(-x/\bar{\gamma}_\Psi\right)\right] \mathrm{d}x \\ &= 1 - \frac{\bar{\gamma}_\Psi}{2\nu} \left[\exp\left(-\frac{\mu - \nu}{\bar{\gamma}_\Psi} \right) - \exp\left(-\frac{\mu + \nu}{\bar{\gamma}_\Psi} \right) \right], \end{aligned} \tag{25}$$

with $\bar{\gamma}_\Psi$, $\Psi \in \{\text{B}, \text{E}\}$, denoting the mean received SNR at Bob or Eve.

As has been proven in [19], the first-order derivative of the function $\bar{S}(U)$ with respect to U is negative, i.e.,

$$\frac{\mathrm{d}\bar{S}(U)}{\mathrm{d}U} < 0. \tag{26}$$

Therefore, the optimal blocklength for maximising the secrecy margin is achieved at

$$\begin{aligned} U^* &= \underset{U \in [U_{\min}, U_{\max}]}{\arg\max} \ \bar{S}(U) \\ &= U_{\min}, \end{aligned} \tag{27}$$

where the minimum blocklength $U_{\min}$ and the maximum blocklength $U_{\max}$ are determined by specific physical-layer protocols. In an ideal scenario where the channel code rate is 1 and the modulation order is 2, i.e., the physical-layer throughput is 1 bit per channel use and $\bar{L}/U = 1$, the possible minimum blocklength is equal to the average packet length of a status update, i.e., $U_{\min} = \bar{L}$.

IV. Numerical Results

In this section, the secrecy margin of permutation-based transmissions is investigated under the constraint of timely delivery of status updates over the legitimate link. Without loss of generality, the network bandwidth is $W = 1$ kHz.

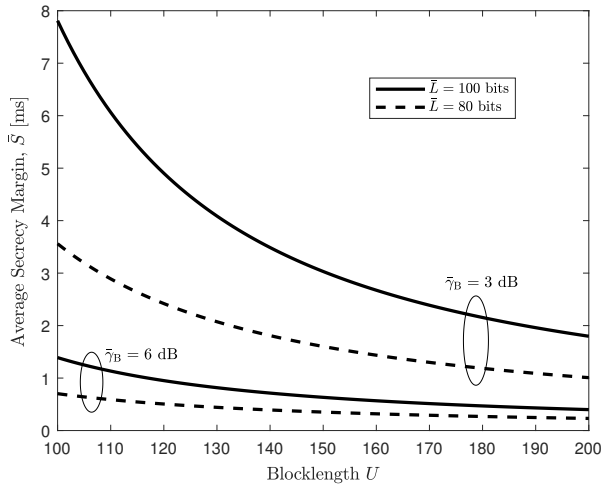
To begin with, the average secrecy margin, $\bar{S}$ given by (24), is plotted as a function of the blocklength U in Fig. 3, where $\bar{S}$ increases as U decreases. This phenomenon agrees with the optimal design (27). Moreover, $\bar{S}$ is improved with the increase in the average packet length $\bar{L}$ of a status update, or with the decrease in the received SNRs $\bar{\gamma}_\Psi$, $\Psi \in \{\mathrm{B}, \mathrm{E}\}$. The main reason behind this is that the higher coding rate $\bar{L}/U$, due to more application-layer data conveyed in a status update, or the lower received SNR $\bar{\gamma}_\Psi$ drives higher packet error probability $\bar{\epsilon}_\Psi$, which results in greater AoI for both Eve and Bob. Furthermore, the secrecy margin $\bar{S}$ is raised as the ratio $\bar{\gamma}_\mathrm{B}/\bar{\gamma}_\mathrm{E}$ increases, because higher ratio $\bar{\gamma}_\mathrm{B}/\bar{\gamma}_\mathrm{E}$ enlarges the gap between the packet error probabilities $\bar{\epsilon}_\mathrm{E}$ and $\bar{\epsilon}_\mathrm{B}$, thus leading to larger gap between Eve's AoI and Bob's AoI.

Then, we will compare the permutation-based transmission with the conventional transport-layer encapsulation in terms of secrecy margin, to explicitly and numerically characterise the advantage of permutation-based transmissions in secure and timely status updates, specifically for short-packet communications in the IoT.

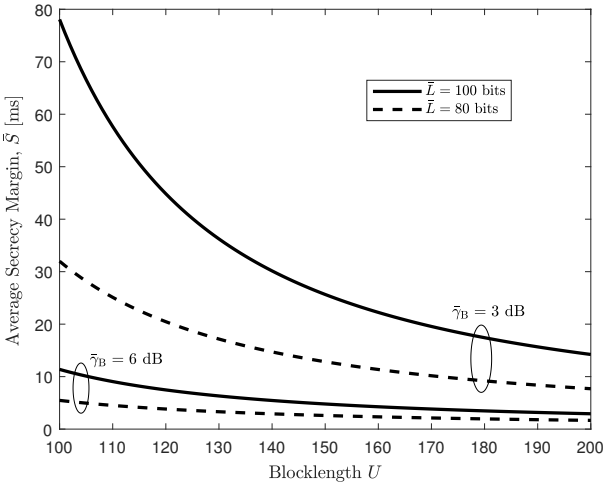
To deliver the same amount of application-layer data, the average packet length $\bar{L}$ utilised in the permutation-based transmission is shorter than that in the conventional transport-layer encapsulation by $\log_2 K$ bits, since the PCDU of $\log_2 K$ bits is not physically encapsulated into the packet but conveyed through the packet length permutation/variation. Given the same coding rate $R = \bar{L}/U$ and the same modulation order, shorter average packet length $\bar{L}$ implies shorter blocklength U. According to (27), shorter blocklength U will lead to higher secrecy margin. Thus, permutation-based transmissions will contribute to the performance improvement for the delivery of status updates within wiretap channels from the perspective of secrecy margin, in addition to the goodput increase and latency reduction.

The parameters in the IoT are set as follows: *(i)* The legitimate link SNR is 1.5 time the wiretapping link SNR, i.e., $\bar{\gamma}_\mathrm{B}/\bar{\gamma}_\mathrm{E} = 1.5$. *(ii)* The average packet length of a status update in permutation-based transmissions is $\bar{L} = (K-1)C/2 + M$, given by (1). *(iii)* The packet length of a status update in the conventional transport-layer encapsulation is $\bar{L} + \log_2 K$, to convey the same amount of information as that in the permutation-based transmission. *(iv)* Given the coding rate $R \in (0, 1)$, the optimal blocklength of the permutation-based transmission is $U^*_\mathrm{pbt} = \lceil \bar{L}/R \rceil$, and that of the conventional transport-layer encapsulation is $U^*_\mathrm{con} = \lceil (\bar{L} + \log_2 K)/R \rceil$.

Given that the permutation-based transmission and the conventional transport-layer encapsulation have the same amount of information contained in a status update while $U^*_\mathrm{pbt} < U^*_\mathrm{con}$, the average secrecy margin of the permutation-based transmission, denoted by $\bar{S}_\mathrm{pbt}$, is higher than that of the conventional transport-layer encapsulation, denoted by $\bar{S}_\mathrm{con}$, based on (27). Therefore, from the perspective of secrecy margin improvement, the performance gain of the permutation-based transmission over the conventional transport-layer encapsulation can be quantified by the secrecy margin difference $\bar{S}_\mathrm{pbt} - \bar{S}_\mathrm{con}$.



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



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

Fig. 3. The average secrecy margin $\bar{S}$ versus the blocklength U.

In Fig. 4, the secrecy margin improvement $\bar{S}_\mathrm{pbt} - \bar{S}_\mathrm{con}$ is plotted versus Bob's received SNR $\bar{\gamma}_\mathrm{B}$, where $K = 128$, $M = 32$, $C = 8$. As shown in this figure, given the amount of information to be delivered for a status update, i.e., $(K-1)C/2 + M + \log_2 K$ bits, the performance gain of the permutation-based transmission in the secrecy margin improvement, $\bar{S}_\mathrm{pbt} - \bar{S}_\mathrm{con}$, is decreased and converges to 0 as the legitimate link SNR $\bar{\gamma}_\mathrm{B}$ increases. The main reason behind this is that, given $\bar{\gamma}_\mathrm{E} = \bar{\gamma}_\mathrm{B}/1.5$, the average packet error probabilities $\bar{\epsilon}_\mathrm{B} = \bar{\epsilon}_\mathrm{E} = 0$ when $\bar{\gamma}_\mathrm{B}$ goes to infinity. As such, both $\bar{S}_\mathrm{pbt}$ and $\bar{S}_\mathrm{con}$ go to 0 as $\bar{\gamma}_\mathrm{B}$ increases.

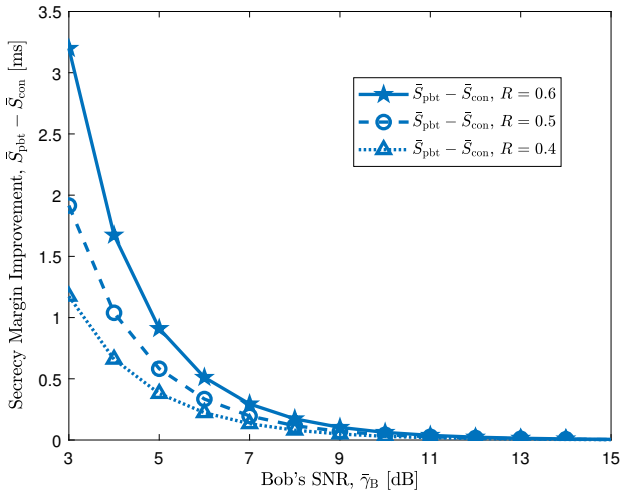


Fig. 4. The secrecy margin improvement $\bar{S}_{\rm pbt} - \bar{S}_{\rm con}$ versus Bob's received SNR $\bar{\gamma}_{\rm B}$, for $K = 128$, $M = 32$, $C = 8$.

In addition, $\bar{S}_{\rm pbt} - \bar{S}_{\rm con}$ gets larger as the coding rate R increases. This indicates that, with the increase in R, the performance gain of the permutation-based transmission over the conventional encapsulation gets larger in terms of secrecy margin improvement.

V. Conclusion

To promote secure and timely delivery of status updates in the IoT, short-packet permutation-based transmissions have been investigated in this paper, where eavesdroppers are wiretapping the status updates delivered over the legitimate link. Through adopting the AoI framework and recent advances in the finite-blocklength information theory, we formulated the average secrecy margin in closed form to quantify the data security and freshness of status updates. Based on the formulation, the optimal packet structure over the network interface was achieved to maximise the average secrecy margin. Both theoretical analysis and numerical results substantiated the secrecy margin improvement achieved by the permutation-based transmission over the conventional transport-layer encapsulation.

In particular, two key insights were reached to facilitate the system design of short-packet permutation-based transmissions:

(i) The optimal blocklength U^* over the network interface is the minimum value in the blocklength range, which maximises the average secrecy margin, given the average packet length $\bar{L}$ of a status update.

(ii) The secrecy margin improvement of the permutation-based transmission is promoted by lowering the legitimate link SNR $\bar{\gamma}_{\rm B}$, heightening the coding rate R, shortening the shortest packet length M, or increasing the number of available lengths, K.

References

[1] 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.

[2] C. Feng and H. Wang, "Secure Short-Packet Communications at the Physical Layer for 5G and Beyond", *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 96-102, Sep. 2021.

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

[4] 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.

[5] M. Yin, Y. Yang, J. Wu and B. Jiao, "Opportunistic bits in short-packet communications: a finite blocklength perspective", *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8085-8099, Dec. 2021.

[6] W. Li, Y. Yang and B. Jiao, "Permutation-based transmissions in finite blocklength regime: Efficient and effective resource utilisation", *IEEE Trans. Commun.*, doi: 10.1109/TCOMM.2023.3253698.

[7] 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.

[8] R. Du, *et al.*, "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.

[9] 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.

[10] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?", in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 2731-2735.

[11] A. Kosta, N. Pappas, and V. Angelakis, "Age of information: A new concept, metric, and tool", *Found. Trends Netw.*, vol. 12, no. 3, pp. 162–259, 2017.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] Y. Yang and L. Hanzo, "Permutation-based short-packet transmissions improve secure URLLCs in the Internet of things", *IEEE Internet Things J.*, vol. 10, no. 12, pp. 11024-11037, Jun. 2023.